EURÓPSKA
KOMISIA

V Bruseli 12. 9. 2018
COM(2018) 630 final

2018/0328 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier

Príspevok Európskej komisie k zasadnutiu lídrov v Salzburgu v dňoch 19. – 20. septembra 2018

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

DÔVODOVÁ SPRÁVA

1. KONTEXT NÁVRHU

• Dôvody a ciele návrhu

Keďže každodenný život a hospodárstva sú stále závislejšie od digitálnych technológií, občania sú čoraz viac vystavení vážnym kybernetickým incidentom. Budúca bezpečnosť závisí od posilnenia schopnosti chrániť Úniu pred kybernetickými hrozbami, keďže civilná infraštruktúra aj vojenské kapacity sa spoliehajú na bezpečné digitálne systémy.

S cieľom riešiť rastúce problémy Únia postupne rozširovala svoje činnosti v tejto oblasti, pričom vychádzala zo stratégie kybernetickej bezpečnosti z roku 2013[1] a jej cieľov a zásad na podporu spoľahlivého, bezpečného a otvoreného kybernetického ekosystému. V roku 2016 Únia prijala svoje prvé opatrenia v oblasti kybernetickej bezpečnosti v podobe smernice Európskeho parlamentu a Rady (EÚ) 2016/1148[2] o bezpečnosti sietí a informačných systémov.

Vzhľadom na rýchlo sa vyvíjajúce prostredie kybernetickej bezpečnosti v septembri 2017 Komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku predložili spoločné oznámenie[3] s názvom „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ“ na ďalšie posilnenie odolnosti Únie, odrádzanie od kybernetických útokov a reakcieschopnosť na ne. V spoločnom oznámení, ktoré nadväzovalo aj na predchádzajúce iniciatívy, sa načrtol súbor navrhovaných opatrení, okrem iného vrátane posilnenia Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), vytvorenia dobrovoľného celoúnijného rámca certifikácie kybernetickej bezpečnosti s cieľom zvýšiť kybernetickú bezpečnosť produktov a služieb v digitálnom svete, ako aj koncepcie rýchlej a koordinovanej reakcie na kybernetické incidenty a krízy veľkého rozsahu.

V spoločnom oznámení sa uznáva, že je aj v strategickom záujme Únie zabezpečiť, aby si zachovala a rozvíjala základné technologické kapacity v oblasti kybernetickej bezpečnosti s cieľom zabezpečiť svoj digitálny jednotný trh, a najmä chrániť kritické siete a informačné systémy a poskytovať kľúčové služby v oblasti kybernetickej bezpečnosti. Únia musí byť schopná autonómne zabezpečiť svoje digitálne aktíva a konkurovať na globálnom trhu kybernetickej bezpečnosti.

V súčasnosti je Únia čistým dovozcom produktov a riešení v oblasti kybernetickej bezpečnosti a vo veľkej miere závisí od mimoeurópskych poskytovateľov[4]. Trh kybernetickej bezpečnosti dosahuje celkovo 600 miliárd EUR, pričom sa očakáva, že v najbližších piatich rokoch vzrastie z hľadiska tržieb, počtu firiem a pracovných miest v priemere približne o 17 %. Medzi 20 poprednými krajinami v oblasti kybernetickej bezpečnosti je však z hľadiska trhu len 6 členských štátov[5].

---

1 SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE: Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor, JOIN(2013) 1 final.

2 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

3 SPOLOČNÉ OZNÁMENIE EURÓPSKEMU PARLAMENTU A RADE „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ“, JOIN(2017) 450 final.

4 Návrh záverečnej správy o štúdii trhu kybernetickej bezpečnosti, 2018.

5 Návrh záverečnej správy o štúdii trhu kybernetickej bezpečnosti, 2018.

V Únii zároveň existuje množstvo odborných znalostí a skúseností z kybernetickej bezpečnosti – v nedávnom mapovaní centier odborných znalostí v oblasti kybernetickej bezpečnosti, ktoré uskutočnila Komisia[6], sa prihlásilo viac než 660 organizácií z celej EÚ. Ak sa tieto odborné znalosti zmenia na predajné produkty a riešenia, mohli by Únii umožniť pokryť celý hodnotový reťazec kybernetickej bezpečnosti. Úsilie výskumnej obce a odvetvia je však roztrieštené, chýba mu zosúladenie a spoločná misia, čo brzdí konkurencieschopnosť EÚ v tejto oblasti, ako aj jej schopnosť zabezpečiť si digitálne aktíva. Sektory relevantné z hľadiska kybernetickej bezpečnosti (napr. energetika, vesmír, obrana, doprava) a čiastkové oblasti sa v súčasnosti nepodporujú dostatočne[7]. Synergie medzi sektormi civilnej a obrannej kybernetickej bezpečnosti sa v Európe takisto nevyužívajú v plnej miere.

Vytvorenie verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti v Únii v roku 2016 bolo výrazným prvým krokom k spájaniu komunít výskumu, priemyslu a verejného sektora s cieľom uľahčiť výskum a inovácie v oblasti kybernetickej bezpečnosti, a v medziach finančného rámca na roky 2014 – 2020 by malo viesť k dobrým, cielenejším výsledkom vo výskume a inováciách. Toto verejno-súkromné partnerstvo umožnilo partnerom z odvetvia vyjadriť svoje záväzky týkajúce sa jednotlivých výdavkov na oblasti vymedzené v strategickom výskumnom a inovačnom programe partnerstva.

Únia však môže presadzovať oveľa väčšie investície a potrebuje účinnejší mechanizmus, ktorým by sa budovali trvalé kapacity, spojilo úsilie, kompetencie a stimuloval vývoj inovačných riešení v reakcii na kyberneticko-bezpečnostné problémy priemyslu v oblasti nových viacúčelových technológií (napr. umelá inteligencia, kvantová výpočtová technika, blockchain a zabezpečená digitálna identita), ako aj v kritických odvetviach (napr. doprava, energetika, zdravotníctvo, financie, verejná správa, telekomunikácie, výroba, obrana, vesmír).

V spoločnom oznámení sa zvažovala možnosť posilnenia spôsobilostí Únie v oblasti kybernetickej bezpečnosti prostredníctvom siete kompetenčných centier kybernetickej bezpečnosti s Európskym centrom kompetencií pre kybernetickú bezpečnosť ako ústredným aktérom. Jeho cieľom je doplniť existujúce úsilie v oblasti budovania kapacít v tejto oblasti na úrovni Únie a na národnej úrovni. V spoločnom oznámení Komisia vyjadrila zámer začať v roku 2018 posúdenie vplyvu, aby preskúmala dostupné možnosti s cieľom vytvoriť štruktúru. Ako prvý krok a vstup pre ďalšie úvahy Komisia začala pilotnú fázu v rámci programu Horizont 2020 s cieľom pomôcť spojiť národné centrá do siete, aby sa vytvoril nový impulz pre rozvoj kompetencií a technológií v oblasti kybernetickej bezpečnosti.

Hlavy štátov a predsedovia vlád na digitálnom samite v Talline v septembri 2017 vyzvali Úniu, aby sa do roku 2025 stala „globálnym lídrom v oblasti kybernetickej bezpečnosti s cieľom zabezpečiť dôveru, spoľahlivosť a ochranu našich občanov, spotrebiteľov a podnikov online a umožniť bezplatný a zákonný internet."

V záveroch Rady[8] prijatých v novembri 2017 sa Komisia vyzýva, aby urýchlene poskytla posúdenie vplyvu realistických možností a do polovice roka 2018 navrhla príslušný právny nástroj na vykonávanie tejto iniciatívy.

---

6 Technické správy Spoločného výskumného centra: Európske centrá odborných znalostí v oblasti kybernetickej bezpečnosti, 2018.

7 Technická správa Spoločného výskumného centra: Výsledky mapovania (podrobnosti pozri v prílohách 4 a 5).

8 Závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ, ktoré prijala Rada pre všeobecné záležitosti 20. novembra 2017.

Cieľom *programu Digitálna Európa, ktorý Komisia navrhla v júni 2018*[9], je rozšíriť a maximalizovať prínosy digitálnej transformácie pre európskych občanov a podniky vo všetkých príslušných oblastiach politiky EÚ, pričom sa posilnia politiky a podporia ambície digitálneho jednotného trhu. V programe sa navrhuje koherentný a prierezový prístup k zaisteniu optimálneho využitia vyspelých technológií a správnej kombinácie technických kapacít a ľudských kompetencií pri digitálnej transformácii – nielen v oblasti kybernetickej bezpečnosti, ale aj pokiaľ ide o inteligentnú dátovú infraštruktúru, umelú inteligenciu, pokročilé zručnosti a aplikácie v priemysle a v oblastiach verejného záujmu. Tieto prvky sú vzájomne závislé, synergické a ak sa podporia súbežne, môžu dosiahnuť rozsah potrebný pre úspech dátového hospodárstva[10]. Aj v *programe Európsky horizont*[11] – nasledujúcom rámcovom programe EÚ pre výskum a inováciu – je kybernetická bezpečnosť zaradená medzi priority.

V danom kontexte sa v tomto nariadení navrhuje zriadenie Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti so sieťou národných koordinačných centier. tento účelový model spolupráce by mal v záujme stimulácie európskeho technologického a odvetvového ekosystému kybernetickej bezpečnosti fungovať takto: Kompetenčné centrum bude podporovať a pomáhať koordinovať prácu siete a „živiť“ komunitu kyberneticko-bezpečnostných kompetencií, pričom bude stáť na čele technologického programu v tejto oblasti a uľahčovať prístup k takto získaným odborným poznatkom. Kompetenčné centrum to bude dosahovať predovšetkým implementáciou relevantných častí programov Digitálna Európa a Európsky horizont – udeľovaním grantov a vykonávaním obstarávaní. Vzhľadom na značné investície do kybernetickej bezpečnosti v iných častiach sveta a na potrebu koordinovať a zlučovať relevantné zdroje v Európe sa kompetenčné centrum navrhuje ako európske partnerstvo[12], ktoré umožní spoločné investície Únie, členských štátov a/alebo príslušného odvetvia. Návrh si preto od členských štátov vyžaduje úmerný príspevok na akcie kompetenčného centra a siete. Hlavným rozhodovacím orgánom je správna rada, v ktorej budú zastúpené všetky členské štáty, no hlasovacie práva budú mať len tie, ktoré finančne prispievajú. Hlasovací mechanizmus v správnej rade sa riadi zásadou dvojitej väčšiny, čo znamená, že sa vyžaduje zastúpenie 75 % finančného príspevku a 75 % hlasov. Vzhľadom na svoju zodpovednosť za rozpočet Únie má Komisia 50 % hlasovacích práv. Pri svojej práci v správnej rade bude Komisia vždy, keď to uzná za vhodné, využívať odborné znalosti Európskej služby pre vonkajšiu činnosť Správnej rade pomáha odvetvová a vedecká poradná rada s cieľom zabezpečiť pravidelný dialóg so súkromným sektorom, spotrebiteľskými organizáciami a inými príslušnými zainteresovanými stranami.

Hlavným vykonávacím orgánom pre finančné zdroje EÚ vyhradené na kybernetickú bezpečnosť v rámci navrhovaného *programu Digitálna Európa* a *programu Európsky horizont* by bolo Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti, v úzkej spolupráci so sieťou národných koordinačných centier a komunitou kyberneticko-bezpečnostných kompetencií (zahŕňajúcou

---

9 COM(2018) 434, návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027.

10 Pozri dokument SWD(2018) 305.

11 COM(2018) 435, návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje Európsky horizont – rámcový program pre výskum a inovácie a ktorým sa stanovujú jeho pravidlá účasti a šírenia.

12 Vymedzené v dokumente COM(2018) 435, návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje Európsky horizont – rámcový program pre výskum a inovácie a ktorým sa stanovujú jeho pravidlá účasti a šírenia; a uvedené v dokumente COM(2018) 434, návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovuje program Digitálna Európa na obdobie 2021 – 2027.

veľkú a rozmanitú skupinu aktérov zapojených do vývoja technológií kybernetickej bezpečnosti, ako sú výskumné subjekty, dodávateľské a odberateľské odvetvia, ale aj verejný sektor).

Takýto komplexný prístup by umožnil podporovanie kybernetickej bezpečnosti v celom hodnotovom reťazci od výskumu až po podporu zavádzania a využívania kľúčových technológií. Finančná účasť členských štátov by mala zodpovedať finančnému príspevku EÚ na túto iniciatívu a je nevyhnutným prvkom jej úspechu.

Vzhľadom na svoje špecifické odborné znalosti a široké a relevantné zastúpenie zainteresovaných strán by mala byť k práci centra a siete prizvaná prispieť aj Európska organizácia kybernetickej bezpečnosti, ktorá je partnerom Komisie v zmluvnom verejno-súkromnom partnerstve v oblasti kybernetickej bezpečnosti v rámci programu Horizont 2020.

Okrem toho by sa Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti malo tiež usilovať o posilnenie synergií medzi civilným a obranným rozmerom kybernetickej bezpečnosti. Malo by podporovať členské štáty a ďalších relevantných aktérov tým, že bude poskytovať poradenstvo, šíriť odborné znalosti a uľahčovať spoluprácu na projektoch a akciách. Na žiadosť členských štátov by mohlo pôsobiť aj ako projektový manažér, najmä pokiaľ ide o Európsky obranný fond. Snahou tejto iniciatívy je prispieť k riešeniu týchto problémov:

- **Nedostatočná spolupráca medzi odvetviami s dopytom po kybernetickej bezpečnosti a dodávateľskými odvetviami.** Európske podniky čelia výzve súčasne si zachovať bezpečnosť a ponúkať zabezpečené produkty a služby svojim klientom. Často však nedokážu primerane zabezpečiť svoje existujúce produkty, služby a aktíva alebo navrhnúť bezpečné inovačné produkty a služby. Kľúčové aktíva v oblasti kybernetickej bezpečnosti sú často príliš nákladné na to, aby ich vyvinuli a zaviedli jednotlivé subjekty, ktorých hlavná obchodná činnosť nesúvisí s kybernetickou bezpečnosťou. Prepojenia medzi dopytom a ponukou na trhu kybernetickej bezpečnosti nie sú zároveň dostatočne rozvinuté, čo vedie k horšej ponuke európskych produktov a riešení prispôsobených potrebám rôznych odvetví, ako aj k nedostatočnej miere dôvery medzi účastníkmi trhu.
- **Absencia účinného mechanizmu spolupráce medzi členskými štátmi v oblasti budovania odvetvových kapacít.** V súčasnosti pre členské štáty neexistuje žiadny efektívny mechanizmus spolupráce s cieľom vybudovať potrebné spôsobilosti na podporu inovácií v oblasti kybernetickej bezpečnosti vo všetkých priemyselných odvetviach a zavádzania prelomových európskych riešení v oblasti kybernetickej bezpečnosti. Existujúce mechanizmy spolupráce členských štátov v oblasti kybernetickej bezpečnosti podľa smernice (EÚ) 2016/1148 nemajú v rámci svojho mandátu tento typ činností.
- **Nedostatočná spolupráca v rámci výskumných a priemyselných komunít a medzi nimi.** Napriek teoretickej kapacite Európy pokryť celý hodnotový reťazec kybernetickej bezpečnosti existujú odvetvia (napr. energetika, vesmír, obrana, doprava) a subdomény, pre ktoré je kybernetická bezpečnosť relevantná a ktoré výskumná obec buď podporuje slabo alebo majú podporu len z obmedzeného počtu centier (napr. postkvantová a kvantová kryptografia, dôveryhodnosť a kybernetická bezpečnosť v kontexte umelej inteligencie). Hoci táto spolupráca zjavne existuje, je to veľmi často krátkodobá dohoda konzultačného druhu, ktorá neumožňuje zapojiť sa do dlhodobých výskumných plánov na riešenie odvetvových výziev v oblasti kybernetickej bezpečnosti.
- **Nedostatočná spolupráca medzi výskumnými a inovačnými komunitami v oblasti kybernetickej bezpečnosti civilného a obranného sektora.** Problém nedostatočnej

úrovne spolupráce sa týka aj civilných a obranných komunít. Existujúce synergie sa nevyužívajú naplno pre absenciu efektívnych mechanizmov, ktoré by týmto komunitám umožnili efektívne spolupracovať a budovať dôveru, ktorá je tu podmienkou úspešnej spolupráce ešte väčšmi než v iných doménach. Je to spojené s obmedzenými finančnými kapacitami na trhu kybernetickej bezpečnosti v EÚ vrátane nedostatočných prostriedkov na podporu inovácie.

- **Súlad s existujúcimi ustanoveniami v tejto oblasti politiky**

Kompetenčná sieť kybernetickej bezpečnosti a Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti budú pôsobiť ako dodatočná podpora existujúcich politických ustanovení a aktérov na poli kybernetickej bezpečnosti. Mandát Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti bude dopĺňať úsilie agentúry ENISA, ale má iné zameranie a vyžaduje si odlišný súbor zručností. Hoci mandát agentúry ENISA predpokladá poradenstvo v oblasti kyberneticko-bezpečnostného výskumu a inovácie v EÚ, navrhovaný mandát sa v prvom rade zameriava na iné úlohy, ktoré sú rozhodujúce pre posilnenie odolnosti kybernetickej bezpečnosti v EÚ. Okrem toho sa v mandáte agentúry ENISA neuvažuje s druhmi činností, ktoré by boli hlavnými úlohami centra a siete – stimulovať rozvoj a zavádzanie technológií v oblasti kybernetickej bezpečnosti a dopĺňať úsilie o budovanie kapacít v tejto oblasti na úrovni EÚ a na vnútroštátnej úrovni.

Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti spolu s kompetenčnou sieťou kybernetickej bezpečnosti bude takisto pracovať na podpore výskumu s cieľom uľahčiť a urýchliť procesy normalizácie a certifikácie, najmä v oblasti systémov certifikácie kybernetickej bezpečnosti v zmysle navrhovaného aktu o kybernetickej bezpečnosti[13][14].

Táto iniciatíva je *de facto* rozšírením verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti (cPPP), ktoré bolo prvým celoeurópskym pokusom spojiť odvetvie kybernetickej bezpečnosti, stranu dopytu (nákupcov kyberneticko-bezpečnostných produktov a riešení vrátane verejnej správy a kľúčových sektorov, napr. dopravy, zdravotníctva, energetiky, financií) a výskumnej obce s cieľom vybudovať platformu udržateľného dialógu a vytvoriť podmienky pre dobrovoľné spoluinvestovanie. Zmluvné verejno-súkromné partnerstvo vzniklo v roku 2016 a do roku 2020 povedie k investíciám vo výške až 1,8 miliardy EUR. Rozsah investícií, ktoré prebiehajú v iných častiach sveta (napr. Spojené štáty len v roku 2017 investovali 19 miliárd dolárov do kybernetickej bezpečnosti) však svedčí o tom, že EÚ musí urobiť viac pre dosiahnutie kritického objemu investícií a prekonanie fragmentácie kapacít v rámci EÚ.

- **Súlad s ostatnými politikami Únie**

---

13 Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií [„akt o kybernetickej bezpečnosti“, COM(2017) 477 final/3].

14 Tým nie sú dotknuté mechanizmy osvedčovania podľa všeobecného nariadenia o ochrane údajov, v ktorých musia zohrávať úlohu orgány na ochranu údajov v súlade s nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti bude pôsobiť ako spoločný implementačný orgán pre viaceré programy Únie na podporu kybernetickej bezpečnosti (program Digitálna Európa a program Európsky horizont) a posilnenie koherentnosti a synergií medzi nimi.

Táto iniciatíva takisto umožní doplniť úsilie členských štátov, a to vhodnými vstupmi pre tvorcov politík v oblasti vzdelávania s cieľom posilniť kyberneticko-bezpečnostné zručnosti (napr. vypracovaním učebných osnov v oblasti kybernetickej bezpečnosti v civilných a vojenských vzdelávacích systémoch), aby sa v tejto sfére v EÚ podporila tvorba kvalifikovanej pracovnej sily, ktorá je kľúčovým aktívom pre firmy, ako aj iné odvetvia angažované v kybernetickej bezpečnosti. Pokiaľ ide o vzdelávanie a odbornú prípravu v oblasti kybernetickej obrany, táto iniciatíva bude v súlade s prebiehajúcimi prácami na platforme vzdelávania, odbornej prípravy a cvičení v oblasti kybernetickej obrany v rámci Európskej akadémie bezpečnosti a obrany.

Táto iniciatíva bude dopĺňať a podporovať úsilie centier digitálnych inovácií v rámci programu Digitálna Európa. Centrá digitálnych inovácií sú neziskové organizácie, ktoré pomáhajú spoločnostiam, najmä startupom, MSP a podnikom so strednou kapitalizáciou zvýšiť konkurencieschopnosť zlepšovaním obchodných/výrobných procesov, ako aj produktov a služieb prostredníctvom inteligentných inovácií umožnených digitálnymi technológiami. Centrá digitálnych inovácií poskytujú podnikové a inovačné služby ako získavanie informácií o trhu, finančné poradenstvo, prístup k príslušným skúšobným a experimentačným zariadeniam, odborná príprava a rozvoj zručností s cieľom pomôcť úspešnému uvedeniu nových produktov alebo služieb na trh alebo zaviesť lepšie výrobné procesy. Niektoré centrá digitálnych inovácií so špecifickými odbornými znalosťami v oblasti kybernetickej bezpečnosti by mohli byť priamo zapojené do kyberneticko-bezpečnostnej kompetenčnej komunity zriadenej touto iniciatívou. Vo väčšine prípadov by však centrá digitálnych inovácií, ktoré nemajú špecifický profil kybernetickej bezpečnosti, uľahčili vo svojich kruhoch prístup ku kyberneticko-bezpečnostnej expertíze, znalostiam a kapacitám, ktoré má komunita k dispozícii, a to úzkou spoluprácou so sieťou národných koordinačných centier a s Európskym centrom odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti. Centrá digitálnych inovácií by tiež podporili zavádzanie inovačných kyberneticko-bezpečnostných produktov a riešení, ktoré zodpovedajú potrebám spoločností a iných koncových používateľov, ktorým poskytujú služby. V neposlednom rade môžu centrá digitálnych inovácií v jednotlivých odvetviach sieti a centru poskytnúť svoje poznatky o skutočných odvetvových potrebách ako vstup pre formovanie programu výskumu a inovácií v reakcii na odvetvové požiadavky.

Budú sa hľadať synergie s príslušnými znalostnými a inovačnými spoločenstvami Európskeho inovačného a technologického inštitútu, najmä s EIT Digital.

2. PRÁVNY ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právny základ

Kompetenčné centrum by sa malo zriadiť na dvojitom právnom základe z dôvodu jeho povahy a osobitných cieľov. Článkom 187 ZFEÚ, v ktorom sa stanovujú štruktúry potrebné na účinné vykonávanie programov Únie v oblasti výskumu, technologického rozvoja a pilotných programov, sa umožňuje, aby kompetenčné centrum vytváralo synergie a spájalo zdroje na investovanie do potrebných kapacít na úrovni členských štátov a na rozvoj európskych spoločných aktív (napr. spoločným obstarávaním potrebnej kyberneticko-bezpečnostnej skúšobnej a experimentačnej infraštruktúry). V prvom odseku článku 188 sa

stanovuje prijatie takýchto opatrení. Napriek tomu by prvý pododsek článku 188 ako jediný právny základ neumožnil, aby činnosti podľa potreby siahali nad rámec oblasti výskumu a vývoja, aby sa splnili všetky ciele kompetenčného centra stanovené v tomto nariadení na podporu trhového zavádzania kyberneticko-bezpečnostných produktov a riešení, pomoc európskemu odvetviu kybernetickej bezpečnosti stať sa konkurencieschopnejším a zvýšiť podiel na trhu pridať hodnotu k vnútroštátnemu úsiliu o riešenie problému nedostatku zručností v oblasti kybernetickej bezpečnosti. Preto na dosiahnutie týchto cieľov treba ako právny základ doplniť článok 173 ods. 3, ktorý Únii umožní stanoviť opatrenia na podporu konkurencieschopnosti odvetvia.

- **Odôvodnenie návrhu z hľadiska zásady subsidiarity a proporcionality**

Kybernetická bezpečnosť je otázkou spoločného záujmu Únie, ako sa potvrdzuje vo vyššie uvedených záveroch Rady. Dokazuje to aj rozsah a cezhraničný charakter incidentov ako *WannaCry* alebo *NonPetya*. Povaha a rozsah technologických výziev v oblasti kybernetickej bezpečnosti, ako aj nedostatočná koordinácia úsilia v rámci odvetvia, verejného sektora a výskumných komunít a medzi nimi si vyžadujú, aby EÚ ďalej podporovala úsilie o koordináciu s cieľom zhromaždiť kritické množstvo zdrojov a zabezpečiť lepšiu správu znalostí a aktív. Je to potrebné vzhľadom na požiadavky na zdroje pri určitých spôsobilostiach pre výskum, vývoj a zavádzanie v oblasti kybernetickej bezpečnosti; potrebu zabezpečiť prístup k interdisciplinárnemu know-how v oblasti kybernetickej bezpečnosti (ten je na vnútroštátnej úrovni často dostupný len čiastočne); globálny charakter odvetvových hodnotových reťazcov, ako aj činnosť svetových konkurentov pracujúcich na rôznych trhoch.

To si vyžaduje zdroje a odborné znalosti v rozsahu, ktorý sotva zodpovedá jednotlivým opatreniam ktoréhokoľvek členského štátu. Napríklad celoeurópska kvantová komunikačná sieť by mohla vyžadovať investície EÚ vo výške približne 900 miliónov EUR v závislosti od investícií členských štátov (ktoré sa majú prepojiť/doplniť) a od toho, do akej miery táto technológia umožní využitie existujúcich infraštruktúr. Táto iniciatíva bude nástrojom na združovanie finančných prostriedkov a umožní, aby v Únii došlo k tomuto druhu investícií.

Ciele tejto iniciatívy nemôžu v plnej miere dosiahnuť samotné členské štáty. Ako sa uvádza vyššie, dajú sa lepšie dosiahnuť na úrovni Únie spojením úsilia a zamedzením zbytočnej duplicity, podporou dosahovania kritického objemu investícií a zabezpečením optimálneho využitia verejného financovania. V súlade so zásadou proporcionality toto nariadenie zároveň neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa. Opatrenia na úrovni EÚ sú preto opodstatnené z hľadiska zásady subsidiarity a proporcionality.

V tomto nástroji sa nestanovujú žiadne nové regulačné povinnosti pre podniky. Podniky, a najmä MSP, si zároveň pravdepodobne znížia náklady súvisiace s ich úsilím o navrhovanie inovačných kyberneticky bezpečných produktov, keďže táto iniciatíva umožňuje združovať zdroje na investovanie do potrebných kapacít na úrovni členských štátov alebo na rozvoj spoločných európskych aktív (napr. spoločným obstarávaním potrebnej skúšobnej a experimentačnej kyberneticko-bezpečnostnej infraštruktúry). Tieto aktíva by mohli využívať priemyselné odvetvia a malé a stredné podniky v rôznych odvetviach na zaistenie kybernetickej bezpečnosti svojich produktov, pričom sa z nej stane ich konkurenčná výhoda.

- **Výber nástroja**

Navrhovaným nástrojom sa zriaďuje orgán zameraný na implementáciu akcií v oblasti kybernetickej bezpečnosti v rámci programov Digitálna Európa a Európsky horizont. Vymedzuje jeho mandát, úlohy, ako aj štruktúru riadenia. Zriadenie takéhoto orgánu Únie si vyžaduje prijatie nariadenia.

3. KONZULTÁCIE SO ZAINTERESOVANÝMI STRANAMI A POSÚDENIA VPLYVU

Návrh na vytvorenie kompetenčnej siete v oblasti kybernetickej bezpečnosti s Európskym centrom odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti je nová iniciatíva. Ide o pokračovanie a rozšírenie zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti vytvoreného v roku 2016.

- **Konzultácie so zainteresovanými stranami**

Kybernetická bezpečnosť je širokou medzisektorovou témou. Komisia použila rôzne konzultačné metódy s cieľom zabezpečiť, aby sa v tejto iniciatíve riadne zohľadnil všeobecný verejný záujem Únie – oproti osobitným záujmom úzkych skupín zainteresovaných strán. Touto metódou sa zabezpečuje transparentnosť a zodpovednosť pri práci Komisie. Hoci sa pre túto iniciatívu osobitne neuskutočnila žiadna otvorená verejná konzultácia vzhľadom na cieľovú skupinu (odvetvová a výskumná komunita a členské štáty), na túto tematickú oblasť sa už zamerali viaceré iné otvorené verejné konzultácie:

- Všeobecná otvorená verejná konzultácia, ktorá sa uskutočnila v roku 2018 na tému investície, výskum a inovácie, MSP a jednotný trh.
- V roku 2017 sa začala 12-týždňová online verejná konzultácia s cieľom získať názory širokej verejnosti (približne 90 respondentov) na hodnotenie a preskúmanie agentúry ENISA.
- V roku 2016 sa uskutočnila 12-týždňová online verejná konzultácia pri príležitosti začatia zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti (približne 240 respondentov).

Komisia zorganizovala aj cielené konzultácie o tejto iniciatíve vrátane seminárov, stretnutí a cielených žiadostí o informácie (od agentúry ENISA a Európskej obrannej agentúry). Konzultačné obdobie, ktoré sa začalo v novembri 2017 a skončilo v marci 2018, trvalo 6 mesiacov. Komisia tiež zmapovala centrá odborných znalostí, čo umožnilo zhromaždiť vstupy od 665 odborných centier kybernetickej bezpečnosti, pokiaľ ide o ich know-how, činnosť, pracovné oblasti, medzinárodnú spoluprácu. Prieskum sa začal v januári a pri analýze sa zohľadnili podnety predložené do 8. marca 2018.

Zainteresované strany z odvetvových a výskumných komunít sa domnievajú, že kompetenčné centrum a sieť by mohli podporiť súčasné úsilie členských štátov prostredníctvom pomoci pri vytváraní celoeurópskeho ekosystému kybernetickej bezpečnosti, ktorý by umožnil lepšiu spoluprácu medzi výskumnými a priemyselnými komunitami. Takisto sa domnievajú, že je potrebné, aby EÚ a členské štáty zaujali proaktívny, dlhodobý a strategický postoj k odvetvovej politike kybernetickej bezpečnosti, ktorá presahuje rámec výskumu a inovácií. Zainteresované strany vyjadrili potrebu získať prístup k hlavným spôsobilostiam, ako sú napríklad skúšobné a experimentačné zariadenia, a zvýšiť ambície pri riešení nedostatku zručností v oblasti kybernetickej bezpečnosti, napr. rozsiahlymi európskymi projektmi, ktoré prilákajú najlepšie talenty. Všetky uvedené aspekty sa zároveň považovali za nevyhnutné na to, aby Únia bola svetovo uznaná za lídra v oblasti kybernetickej bezpečnosti.

Členské štáty v rámci konzultačných činností, ktoré sa uskutočnili od septembra[15], ako aj v osobitných záveroch Rady[16] privítali zámer vytvoriť kompetenčnú sieť kybernetickej

[15] Napr. okrúhly stôl na vysokej úrovni s členskými štátmi, podpredsedom Komisie Ansipom, komisárkou Gabrielovou, 5. decembra 2017.

bezpečnosti s cieľom stimulovať vývoj a zavádzanie kyberneticko-bezpečnostných technológií, pričom zdôraznili potrebu ich začlenenia do všetkých členských štátov a ich existujúcich centier excelentnosti a kompetencií s osobitnou pozornosťou venovanou komplementárnosti. Konkrétne pokiaľ ide o budúce kompetenčné centrum, členské štáty zdôraznili význam ich koordinačnej úlohy pri podpore siete. Najmä v súvislosti s vnútroštátnymi činnosťami a potrebami v oblasti kybernetickej obrany sa mapovaním potrieb členských štátov v tejto oblasti, ktoré uskutočnila Európska služba pre vonkajšiu činnosť v marci 2018, preukázalo, že väčšina členských štátov vníma pridanú hodnotu podpory EÚ vo vzdelávaní a odbornej príprave v oblasti kybernetickej obrany, ako aj v podpore priemyslu prostredníctvom výskumu a vývoja[17]. Iniciatíva by sa skutočne realizovala spolu s členskými štátmi alebo nimi podporovanými subjektmi. Spolupráca medzi komunitami odvetvia, výskumu a/alebo verejného sektora by umožnila spojiť a posilniť existujúce subjekty a úsilie, aby nevznikli nové. Členské štáty by sa takisto podieľali na vymedzení osobitných akcií zameraných na verejný sektor ako priameho používateľa kyberneticko-bezpečnostných technológií a know-how.

- **Posúdenie vplyvu**

Posúdenie vplyvu tejto iniciatívy bolo predložené výboru pre kontrolu regulácie 11. apríla 2017 a výbor k nemu vydal kladné stanovisko s výhradami. Posúdenie vplyvu bolo následne preskúmané na základe pripomienok výboru. Stanovisko výboru a príloha, v ktorej sa vysvetľuje, ako sa pripomienky výboru zohľadnili, sa uverejňujú spolu s týmto návrhom.

V posúdení vplyvu sa zohľadnilo niekoľko možností politiky, a to tak legislatívnych, ako aj nelegislatívnych. Na účely dôkladného posúdenia sa ponechali tieto možnosti:

- Základný scenár – možnosť spolupráce – predpokladá sa pokračovanie súčasného prístupu k budovaniu odvetvových a technologických kapacít v oblasti kybernetickej bezpečnosti v EÚ podporou výskumu a inovácie a súvisiacich mechanizmov spolupráce podľa deviateho rámcového programu.
- Možnosť 1: Kompetenčná sieť kybernetickej bezpečnosti s Európskym centrom odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti s dvojitým mandátom na vykonávanie opatrení na podporu priemyselných technológií, ako aj v oblasti výskumu a inovácie.
- Možnosť 2: Kompetenčná sieť kybernetickej bezpečnosti s Európskym výskumným a kompetenčným centrom kybernetickej bezpečnosti zameraná na výskumné a inovačné činnosti.

Možnosti vyradené v počiatočnej fáze zahŕňali 1) neprijať vôbec žiadne opatrenia, 2) možnosť vytvoriť iba kompetenčnú sieť kybernetickej bezpečnosti, 3) možnosť vytvoriť iba centralizovanú štruktúru, ako aj 4) možnosť využiť existujúcu agentúru [Agentúru Európskej únie pre sieťovú a informačnú bezpečnosť – (ENISA), Výkonnú agentúru pre výskum (REA) alebo Výkonnú agentúru pre inovácie a siete (INEA)].

V analýze sa dospelo k záveru, že možnosť 1 je najvhodnejšia na dosiahnutie cieľov iniciatívy, pričom ponúka najvyšší ekonomický, spoločenský a environmentálny vplyv a chráni záujmy Únie. Hlavné argumenty v prospech tejto možnosti zahŕňali schopnosť

---

16 Rada pre všeobecné záležitosti: Závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ (20. novembra 2017).

17 ESVČ, marec 2018.

vybudovať skutočnú kyberneticko-bezpečnostnú odvetvovú politiku podporou činností, ktoré sa netýkajú len výskumu a vývoja, ale aj zavedenia na trh; flexibilitu na umožnenie rôznych modelov spolupráce so sieťou kompetenčných centier s cieľom optimalizovať využívanie existujúcich poznatkov a zdrojov; schopnosť štruktúrovať spoluprácu a spoločné záväzky verejných a súkromných zainteresovaných strán pochádzajúcich zo všetkých relevantných sektorov vrátane obrany. V neposlednom rade umožňuje možnosť 1 aj posilnenie synergií a môže fungovať ako implementačný mechanizmus v prípade dvoch rôznych zdrojov financovania kybernetickej bezpečnosti v EÚ v kontexte budúceho viacročného finančného rámca (programy Digitálna Európa a Európsky horizont).

- **Základné práva**

Táto iniciatíva umožní verejným orgánom a priemyselným odvetviam v jednotlivých členských štátoch účinnejšie predchádzať kybernetickým hrozbám a reagovať na ne, keďže im ponúkne a pomôže zaviesť bezpečnejšie produkty a riešenia. Týka sa to najmä ochrany prístupu k základným službám (napr. doprava, zdravotníctvo, bankovníctvo a finančné služby).

Zvýšená kapacita Európskej únie autonómne zabezpečiť svoje produkty a služby zároveň pravdepodobne pomôže občanom využívať ich demokratické práva a hodnoty (napr. lepšie chrániť ich informačné práva zakotvené v Charte základných práv, najmä právo na ochranu osobných údajov a súkromný život) a následne zvýšiť ich dôveru v digitálnu spoločnosť a hospodárstvo.

4. VPLYV NA ROZPOČET

Hlavným vykonávacím orgánom finančných zdrojov EÚ vyhradených na kybernetickú bezpečnosť v rámci programov Digitálna Európa a Európsky horizont bude Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti v spolupráci s kompetenčnou sieťou kybernetickej bezpečnosti.

Vplyv na rozpočet, pokiaľ ide o implementáciu programu Digitálna Európa, je podrobne uvedený v legislatívnom finančnom výkaze, ktorý je prílohou k tomuto návrhu. Príspevok z finančného krytia klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 21 ods. 1 písm. b) navrhne Komisia počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody. Návrh bude vychádzať z výsledkov procesu strategického plánovania vymedzeného v článku 6 ods. 6 nariadenia XXX [rámcový program Európsky horizont].

5. ĎALŠIE PRVKY

- **Plány vykonávania, spôsob monitorovania, hodnotenia a podávania správ**

Návrh obsahuje explicitnú doložku o hodnotení, podľa ktorej Komisia vykoná nezávislé hodnotenie (článok 38). Komisia následne predloží Európskemu parlamentu a Rade hodnotiacu správu, ku ktorej v prípade potreby priloží návrh na preskúmanie s cieľom zmerať vplyv nástroja a jeho pridanú hodnotu. Pri hodnotení sa uplatní metodika lepšej právnej regulácie Komisie.

Výkonný riaditeľ by mal predkladať správnej rade ex post hodnotenie činností Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a činností siete každé dva roky, ako sa stanovuje v článku 17 tohto návrhu.

Výkonný riaditeľ by mal pripraviť aj nadväzujúci akčný plán týkajúci sa záverov retrospektívnych hodnotení a každé dva roky podávať správu o pokroku Komisii. Správna rada by mala byť zodpovedná za monitorovanie primeraných krokov nadväzujúcich na tieto závery, ako sa uvádza v článku 16 tohto návrhu.

Podozrenia na nesprávne riadenie činností tohto právneho subjektu môžu byť predmetom skúmania zo strany európskeho ombudsmana v súlade s ustanoveniami článku 228 zmluvy.

2018/0328 (COD)

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY,

ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier

Príspevok Európskej komisie k zasadnutiu lídrov v Salzburgu v dňoch 19. – 20. septembra 2018

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 173 ods. 3 a článok 188 prvý odsek,

so zreteľom na návrh Európskej komisie,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[18],

so zreteľom na stanovisko Výboru regiónov[19],

konajúc v súlade s riadnym legislatívnym postupom,

keďže:

(1) Náš každodenný život a hospodárstva sú čoraz závislejšie od digitálnych technológií a občania sú čoraz viac vystavovaní vážnym kybernetickým incidentom. Budúca bezpečnosť závisí okrem iného od zlepšenia schopnosti technológií a príslušného odvetvia chrániť Úniu pred kybernetickými hrozbami, keďže civilná infraštruktúra i vojenské spôsobilosti si vyžadujú bezpečné digitálne systémy.

(2) Únia v nadväznosti na kyberneticko-bezpečnostnú stratégiu z roku 2013[20], ktorej cieľom je spoľahlivý, bezpečný a otvorený kybernetický ekosystém, vytrvalo posilňuje svoju činnosť pri riešení narastajúcich výziev v oblasti kybernetickej bezpečnosti. V roku 2016 Únia prijala v oblasti kybernetickej bezpečnosti prvé opatrenia v podobe smernice Európskeho parlamentu a Rady (EÚ) 2016/1148[21] o bezpečnosti sietí a informačných systémov.

---

18 Ú. v. EÚ C, s. .

19 Ú. v. EÚ C , , s. .

20 Spoločné oznámenie Európskemu parlamentu a Rade: Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor, JOIN(2013) 1 final.

21 Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

(3) V septembri 2017 Komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku predložili spoločné oznámenie[22] s názvom „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ“ na ďalšie posilnenie odolnosti Únie, odrádzanie od kybernetických útokov a reakcieschopnosť na ne.

(4) Hlavy štátov a predsedovia vlád na digitálnom samite v Tallinne v septembri 2017 vyzvali Úniu stať sa „do roku 2025 globálnym lídrom v oblasti kybernetickej bezpečnosti, a tak zabezpečiť dôveru, istotu a ochranu našich občanov, spotrebiteľov a podnikov v online prostredí a umožniť bezplatné internetové pripojenie upravené zákonom.“

(5) Výrazné narušenie sietí a informačných systémov môže ovplyvniť jednotlivé členské štáty i Úniu ako celok. Bezpečnosť sietí a informačných systémov je preto základným predpokladom hladkého fungovania vnútorného trhu. Únia sa v súčasnosti musí spoliehať na neeurópskych poskytovateľov kybernetickej bezpečnosti. Je však v jej strategickom záujme zabezpečiť, aby si zachovala a rozvíjala základné kybernetickobezpečnostné technologické kapacity na zabezpečenie svojho digitálneho jednotného trhu, a najmä na ochranu kritických sietí a informačných systémov a na poskytovanie kľúčových služieb v oblasti kybernetickej bezpečnosti.

(6) V Únii existuje množstvo expertízy a skúseností v oblasti kybernetickobezpečnostného výskumu, technológií a odvetvového vývoja, no činnosť odvetvových a výskumných komunít je fragmentovaná a chýba jej zosúladenie a spoločná misia, čo brzdí konkurencieschopnosť v tejto sfére. Tieto činnosti a odborné znalosti treba zlúčiť, prepojiť a efektívne využiť, aby sa posilnili a doplnili existujúce výskumné, technologické a odvetvové kapacity na úrovni Únie i členských štátov.

(7) Rada vo svojich záveroch z novembra 2017 vyzvala Komisiu, aby urýchlene poskytla hodnotenie vplyvu možností zriadenia siete kompetenčných centier kybernetickej bezpečnosti a Európskeho výskumného a kompetenčného centra, a aby do polovice roka 2018 navrhla príslušný právny nástroj.

(8) Kompetenčné centrum by malo byť hlavným nástrojom Únie na zlučovanie investícií do výskumu, technológií a vývoja v oblasti kybernetickej bezpečnosti a na realizáciu relevantných projektov a iniciatív spolu s kompetenčnou sieťou pre kybernetickú bezpečnosť. Malo by poskytovať finančnú podporu pre kybernetickú bezpečnosť z programov Európsky horizont a Digitálna Európa a v náležitých prípadoch by malo byť otvorené aj Európskemu fondu regionálneho rozvoja a ďalším programom. Tento prístup by mal prispieť k vytvoreniu synergií, ku koordinácii finančnej podpory v oblasti výskumu, inovácií, technológií a rozvoja odvetvia kybernetickej bezpečnosti a k predchádzaniu duplicite.

(9) Keďže ciele tejto iniciatívy možno najlepšie dosiahnuť, ak sa do nej zapoja všetky alebo aspoň čo najviac členských štátov, a ako stimul pre účasť členských štátov, mali by mať hlasovacie práva iba tie členské štáty, ktoré finančne prispievajú na krytie administratívnych a prevádzkových nákladov kompetenčného centra.

(10) Finančné zapojenie zúčastnených členských štátov by malo zodpovedať finančnému príspevku Únie na túto iniciatívu.

---

[22] Spoločné oznámenie Európskemu parlamentu a Rade – Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ, JOIN(2017) 450 final.

(11) Kompetenčné centrum by malo uľahčovať a pomáhať koordinovať prácu kompetenčnej siete kybernetickej bezpečnosti (ďalej len „sieť“) pozostávajúcu z národných koordinačných centier v každom členskom štáte. Národné koordinačné centrá by mali dostávať priamu finančnú podporu Únie vrátane grantov udeľovaných bez výzvy na predkladanie návrhov s cieľom vykonávať činnosti súvisiace s týmto nariadením.

(12) Národné koordinačné centrá by si mali vyberať členské štáty. Okrem potrebných administratívnych kapacít by tieto centrá mali buď samé disponovať alebo mať priamy prístup ku kyberneticko-bezpečnostnej technologickej expertíze, a to najmä v oblastiach ako kryptografia, bezpečnostné služby IKT, detekcia narušení, systémová bezpečnosť, sieťová bezpečnosť, bezpečnosť softvéru a aplikácií či aspekty bezpečnosti a ochrany súkromia týkajúce sa ľudí a celej spoločnosti. Zároveň by mali byť schopné efektívne sa zapájať a koordinovať svoju činnosť s príslušným odvetvím, verejným sektorom vrátane orgánov, ktoré boli na túto činnosť určené podľa smernice Európskeho parlamentu a Rady (EÚ) 2016/1148[23], a výskumnou obcou.

(13) Ak sa národným koordinačným centrám poskytuje finančná podpora pre tretie strany na vnútroštátnej úrovni, prevedie sa na príslušné zainteresované strany prostredníctvom kaskádových dohôd o grante.

(14) Nové technológie, ako napríklad umelá inteligencia, internet vecí, vysokovýkonná výpočtová technika (HPC), kvantová výpočtová technika, blockchain a koncepty ako zabezpečená digitálna identita popri riešeniach prinášajú aj nové kyberneticko-bezpečnostné výzvy. Vyhodnocovanie a validácia spoľahlivosti existujúcich alebo budúcich systémov IKT si bude vyžadovať skúšanie odolnosti bezpečnostných riešení proti útokom na HPC a kvantových strojoch. Kompetenčné centrum, sieť a komunita kyberneticko-bezpečnostných kompetencií by mali pomôcť pri vývoji a šírení najmodernejších kyberneticko-bezpečnostných riešení. Zároveň by kompetenčné centrum a sieť mali slúžiť vývojárom a prevádzkovateľom v kľúčových odvetviach ako doprava, energetika, zdravotníctvo, financie, verejná správa, telekomunikácie, výroba, obrana a vesmír, aby im pomohli riešiť otázky kybernetickej bezpečnosti.

(15) Kompetenčné centrum by malo mať niekoľko kľúčových funkcií. Po prvé by kompetenčné centrum malo podporovať a pomáhať koordinovať prácu Európskej kompetenčnej siete kybernetickej bezpečnosti a podporovať komunitu kyberneticko-bezpečnostných kompetencií. Centrum by malo viesť technologický program v oblasti kybernetickej bezpečnosti a uľahčovať prístup k odborným poznatkom, ktoré sieť a komunita zhromaždí. Po druhé, malo by implementovať príslušné časti programov Digitálna Európa a Európsky horizont prideľovaním grantov – obyčajne na základe verejnej výzvy na predkladanie návrhov. Po tretie, kompetenčné centrum by malo uľahčovať spoločné investície Únie, členských štátov a/alebo odvetvia.

(16) Kompetenčné centrum by malo stimulovať a podporovať spoluprácu a koordináciu činností komunity kyberneticko-bezpečnostných kompetencií, ktorá je veľkou, otvorenou a rôznorodou skupinou aktérov v oblasti kyberneticko-bezpečnostných technológií. Do tejto komunity by mali patriť predovšetkým výskumné subjekty, dodávateľské sektory, odberateľské sektory a verejný sektor. Komunita kyberneticko-bezpečnostných technológií by mala poskytovať vstupy pre činnosti a pracovný plán

[23] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

kompetenčného centra, a zároveň by mala môcť využívať komunitné činnosti kompetenčného centra a siete, no inak by nemala byť z hľadiska výziev na predkladanie návrhov alebo ponúk nijako privilegovaná.

(17) S cieľom reagovať na potreby dodávateľských i odberateľských sektorov by úloha kompetenčného centra poskytovať kyberneticko-bezpečnostné poznatky a technickú pomoc rôznym odvetviam mala zahŕňať tak produkty a služby IKT, ako aj všetky ďalšie odvetvové a technologické produkty a riešenia, do ktorých sa má aspekt kybernetickej bezpečnosti integrovať.

(18) Hoci kompetenčné centrum a sieť by sa mali usilovať o synergie medzi kybernetickou bezpečnosťou v civilnej a obrannej sfére, projekty financované z programu Európsky horizont sa budú implementovať v súlade s nariadením XXX [nariadenie o Európskom horizonte], podľa ktorého sa výskumné a inovačné činnosti vykonávané v rámci Európskeho horizontu zameriavajú na civilné aplikácie.

(19) V záujme štruktúrovanej a udržateľnej spolupráce by mal byť vzťah medzi kompetenčným centrom a národnými koordinačnými centrami upravený zmluvne.

(20) Vhodným spôsobom by sa mala zaručiť zodpovednosť a transparentnosť kompetenčného centra.

(21) Vzhľadom na svoje odborné poznatky v oblasti kybernetickej bezpečnosti by mali byť v komunite kyberneticko-bezpečnostných kompetencií, ako aj v odvetvovej a vedeckej poradnej rade aktívne zapojené Spoločné výskumné centrum Komisie a Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA).

(22) Ak národné koordinačné centrá a subjekty, ktoré sú súčasťou komunity kyberneticko-bezpečnostných kompetencií, dostávajú finančný príspevok zo všeobecného rozpočtu Únie, mali by propagovať skutočnosť, že príslušné činnosti sa vykonávajú v kontexte tejto iniciatívy.

(23) Z príspevku Únie na kompetenčné centrum by sa mala financovať polovica nákladov spojených so zriadením, administratívou a koordinačnými činnosťami kompetenčného centra. Aby sa predišlo dvojitému financovaniu, tieto činnosti by sa nemali súbežne podporovať z príspevkov z iných programov Únie.

(24) Správna rada kompetenčného centra zložená zo zástupcov členských štátov a Komisie by mala vymedziť všeobecné smerovanie činnosti kompetenčného centra a zabezpečiť, aby vykonávalo svoje úlohy v súlade s týmto nariadením. Správna rada by mala mať potrebné právomoci na zostavovanie rozpočtu, overovanie jeho plnenia, prijatie vhodných rozpočtových pravidiel, navrhnutie transparentných pracovných postupov rozhodovania kompetenčného centra, prijatie pracovného plánu a viacročného strategického plánu kompetenčného centra, v ktorých sa budú odrážať priority pri plnení cieľov a úloh kompetenčného centra, prijatie vlastného rokovacieho poriadku, menovanie výkonného riaditeľa a rozhodovanie o predlžovaní či ukončení jeho funkčného obdobia.

(25) Aby kompetenčné centrum mohlo fungovať riadne a efektívne, Komisia a členské štáty by mali zabezpečiť, aby osoby, ktoré majú byť vymenované za členov správnej rady, mali zodpovedajúce odborné znalosti a skúsenosti v príslušných funkčných oblastiach. Komisia a členské štáty by mali vynaložiť úsilie aj na obmedzenie obmeny svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce.

(26) Bezproblémové fungovanie kompetenčného centra si vyžaduje, aby bol jeho výkonný riaditeľ vymenovaný na základe zásluh a zdokumentovaných administratívnych a

riadiacich schopností, ako aj na základe kvalifikácie a skúseností vo sfére kybernetickej bezpečnosti, a aby vykonával svoje povinnosti úplne nezávisle.

(27) Kompetenčné centrum by malo mať odvetvovú a vedeckú poradnú radu ako poradný orgán s cieľom zabezpečiť pravidelný dialóg so súkromným sektorom, spotrebiteľskými organizáciami a inými príslušnými zainteresovanými stranami. Odvetvová a vedecká poradná rada by sa mala zameriavať na otázky relevantné pre zainteresované strany, o ktorých by mala informovať správnu radu kompetenčného centra. Zloženie odvetvovej a vedeckej poradnej rady a jej zverené úlohy, ako napríklad poskytovanie konzultácií k pracovnému plánu, by mali zaručovať dostatočné zastúpenie zainteresovaných strán v práci kompetenčného centra.

(28) Kompetenčné centrum by malo prostredníctvom odvetvovej a vedeckej poradnej rady môcť využiť konkrétne odborné znalosti, ako aj široké zastúpenie zainteresovaných strán vyplývajúce zo zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti za trvania programu Horizont 2020.

(29) Kompetenčné centrum by malo disponovať pravidlami na predchádzanie a riadenie konfliktu záujmov. Kompetenčné centrum by malo zároveň uplatňovať príslušné pravidlá Únie týkajúce sa prístupu verejnosti k dokumentom, ako sa stanovujú v nariadení Európskeho parlamentu a Rady (ES) č. 1049/2001[24]. Spracovávanie osobných údajov kompetenčným centrom podlieha nariadeniu Európskeho parlamentu a Rady (EÚ) XXX/2018. Kompetenčné centrum by malo dodržiavať ustanovenia platné pre inštitúcie Únie, ako aj vnútroštátne právne predpisy o zaobchádzaní s informáciami, najmä s citlivými neutajovanými informáciami a utajovanými skutočnosťami EÚ.

(30) Finančné záujmy Únie a členských štátov by sa mali chrániť primeranými opatreniami v celom cykle výdavkov vrátane predchádzania, odhaľovania a vyšetrovania nezrovnalostí, vymáhania stratených, neoprávnene vyplatených alebo nesprávne použitých finančných prostriedkov a prípadne uloženia správnych a finančných sankcií v súlade s nariadením Európskeho parlamentu a Rady (EÚ, Euratom) XXX[25] [nariadenie o rozpočtových pravidlách].

(31) Kompetenčné centrum by malo fungovať otvorene a transparentne, malo by včas poskytovať všetky náležité informácie a propagovať svoje činnosti, okrem iného cez informačné aktivity a šírením informácií v radoch širokej verejnosti. Rokovací poriadok orgánov kompetenčného centra by sa mal zverejniť.

(32) Vnútorný audítor Komisie by mal mať vo vzťahu ku kompetenčnému centru rovnaké právomoci, aké má vo vzťahu ku Komisii.

(33) Komisia, kompetenčné centrum, Dvor audítorov a Európsky úrad pre boj proti podvodom by mali mať prístup ku všetkým potrebným informáciám a priestorom na výkon auditov a vyšetrovanie grantov, zmlúv a dohôd, ktoré kompetenčné centrum podpísalo.

(34) Keďže ciele tohto nariadenia – zachovanie a rozvoj technologických a priemyselných kapacít EÚ v oblasti kybernetickej bezpečnosti, zvyšovanie konkurencieschopnosti odvetvia kybernetickej bezpečnosti v Únii a premenu kybernetickej bezpečnosti na

---

[24] Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

[25] [doplniť názov a odkaz na Ú. v.].

konkurenčnú výhodu iných odvetví Únie – nie je možné uspokojivo dosiahnuť na úrovni členských štátov, pretože existujúce obmedzené zdroje sú rozptýlené a sú potrebné rozsiahle investície, ale na zabránenie zbytočnej duplicite pri tomto úsilí, ako aj v záujme podpory získavania kritického objemu investícií a na zaistenie optimálneho využitia verejných prostriedkov ich možno lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie uvedeného cieľa,

PRIJALI TOTO NARIADENIE:

KAPITOLA I

VŠEOBECNÉ USTANOVENIA A ZÁSADY KOMPETENČNÉHO CENTRA A SIETE

Článok 1

Predmet úpravy

1. Týmto nariadením sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ďalej len „kompetenčné centrum“), ako aj sieť národných koordinačných centier, a stanovujú sa v ňom pravidlá nominácie národných koordinačných centier a zriadenia komunity kyberneticko-bezpečnostných kompetencií.

2. Kompetenčné centrum prispieva k vykonávaniu kyberneticko-bezpečnostnej zložky programu Digitálna Európa zriadeného nariadením XXX, a najmä akcií súvisiacich s článkom 6 nariadenia (EÚ) XXX [program Digitálna Európa], ako aj programu Európsky horizont zriadeného nariadením XXX, a najmä piliera II oddielu 2.2.6 prílohy I k rozhodnutiu XXX, ktorým sa stanovuje špecifický program na vykonávanie programu Európsky horizont – rámcový program pre výskum a inovácie [ref. č. osobitného programu].

3. Kompetenčné centrum má sídlo v [Bruseli v Belgicku].

4. Kompetenčné centrum má právnu subjektivitu. V každom členskom štáte má najširšiu právnu spôsobilosť priznávanú právnickým osobám podľa zákonov daného členského štátu. Môže predovšetkým nadobúdať alebo scudzovať hnuteľný a nehnuteľný majetok a môže byť účastníkom súdnych konaní.

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „kybernetická bezpečnosť“ je ochrana sietí a informačných systémov, ich používateľov a iných osôb pred kybernetickými hrozbami;

2. „kyberneticko-bezpečnostné produkty a riešenia“ sú produkty, služby alebo procesy IKT, ktorých osobitným cieľom je ochrana sietí a informačných systémov, ich používateľov a dotknutých osôb pred kybernetickými hrozbami;

3. „verejný orgán“ je akýkoľvek vládny alebo iný orgán verejnej správy vrátane verejných poradných orgánov na štátnej, regionálnej alebo miestnej úrovni, alebo akákoľvek fyzická alebo právnická osoba vykonávajúca funkcie verejnej správy podľa vnútroštátneho práva vrátane osobitných úloh;

4. „zúčastnený členský štát“ je členský štát, ktorý dobrovoľne finančne prispieva na krytie administratívnych a prevádzkových nákladov kompetenčného centra.

Článok 3

Poslanie centra a siete

1. Kompetenčné centrum a sieť pomáhajú Únii:

   a) udržiavať a rozvíjať technologické a odvetvové kapacity kybernetickej bezpečnosti potrebné na zabezpečenie jej digitálneho jednotného trhu;

   b) zvyšovať konkurencieschopnosť odvetvia kybernetickej bezpečnosti v Únii a premeniť kybernetickú bezpečnosť na konkurenčnú výhodu iných odvetví Únie.

2. Kompetenčné centrum podľa potreby vykonáva svoje úlohy v spolupráci so sieťou národných koordinačných centier a s komunitou kyberneticko-bezpečnostných kompetencií.

Článok 4

Ciele a úlohy centra

Kompetenčné centrum má tieto ciele a súvisiace úlohy:

1. podporovať a pomáhať pri koordinácii činnosti siete národných koordinačných centier (ďalej len „sieť“) uvedenej v článku 6 a komunity kyberneticko-bezpečnostných kompetencií uvedenej v článku 8;

2. prispievať k vykonávaniu kyberneticko-bezpečnostnej zložky programu Digitálna Európa zriadeného nariadením XXX[26], a najmä akcií súvisiacich s článkom 6 nariadenia (EÚ) XXX [program Digitálna Európa], ako aj programu Európsky horizont zriadeného nariadením XXX[27], a najmä piliera II oddielu 2.2.6 prílohy I k rozhodnutiu XXX, ktorým sa stanovuje špecifický program na vykonávanie programu Európsky horizont – rámcový program pre výskum a inovácie [ref. č. osobitného programu], ako aj ďalších programov Únie, ak sa tak stanoví v právnych aktoch Únie];

3. posilňovať kyberneticko-bezpečnostné spôsobilosti, znalosti a infraštruktúru k dispozícii jednotlivým odvetviam, verejnému sektoru a výskumnej obci, a to plnením týchto úloh:

   a) z hľadiska najmodernejšej odvetvovej a výskumnej infraštruktúry kybernetickej bezpečnosti a súvisiacich služieb: nadobúdanie, zdokonaľovanie, prevádzka a sprístupňovanie tejto infraštruktúry a súvisiacich služieb širokej škále používateľov v celej Únii z radov

[26] [doplniť celý názov a odkaz na Ú. v.].
[27] [doplniť celý názov a odkaz na Ú. v.].

jednotlivých odvetví (vrátane MSP), verejného sektora, výskumnej a vedeckej obce;

b) z hľadiska najmodernejšej odvetvovej a výskumnej infraštruktúry kybernetickej bezpečnosti a súvisiacich služieb: podpora iných subjektov (aj finančná) pri nadobúdaní, zdokonaľovaní, prevádzke a sprístupňovaní tejto infraštruktúry a súvisiacich služieb širokej škále používateľov v celej Únii z radov jednotlivých odvetví (vrátane MSP), verejného sektora, výskumnej a vedeckej obce;

c) poskytovanie kyberneticko-bezpečnostných znalostí a technickej pomoci odvetviam a verejným orgánom, najmä podporou opatrení zameraných na uľahčenie prístupu k odborným znalostiam, ktoré má k dispozícii sieť a komunita kyberneticko-bezpečnostných kompetencií;

4. prispievať k plošnému zavádzaniu najmodernejších kyberneticko-bezpečnostných produktov a riešení v celom hospodárstve, a to plnením týchto úloh:

a) stimulácia kyberneticko-bezpečnostného výskumu, vývoja a zavádzania kyberneticko-bezpečnostných produktov a riešení Únie verejnými orgánmi a používateľskými odvetviami;

a) pomoc verejným orgánom, odberateľským odvetviam a iným používateľom pri osvojovaní a integrácii najnovších kyberneticko-bezpečnostných riešení;

b) podpora najmä verejných orgánov pri organizácii verejných obstarávaní alebo samotné obstarávanie najmodernejších kyberneticko-bezpečnostných produktov a riešení v mene verejných orgánov;

c) finančná podpora a technická pomoc pre začínajúce podniky a MSP pôsobiace v oblasti kybernetickej bezpečnosti, aby sa napojili na potenciálne trhy a prilákali investície;

5. zlepšovať chápanie kybernetickej bezpečnosti a prispievať k dopĺňaniu chýbajúcich zručností v Únii v oblasti kybernetickej bezpečnosti, a to plnením týchto úloh:

a) podpora ďalšieho rozvoja kyberneticko-bezpečnostných zručností, podľa potreby v spolupráci s príslušnými agentúrami a orgánmi EÚ vrátane agentúry ENISA;

6. prispievať k posilňovaniu kyberneticko-bezpečnostného výskumu a vývoja v Únii, a to:

a) finančnou podporou kyberneticko-bezpečnostného výskumu na základe spoločného, priebežne hodnoteného a zdokonaľovaného viacročného programu zameraného na stratégiu, odvetvie, technológiu a výskum;

b) podporou rozsiahlych výskumných a demonštračných projektov, ktoré sa zameriavajú na kyberneticko-bezpečnostné spôsobilosti ďalšej generácie, v spolupráci s odvetvím a so sieťou;

c) podporou výskumu a inovácie v oblasti stanovovania kyberneticko-bezpečnostných noriem;

7. posilniť spoluprácu medzi civilnou a obrannou sférou, pokiaľ ide o technológie a aplikácie dvojakého použitia v oblasti kybernetickej bezpečnosti, a to plnením týchto úloh:

a) podpora členských štátov a zainteresovaných strán z odvetvia a výskumnej obce v oblastiach výskumu, vývoja a zavádzania;

b) prispievanie k spolupráci medzi členskými štátmi podporou vzdelávania, odbornej prípravy a cvičení;

c) združovanie zainteresovaných strán v záujme synergií medzi civilným a obranným kyberneticko-bezpečnostným výskumom a trhmi;

8. posilňovať synergie medzi civilným a obranným rozmerom kybernetickej bezpečnosti v súvislosti s Európskym obranným fondom, a to plnením týchto úloh:

a) poradenstvo, šírenie odborných poznatkov a podpora spolupráce relevantných zainteresovaných strán;

b) na žiadosť členských štátov riadenie nadnárodných projektov v oblasti kybernetickej obrany, a teda plnenie funkcie projektového manažéra v zmysle nariadenia XXX [nariadenie, ktorým sa zriaďuje Európsky obranný fond].

Článok 5

Investície do infraštruktúr, spôsobilostí, produktov alebo riešení a ich využívanie

1. Ak kompetenčné centrum poskytuje financovanie na infraštruktúry, spôsobilosti, produkty alebo riešenia podľa článku 4 ods. 3 a 4 formou grantu alebo ceny, v pracovnom pláne kompetenčného centra sa môžu vymedziť najmä:

a) pravidlá prevádzky infraštruktúry alebo spôsobilosti, prípadne vrátane zverenia prevádzky hostiteľskému subjektu na základe kritérií, ktoré určí kompetenčné centrum;

b) pravidlá prístupu k infraštruktúre alebo spôsobilosti a jej využívania.

2. Kompetenčné centrum môže niesť zodpovednosť za celkové vykonávanie relevantných spoločných obstarávacích akcií vrátane obstarávania vo fáze pred komerčným využitím v mene členov siete, členov komunity kyberneticko-bezpečnostných kompetencií alebo iných tretích strán, ktoré zastupujú používateľov kyberneticko-bezpečnostných produktov a riešení. Na tento účel môže kompetenčnému centru pomáhať jedno alebo viacero národných koordinačných centier alebo členovia komunity kyberneticko-bezpečnostných kompetencií.

Článok 6

Nominácia národných koordinačných centier

1. Do [dátum] každý členský štát nominuje subjekt, ktorý má na účely tohto nariadenia pôsobiť ako národné koordinačné centrum, a túto nomináciu oznámi Komisii.

2. Komisia na základe posúdenia súladu daného subjektu s kritériami stanovenými v odseku 4 vydá do šiestich mesiacov od prijatia nominácie od členského štátu rozhodnutie, ktorým udelí danému subjektu akreditáciu národného koordinačného centra alebo nomináciu zamietne. Zoznam národných koordinačných centier Komisia uverejní.

3. Členské štáty môžu za národné koordinačné centrum na účely tohto nariadenia kedykoľvek nominovať nový subjekt. Na nomináciu každého nového subjektu sa vzťahujú odseky 1 a 2.

4. Nominované národné koordinačné centrum musí byť schopné podporiť kompetenčné centrum a sieť pri plnení ich poslania podľa článku 3 tohto nariadenia. Musia buď samé disponovať kyberneticko-bezpečnostnou technologickou expertízou alebo k nej mať priamy prístup a musia byť schopné účinnej spolupráce a koordinácie s odvetvím, verejným sektorom a výskumnou obcou.

5. Vzťah medzi kompetenčným centrom a národnými koordinačnými centrami sa zakladá na zmluvnej dohode uzatvorenej medzi kompetenčným centrom a každým z národných koordinačných centier. V danej dohode sa stanovia pravidlá upravujúce vzťah a rozdelenie úloh medzi kompetenčným centrom a každým z národných koordinačných centier.

6. Sieť národných koordinačných centier zahŕňa všetky národné koordinačné centrá nominované členskými štátmi.

Článok 7

Úlohy národných koordinačných centier

1. Národné koordinačné centrá plnia tieto úlohy:

   a) podpora kompetenčného centra pri dosahovaní jeho cieľov, a najmä pri koordinácii komunity kyberneticko-bezpečnostných kompetencií;

   b) podpora účasti odvetvia a ďalších aktérov na úrovni členských štátov na cezhraničných projektoch;

   c) v spolupráci s kompetenčným centrom prispievanie k identifikácii a riešeniu kyberneticko-bezpečnostných výziev v jednotlivých odvetviach;

   d) funkcia styčného bodu s komunitou kyberneticko-bezpečnostných kompetencií a s kompetenčným centrom na národnej úrovni;

   e) snaha o vytvorenie synergií s relevantnými činnosťami na štátnej a regionálnej úrovni;

   f) realizácia špecifických akcií, na ktoré kompetenčné centrum udelilo granty, vrátane poskytovania finančnej podpory tretím stranám podľa článku 204 nariadenia XXX [nové nariadenie o rozpočtových pravidlách] za podmienok stanovených v príslušných dohodách o grante;

   g) propagácia a šírenie relevantných výsledkov činnosti siete, komunity kyberneticko-bezpečnostných kompetencií a kompetenčného centra na štátnej alebo regionálnej úrovni;

   h) posudzovanie žiadostí subjektov so sídlom v členskom štáte koordinačného centra o začlenenie do komunity kyberneticko-bezpečnostných kompetencií.

2. Na účely písmena f) možno finančnú podporu tretím stranám poskytnúť v ktorejkoľvek z foriem uvedených v článku 125 nariadenia XXX [nové nariadenie o rozpočtových pravidlách] vrátane jednorazových platieb.

3. Národné koordinačné centrá môžu získať od Únie grant v súlade s článkom 195 písm. d) nariadenia XXX [nové nariadenie o rozpočtových pravidlách] na plnenie úloh stanovených v tomto článku.

4. Národné koordinačné centrá v rámci siete podľa potreby spolupracujú na účely plnenia úloh uvedených v odseku 1 písm. a), b), c), e) a g).

Článok 8

Komunita kyberneticko-bezpečnostných kompetencií

1. Komunita kyberneticko-bezpečnostných kompetencií prispieva k napĺňaniu poslania kompetenčného centra v zmysle článku 3 a v celej Únii podporuje a šíri odborné znalosti v oblasti kybernetickej bezpečnosti.

2. Komunita kyberneticko-bezpečnostných kompetencií pozostáva z odvetvových, akademických a neziskových výskumných organizácií a združení, ako aj z verejných orgánov a iných orgánov, ktoré sa venujú prevádzkovým a technickým záležitostiam. V Únii združuje hlavné strany zainteresované na technologických a odvetvových spôsobilostiach v oblasti kybernetickej bezpečnosti. Zahŕňa národné koordinačné centrá, ako aj inštitúcie a orgány Únie s príslušnými odbornými znalosťami.

3. Za členov komunity kyberneticko-bezpečnostných kompetencií možno akreditovať iba subjekty so sídlom v Únii. Musia preukázať, že majú odborné znalosti aspoň v jednej z týchto domén kybernetickej bezpečnosti:

   a) výskum;

   b) odvetvový vývoj;

   c) vzdelávanie a odborná príprava.

4. Kompetenčné centrum akredituje subjekty zriadené podľa vnútroštátneho práva za členov komunity kyberneticko-bezpečnostných kompetencií na základe posúdenia splnenia kritérií uvedených v odseku 3, ktoré vykoná národné koordinačné centrum členského štátu, kde má daný subjekt sídlo. Akreditácia nie je časovo obmedzená, no kompetenčné centrum ju môže kedykoľvek odňať, ak kompetenčné centrum alebo národné koordinačné centrum dospeje k záveru, že daný subjekt nespĺňa kritériá odseku 3 alebo spadá pod príslušné ustanovenia článku 136 nariadenia XXX [nové nariadenie o rozpočtových pravidlách].

5. Kompetenčné centrum akredituje príslušné orgány, agentúry a úrady Únie za členov komunity kyberneticko-bezpečnostných kompetencií na základe posúdenia, či daný subjekt spĺňa kritériá uvedené v odseku 3. Akreditácia nie je časovo obmedzená, no kompetenčné centrum ju môže kedykoľvek odňať, ak dospeje k záveru, že daný subjekt nespĺňa kritériá odseku 3 alebo spadá pod príslušné ustanovenia článku 136 nariadenia XXX [nové nariadenie o rozpočtových pravidlách].

6. Na práci komunity sa môžu zúčastňovať zástupcovia Komisie.

Článok 9

Úlohy členov komunity kyberneticko-bezpečnostných kompetencií

Členovia komunity kyberneticko-bezpečnostných kompetencií:

1. podporujú kompetenčné centrum pri napĺňaní poslania a cieľov stanovených v článkoch 3 a 4, pričom na tento účel úzko spolupracujú s kompetenčným centrom a príslušnými národnými koordinačnými centrami;

2. sa zapájajú do činností podporovaných kompetenčným centrom a národnými koordinačnými centrami;

3. sa podľa potreby zúčastňujú pracovných skupín zriadených správnou radou kompetenčného centra na výkon osobitných činností v zmysle pracovného plánu kompetenčného centra;

4. podľa potreby podporujú kompetenčné centrum a národné koordinačné centrá pri propagácii konkrétnych projektov;

5. propagujú a šíria relevantné výsledky činností a projektov vykonávaných v rámci komunity.

Článok 10

Spolupráca kompetenčného centra s inštitúciami, orgánmi, úradmi a agentúrami Únie

1. Kompetenčné centrum spolupracuje s relevantnými inštitúciami, orgánmi, úradmi a agentúrami Únie vrátane Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť, tímu reakcie na núdzové počítačové situácie (CERT-EU), Európskej služby pre vonkajšiu činnosť, Spoločného výskumného centra Komisie, Výkonnej agentúry pre výskum, Výkonnej agentúry pre inovácie a siete, Európskeho centra boja proti počítačovej kriminalite pri Europole, ako aj Európskej obrannej agentúry.

2. Spolupráca prebieha v rámci pracovných dohôd. Tieto dohody sa vopred predložia Komisii na schválenie.

KAPITOLA II

ORGANIZÁCIA KOMPETENČNÉHO CENTRA

Článok 11

Členstvo a štruktúra

1. Členmi kompetenčného centra sú Únia zastúpená Komisiou a členské štáty.

2. Štruktúra kompetenčného centra zahŕňa tieto orgány:

   a) správna rada, ktorá plní úlohy stanovené v článku 13;

   b) výkonný riaditeľ, ktorý plní úlohy stanovené v článku 16;

   c) odvetvová a vedecká poradná rada, ktorá plní funkcie stanovené v článku 20.

ODDIEL I

SPRÁVNA RADA

Článok 12

Zloženie správnej rady

1. Správna rada je zložená z jedného zástupcu každého členského štátu a z piatich zástupcov Komisie v mene Únie.

2. Každý člen správnej rady má náhradníka, ktorý zastupuje člena v jeho neprítomnosti.

3. Členovia správnej rady a ich náhradníci sa vymenúvajú na základe ich znalostí v technologickej oblasti, ako aj na základe relevantných riadiacich, administratívnych a rozpočtových zručností. Komisia a členské štáty sa vynasnažia obmedziť fluktuáciu svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce. Komisia a členské štáty sa usilujú o vyvážené zastúpenie mužov a žien v správnej rade.

4. Funkčné obdobie členov správnej rady a ich náhradníkov je štyri roky. Toto obdobie je obnoviteľné.

5. Členovia správnej rady konajú nezávisle, transparentne a v záujme kompetenčného centra, pričom chránia jeho ciele, poslanie, identitu, samostatnosť a súdržnosť.

6. Komisia môže v prípade potreby pozvať na zasadnutia správnej rady pozorovateľov vrátane zástupcov relevantných orgánov, úradov a agentúr Únie.

7. Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) je v správnej rade stálym pozorovateľom.

Článok 13

Úlohy správnej rady

1. Správna rada nesie celkovú zodpovednosť za strategické zameranie a prevádzku kompetenčného centra a vykonáva dohľad nad realizáciou jeho činností.

2. Správna rada prijme svoj rokovací poriadok. Súčasťou uvedeného rokovacieho poriadku sú osobitné postupy na identifikáciu a predchádzanie konfliktu záujmov, ako aj na zabezpečenie dôvernosti všetkých citlivých informácií.

3. Správna rada prijíma potrebné strategické rozhodnutia, najmä:

   a) prijíma viacročný strategický plán, ktorý zahŕňa súpis hlavných priorít a plánovaných iniciatív kompetenčného centra vrátane odhadu finančných potrieb a zdrojov;

   b) prijíma pracovný plán, ročnú účtovnú závierku, súvahu a výročnú správu o činnosti kompetenčného centra na základe návrhu výkonného riaditeľa;

   c) prijíma osobitné rozpočtové pravidlá kompetenčného centra v súlade s [článkom 70 nariadenia o rozpočtových pravidlách];

   d) prijíma postup vymenovania výkonného riaditeľa;

   e) prijíma kritériá a postupy posudzovania a akreditácie subjektov za členov komunity kyberneticko-bezpečnostných kompetencií;

   f) vymenúva, odvoláva a predlžuje funkčné obdobie výkonného riaditeľa, poskytuje mu usmernenie a monitoruje jeho výsledky, a vymenúva účtovníka;

   g) prijíma ročný rozpočet kompetenčného centra vrátane zodpovedajúceho plánu pracovných miest, v ktorom sa uvedie počet dočasných pracovných miest podľa funkčnej skupiny a platovej triedy a počet zmluvných zamestnancov a vyslaných národných expertov vyjadrený v ekvivalentoch plného pracovného úväzku;

   h) prijíma pravidlá týkajúce sa konfliktu záujmov;

   i) spolu s členmi komunity kyberneticko-bezpečnostných kompetencií zriaďuje pracovné skupiny;

   j) vymenúva členov odvetvovej a vedeckej poradnej rady;

   k) zriadi funkciu vnútorného auditu v súlade s delegovaným nariadením Komisie (EÚ) č. 1271/2013[28];

[28] Delegované nariadenie Komisie (EÚ) č. 1271/2013 z 30. septembra 2013 o rámcovom nariadení o rozpočtových pravidlách pre subjekty uvedené v článku 208 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 966/2012 (Ú. v. EÚ L 328, 7.12.2013, s. 42).

l) globálne propaguje kompetenčné centrum s cieľom zvýšiť jeho atraktivitu a zabezpečiť mu postavenie svetového centra excelentnosti v oblasti kybernetickej bezpečnosti;

m) na základe odporúčania výkonného riaditeľa formuluje komunikačnú politiku kompetenčného centra;

n) zodpovedá za monitorovanie primeraných opatrení v nadväznosti na závery spätných hodnotení;

o) podľa potreby stanovuje vykonávacie pravidlá k služobnému poriadku a podmienkam zamestnávania v súlade s článkom 31 ods. 3;

p) podľa potreby stanovuje pravidlá vysielania národných expertov do kompetenčného centra a pravidlá využívania stážistov v súlade s článkom 32 ods. 2;

q) prijíma bezpečnostné pravidlá kompetenčného centra;

r) prijíma stratégiu boja proti podvodom, ktorá musí byť primeraná riziku podvodov so zreteľom na analýzu efektívnosti nákladov na opatrenia, ktoré sa majú vykonávať;

s) prijíma metodiku výpočtu finančného príspevku členských štátov;

t) zodpovedá za všetky úlohy, ktoré nie sú osobitne pridelené konkrétnemu orgánu kompetenčného centra; takéto úlohy môže delegovať na ktorýkoľvek orgán kompetenčného centra.

Článok 14

Predseda a zasadnutia správnej rady

1. Správna rada si spomedzi členov s hlasovacím právom volí predsedu a podpredsedu na dva roky. Mandát predsedu a podpredsedu možno predĺžiť raz na základe rozhodnutia správnej rady. Ak však ich členstvo v správnej rade kedykoľvek počas ich funkčného obdobia zanikne, ich funkčné obdobie sa automaticky končí k danému dátumu. Ak predseda nie je schopný plniť si svoje povinnosti, podpredseda ho nahradí *ex officio*. Predseda sa na hlasovaní zúčastňuje.

2. Riadne zasadnutia správnej rady sa konajú aspoň trikrát do roka. Na žiadosť Komisie, na žiadosť tretiny všetkých členov, na žiadosť predsedu alebo na žiadosť výkonného riaditeľa pri plnení jeho povinností možno zvolať mimoriadne zasadnutia.

3. Výkonný riaditeľ sa zúčastňuje na rokovaniach, pokiaľ správna rada nerozhodne inak, ale nemá hlasovacie právo. Správna rada môže na zasadnutia v jednotlivých prípadoch prizvať iné osoby ako pozorovateľov.

4. Na zasadnutiach správnej rady sa môžu na pozvanie predsedu zúčastniť členovia odvetvovej a vedeckej poradnej rady, avšak bez hlasovacieho práva.

5. Členom správnej rady a ich náhradníkom môžu v súlade s rokovacím poriadkom pomáhať poradcovia alebo experti.

6. Sekretariát pre správnu radu zabezpečuje kompetenčné centrum.

Článok 15

Pravidlá hlasovania správnej rady

1. Únia má 50 % hlasovacích práv. Hlasovacie práva Únie sú nedeliteľné.
2. Každý zúčastnený členský štát má jeden hlas.
3. Správna rada prijíma rozhodnutia väčšinou najmenej 75 % všetkých hlasov vrátane hlasov neprítomných členov, ktoré zodpovedajú aspoň 75 % celkových finančných príspevkov do kompetenčného centra. Finančný príspevok sa vypočíta na základe odhadovaných výdavkov navrhnutých členskými štátmi v zmysle článku 17 ods. 2 písm. c) a na základe správy o výške príspevkov zúčastnených členských štátov uvedenej v článku 22 ods. 5.
4. Hlasovacie práva majú iba zástupcovia Komisie a zástupcovia zúčastnených členských štátov.
5. Predseda sa na hlasovaní zúčastňuje.

ODDIEL II

VÝKONNÝ RIADITEĽ

Článok 16

Vymenovanie, odvolanie alebo predĺženie funkčného obdobia výkonného riaditeľa

1. Výkonný riaditeľ je osoba s odbornými znalosťami a výbornou povesťou v oblastiach, v ktorých kompetenčné centrum pôsobí.
2. Výkonný riaditeľ pôsobí ako dočasný zástupca kompetenčného centra podľa článku 2 písm. a) podmienok zamestnávania ostatných zamestnancov.
3. Výkonného riaditeľa vymenúva správna rada zo zoznamu kandidátov navrhnutých Komisiou pri uplatnení otvoreného a transparentného výberového konania.
4. Na účely uzatvorenia zmluvy s výkonným riaditeľom zastupuje kompetenčné centrum predseda správnej rady.
5. Funkčné obdobie výkonného riaditeľa je štyri roky. Na konci tohto obdobia Komisia vykoná posúdenie, v ktorom zohľadní hodnotenie výsledkov činnosti výkonného riaditeľa a budúce úlohy a výzvy kompetenčného centra.
6. Správna rada konajúc na návrh Komisie, v ktorom sa zohľadní posúdenie uvedené v odseku 5, môže predĺžiť funkčné obdobie výkonného riaditeľa raz, najviac o štyri roky.
7. Výkonný riaditeľ, ktorého funkčné obdobie sa predĺžilo, sa nemôže zúčastniť na ďalšom výberovom konaní na rovnakú funkciu.
8. Výkonný riaditeľ môže byť odvolaný z funkcie len na základe rozhodnutia správnej rady, ktorá koná na návrh Komisie.

Článok 17

Úlohy výkonného riaditeľa

1. Výkonný riaditeľ zodpovedá za prevádzku a každodenné riadenie kompetenčného centra a je jeho právnym zástupcom. Výkonný riaditeľ sa zodpovedá správnej rade a svoje úlohy plní úplne nezávisle v rámci udelených právomocí.

2. Výkonný riaditeľ najmä nezávisle plní tieto úlohy:

a) výkon rozhodnutí správnej rady;

b) podpora činnosti správnej rady, zabezpečovanie sekretariátu pre jej zasadnutia a poskytovanie všetkých informácií potrebných na plnenie jej úloh;

c) po konzultácii so správnou radou a s Komisiou – vypracovanie a predkladanie návrhu viacročného strategického plánu a návrhu ročného pracovného plánu kompetenčného centra správnej rade na schválenie, vrátane rozsahu výziev na predkladanie návrhov, výziev na vyjadrenie záujmu alebo výziev na predkladanie ponúk, ktoré si vykonávanie pracovného plánu vyžaduje, ako aj súvisiacich odhadov výdavkov navrhnutých členskými štátmi a Komisiou;

d) príprava a predloženie návrhu ročného rozpočtu správnej rade na schválenie vrátane zodpovedajúceho plánu pracovných miest, v ktorom sa uvedie počet dočasných pracovných miest v každej platovej triede a funkčnej skupine, ako aj počet zmluvných zamestnancov a vyslaných národných expertov vyjadrený v ekvivalentoch plného pracovného úväzku;

e) vykonávanie pracovného plánu a podávanie správ o ňom správnej rade;

f) vypracovanie návrhu výročnej správy o činnosti kompetenčného centra vrátane informácií o príslušných výdavkoch;

g) zaistenie uplatnenia účinných monitorovacích a hodnotiacich postupov vo vzťahu k výsledkom kompetenčného centra;

h) vypracovanie akčného plánu v nadväznosti na závery spätných hodnotení a predloženie správy o pokroku Komisii každé dva roky;

i) príprava, vyrokúvanie a uzavretie dohôd s národnými koordinačnými centrami;

j) zodpovednosť za administratívne, finančné a personálne otázky vrátane plnenia rozpočtu kompetenčného centra, s náležitým zohľadnením odporúčaní získaných z vnútorného auditu a v rámci kompetencií delegovaných správnou radou;

k) schvaľovanie a riadenie vyhlasovania výziev na predkladanie návrhov v súlade s pracovným plánom, ako aj spravovanie dohôd a rozhodnutí o grante;

l) schvaľovanie zoznamu akcií vybraných na financovanie na základe poradia určeného panelom nezávislých expertov;

m) schvaľovanie a riadenie vyhlasovania výziev na predkladanie ponúk v súlade s pracovným plánom, ako aj spravovanie príslušných zmlúv;

n) schvaľovanie ponúk vybraných na financovanie;

o) predkladanie návrhu ročnej účtovnej závierky a súvahy vnútornému auditu a následne správnej rade;

p) zabezpečenie hodnotenia a riadenia rizík;

q) podpisovanie individuálnych dohôd a rozhodnutí o grante, ako aj zmlúv;

r) podpisovanie verejných zákaziek;

s) vypracovanie akčného plánu v nadväznosti na závery správ z interného alebo externého auditu, ako aj z vyšetrovaní Európskeho úradu pre boj proti

podvodom (OLAF) a predkladanie správ o pokroku, a to dvakrát ročne Komisii a pravidelne správnej rade;

t) vypracovanie návrhu rozpočtových pravidiel platných pre kompetenčné centrum;

u) zavedenie a zabezpečenie fungovania účinného a efektívneho systému vnútornej kontroly a informovanie správnej rady o všetkých jeho podstatných zmenách;

v) zabezpečenie účinnej komunikácie s inštitúciami Únie;

w) prijímanie akýchkoľvek ďalších opatrení potrebných na vyhodnotenie pokroku kompetenčného centra v plnení jeho poslania a cieľov v zmysle článkov 3 a 4 tohto nariadenia;

a) plnenie všetkých ďalších úloh zverených alebo delegovaných výkonnému riaditeľovi správnou radou.

ODDIEL III

ODVETVOVÁ A VEDECKÁ PORADNÁ RADA

Článok 18

Zloženie odvetvovej a vedeckej poradnej rady

1. Odvetvová a vedecká poradná rada má najviac 16 členov. Členov vymenúva správna rada spomedzi zástupcov subjektov komunity kyberneticko-bezpečnostných kompetencií.

2. Členovia odvetvovej a vedeckej poradnej rady musia mať odborné znalosti z oblasti kyberneticko-bezpečnostného výskumu, odvetvového vývoja, odborných služieb alebo ich zavádzania. Požiadavky na tieto odborné znalosti bližšie určí správna rada.

3. Postupy menovania členov správnou radou, ako aj postupy fungovania poradnej rady sa bližšie určia v rokovacom poriadku kompetenčného centra a uverejnia sa.

4. Funkčné obdobie členov odvetvovej a vedeckej poradnej rady je tri roky. Toto obdobie je obnoviteľné.

5. Na zasadnutiach odvetvovej a vedeckej poradnej rady sa môžu zúčastňovať zástupcovia Komisie a Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť, ktorí môžu prácu poradnej rady podporovať.

Článok 19

Fungovanie odvetvovej a vedeckej poradnej rady

1. Odvetvová a vedecká poradná rada zasadá aspoň dvakrát ročne.

2. Odvetvová a vedecká poradná rada môže radiť správnej rade v otázkach zriaďovania pracovných skupín pre konkrétne problémy relevantné pre prácu kompetenčného centra podľa potreby, pričom celková koordinácia spočíva na jednom alebo viacerých členoch odvetvovej a vedeckej poradnej rady.

3. Odvetvová a vedecká poradná rada si zvolí predsedu.

4. Odvetvová a vedecká poradná rada prijme svoj rokovací poriadok, kde určí menovanie zástupcov, ktorí poradnú radu podľa potreby zastupujú, ako aj trvanie ich funkčného obdobia.

Článok 20

Úlohy odvetvovej a vedeckej poradnej rady

Odvetvová a vedecká poradná rada radí kompetenčnému centru pri výkone jeho činností a:

1. poskytuje výkonnému riaditeľovi a správnej rade strategické poradenstvo a vstupy pre vypracovanie pracovného plánu a viacročného strategického plánu v lehotách, ktoré stanoví správna rada;
2. organizuje verejné konzultácie otvorené všetkým zainteresovaným stranám z verejného a súkromného sektora, ktoré majú záujmy v oblasti kybernetickej bezpečnosti, s cieľom získať vstupy pre strategické poradenstvo uvedené v odseku 1;
3. podporuje a zhromažďuje spätnú väzbu k pracovnému plánu a viacročnému strategickému plánu kompetenčného centra.

KAPITOLA III
FINANČNÉ USTANOVENIA

Článok 21

Finančný príspevok Únie

1. Príspevok Únie na krytie administratívnych a prevádzkových nákladov kompetenčného centra zahŕňa:
   a) 1 981 668 000 EUR z programu Digitálna Európa, z toho najviac 23 746 000 EUR na administratívne náklady;
   b) sumu z programu Európsky horizont (vrátane krytia administratívnych nákladov), ktorá sa určí pri zohľadnení procesu strategického plánovania, ktorý sa vykoná podľa článku 6 ods. 6 nariadenia XXX [nariadenie o Európskom horizonte].
2. Maximálny príspevok Únie sa vyplatí z rozpočtových prostriedkov pridelených vo všeobecnom rozpočte Únie na [program Digitálna Európa] a na osobitný program na vykonávanie programu Európsky horizont stanovený rozhodnutím XXX.
3. Kompetenčné centrum implementuje kyberneticko-bezpečnostné akcie [programu Digitálna Európa] a [programu Európsky horizont] v súlade s článkom 62 písm. c) bodom iv) nariadenia (EÚ, Euratom) XXX[29] [nariadenie o rozpočtových pravidlách].
4. Finančný príspevok Únie nezahŕňa úlohy uvedené v článku 4 ods. 8 písm. b).

[29] [doplniť celý názov a odkaz na Ú. v.].

Článok 22

Príspevky zúčastnených členských štátov

1. Zúčastnené členské štáty poskytnú celkový príspevok na krytie prevádzkových a administratívnych nákladov kompetenčného centra aspoň v rovnakej výške ako príspevok podľa článku 21 ods. 1 tohto nariadenia.

2. Na účely hodnotenia príspevkov uvedených v odseku 1 a v článku 23 ods. 3 písm. b) bode ii) sa náklady určujú na základe obvyklých postupov nákladového účtovníctva daných členských štátov, príslušných účtovných štandardov daného členského štátu a príslušných medzinárodných účtovných štandardov a medzinárodných štandardov finančného výkazníctva. Náklady osvedčuje nezávislý externý audítor vymenovaný príslušným členským štátom. Ak by z osvedčenia vyplynuli akékoľvek pochybnosti, metódu určenia hodnoty príspevkov môže overiť kompetenčné centrum.

3. Ak by niektorý zúčastnený členský štát neplnil svoje záväzky týkajúce sa finančného príspevku, výkonný riaditeľ mu to písomne oznámi a určí primeranú lehotu na nápravu. Ak v určenej lehote nedošlo k náprave situácie, výkonný riaditeľ zvolá zasadnutie správnej rady, aby rozhodla, či sa neplniacemu zúčastnenému členskému štátu má odňať hlasovacie právo alebo sa majú prijať iné opatrenia, až kým nesplní svoje záväzky. Hlasovacie právo neplniaceho členského štátu sa pozastaví, až kým si nesplní svoje záväzky.

4. Komisia môže ukončiť alebo pozastaviť poskytovanie finančného príspevku Únie na kompetenčné centrum alebo ho primerane znížiť, ak zúčastnené členské štáty neprispievajú, prispievajú iba čiastočne alebo sú v omeškaní s poskytovaním príspevkov uvedených v odseku 1.

5. Zúčastnené členské štáty predkladajú správnej rade každoročne do 31. januára správu o výške príspevkov uvedených v odseku 1, ktoré sa vykonali v každom predchádzajúcom rozpočtovom roku.

Článok 23

Náklady a zdroje kompetenčného centra

1. Kompetenčné centrum je spolufinancované Úniou a členskými štátmi formou finančných príspevkov vyplácaných v splátkach a príspevkov pozostávajúcich z nákladov vynaložených národnými koordinačnými centrami a príjemcami pri vykonávaní akcií, ktoré kompetenčné centrum neuhrádza.

2. Administratívne náklady kompetenčného centra neprekročia sumu [suma] EUR a hradia sa z finančných príspevkov každoročne rozdelených rovnakým dielom medzi Úniu a zúčastnené členské štáty. Ak sa časť príspevku na administratívne náklady nevyužije, môže sa poskytnúť na uhradenie prevádzkových nákladov kompetenčného centra.

3. Prevádzkové náklady kompetenčného centra sa hradia z týchto príspevkov:

   a) finančný príspevok Únie;

   b) príspevky zúčastnených členských štátov vo forme:

      i) finančných príspevkov a

      ii) nefinančných príspevkov zúčastnených členských štátov v podobe nákladov vynaložených národnými koordinačnými centrami a

príjemcami pri vykonávaní nepriamych akcií, od ktorých sa odpočíta príspevok kompetenčného centra a akýkoľvek iný príspevok Únie na tieto náklady.

4. Zdroje kompetenčného centra zahrnuté do jeho rozpočtu sa skladajú z týchto príspevkov:

   a) finančné príspevky zúčastnených členských štátov na administratívne náklady;

   b) finančné príspevky zúčastnených členských štátov na prevádzkové náklady;

   c) všetky prípadné príjmy kompetenčného centra;

   d) akékoľvek iné finančné príspevky, zdroje a príjmy.

5. Všetky úroky z príspevkov, ktoré kompetenčnému centru poskytli zúčastnené členské štáty, sa považujú za jeho príjmy.

6. Všetky zdroje kompetenčného centra a jeho činností sú zamerané na dosiahnutie cieľov stanovených v článku 4.

7. Kompetenčné centrum vlastní všetky aktíva, ktoré vytvorí alebo ktoré sú naň prevedené na účely plnenia jeho cieľov.

8. S výnimkou likvidácie kompetenčného centra sa jeho zúčastneným členom prebytky príjmov oproti výdavkom nevyplácajú.

Článok 24

Finančné záväzky

Finančné záväzky kompetenčného centra nepresiahnu sumu finančných zdrojov, ktoré sú k dispozícii v rozpočte alebo ktoré preň vyčlenili jeho členovia.

Článok 25

Rozpočtový rok

Rozpočtový rok trvá od 1. januára do 31. decembra.

Článok 26

Zostavovanie rozpočtu

1. Výkonný riaditeľ každoročne vypracúva návrh výkazu odhadov príjmov a výdavkov kompetenčného centra na nasledujúci rozpočtový rok a postupuje ho správnej rade spolu s návrhom plánu pracovných miest. Príjmy a výdavky musia byť v rovnováhe. Výdavky kompetenčného centra zahŕňajú výdavky na pracovníkov, administratívu, infraštruktúru a prevádzku. Administratívne výdavky sa udržiavajú na minimálnej úrovni.

2. Správna rada každý rok na základe návrhu výkazu odhadov príjmov a výdavkov uvedeného v odseku 1 vytvorí výkaz odhadovaných príjmov a výdavkov kompetenčného centra na nasledujúci rozpočtový rok.

3. Výkaz odhadov uvedený v odseku 2, ktorý je súčasťou návrhu jednotného programového dokumentu, správna rada každoročne do 31. januára zasiela Komisii.

4. Komisia na základe tohto výkazu odhadov zaradí do návrhu rozpočtu Únie odhady, ktoré pokladá za potrebné pre plán pracovných miest, a výšku príspevku, ktorá sa má

uhradiť zo všeobecného rozpočtu, ktoré predloží Európskemu parlamentu a Rade v súlade s článkom 313 a 314 ZFEÚ.

5. Európsky parlament a Rada schvaľujú rozpočtové prostriedky na príspevok na kompetenčné centrum.

6. Európsky parlament a Rada prijímajú plán pracovných miest kompetenčného centra.

7. Správna rada prijíma rozpočet centra spolu s pracovným plánom. Rozpočet sa stáva konečným po prijatí všeobecného rozpočtu Únie s konečnou platnosťou. Správna rada v prípade potreby upraví rozpočet a pracovný plán kompetenčného centra v súlade so všeobecným rozpočtom Únie.

Článok 27

Predkladanie účtovnej závierky kompetenčného centra a absolutórium

Predkladanie predbežnej a konečnej účtovnej závierky kompetenčného centra a absolutórium sa riadi pravidlami a harmonogramom podľa nariadenia o rozpočtových pravidlách a jeho vlastnými rozpočtovými pravidlami prijatými podľa článku 29.

Článok 28

Operačné a finančné vykazovanie

1. Výkonný riaditeľ každý rok podáva správnej rade správu o plnení svojich povinností v súlade s rozpočtovými pravidlami kompetenčného centra.

2. Do dvoch mesiacov od konca každého rozpočtového roka predloží výkonný riaditeľ správnej rade na schválenie výročnú správu o činnosti týkajúcu sa pokroku, ktorý kompetenčné centrum dosiahlo v predchádzajúcom kalendárnom roku, najmä pokiaľ ide o pracovný plán na daný rok. Správa musí okrem iného obsahovať informácie o:

   a) vykonaných operačných akciách a súvisiacich výdavkoch;

   b) navrhnutých akciách s rozdelením podľa druhu účastníkov vrátane MSP a podľa členských štátov;

   c) akciách vybraných na financovanie s rozdelením podľa druhu účastníkov vrátane MSP a podľa členských štátov a s uvedením príspevku kompetenčného centra pre jednotlivých účastníkov a na jednotlivé akcie;

   d) pokroku pri dosahovaní cieľov vytýčených v článku 4 a návrhoch ďalších krokov potrebných na dosiahnutie týchto cieľov.

3. Po schválení správnou radou sa výročná správa o činnosti zverejní.

Článok 29

Rozpočtové pravidlá

Kompetenčné centrum prijme svoje osobitné rozpočtové pravidlá v súlade s článkom 70 nariadenia XXX [nové nariadenie o rozpočtových pravidlách].

Článok 30

Ochrana finančných záujmov

1. Kompetenčné centrum prijme príslušné opatrenia na zabezpečenie toho, aby sa pri vykonávaní akcií financovaných na základe tohto nariadenia chránili finančné záujmy Únie uplatňovaním preventívnych opatrení na zamedzenie podvodom, korupcii a iným protiprávnym činnostiam, účinnými kontrolami, vymáhaním neoprávnene vyplatených súm pri odhalení nezrovnalostí a v prípade potreby aj ukladaním účinných, primeraných a odrádzajúcich administratívnych sankcií.

2. Kompetenčné centrum umožní pracovníkom Komisie a ďalším osobám povereným Komisiou, ako aj Dvorom audítorov, prístup do svojich vonkajších a vnútorných priestorov a k všetkým informáciám potrebným na vykonanie auditov vrátane informácií v elektronickej podobe.

3. Európsky úrad pre boj proti podvodom (OLAF) môže vykonávať vyšetrovania vrátane kontrol a inšpekcií na mieste v súlade s ustanoveniami a postupmi stanovenými v nariadení Rady (Euratom, ES) č. 2185/96[30] a nariadení Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013[31] s cieľom zistiť, či v súvislosti s dohodou o grante alebo zmluvou financovanou priamo alebo nepriamo v súlade s týmto nariadením došlo k podvodu, korupcii alebo akémukoľvek inému protiprávnemu konaniu poškodzujúcemu finančné záujmy Únie.

4. Bez toho, aby boli dotknuté odseky 1, 2 a 3 tohto článku, zmluvy a dohody o grante vyplývajúce z vykonávania tohto nariadenia musia obsahovať ustanovenia, ktorými sa výslovne udeľuje Komisii, kompetenčnému centru, Dvoru audítorov a úradu OLAF právomoc na vykonávanie takýchto auditov a vyšetrovaní v súlade s ich príslušnými právomocami. Ak sa vykonávanie celej akcie alebo jej časti zabezpečuje externe alebo subdeleguje alebo ak si vyžaduje zadanie verejnej zákazky alebo udelenie finančnej podpory tretej strane, zmluva alebo dohoda o grante musí zahŕňať záväzok dodávateľa alebo príjemcu uložiť každej zapojenej tretej strane povinnosť výslovne akceptovať uvedené právomoci Komisie, kompetenčného centra, Dvora audítorov a úradu OLAF.

KAPITOLA IV

ZAMESTNANCI KOMPETENČNÉHO CENTRA

Článok 31

Zamestnanci

1. Na zamestnancov kompetenčného centra sa vzťahuje Služobný poriadok úradníkov Európskej únie (ďalej len „služobný poriadok“) a Podmienky zamestnávania ostatných zamestnancov Európskej únie (ďalej len „podmienky zamestnávania“) stanovené nariadením Rady (EHS, Euratom, ESUO) č. 259/68[32], ako aj pravidlá

[30] Nariadenie Rady (Euratom, ES) č. 2185/96 z 11. novembra 1996 o kontrolách a inšpekciách na mieste, vykonávaných Komisiou s cieľom ochrany finančných záujmov Európskych spoločenstiev pred spreneverou a inými podvodmi (Ú. v. ES L 292, 15.11.1996, s. 2).

[31] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) No 883/2013 z 11. septembra 2013 o vyšetrovaniach vykonávaných Európskym úradom pre boj proti podvodom (OLAF), ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 1073/1999 a nariadenie Rady (Euratom) č. 1074/1999 (Ú. v. EÚ L 248, 18.9.2013, s. 1).

[32] Nariadenie Rady (EHS, Euratom, ESUO) č. 259/68 z 29. februára 1968, ktorým sa ustanovuje Služobný poriadok úradníkov a Podmienky zamestnávania ostatných zamestnancov Európskych spoločenstiev a prijímajú osobitné opatrenia dočasne uplatniteľné na úradníkov Komisie (Ú. v. ES L 56, 4.3.1968, s. 1).

prijaté spoločne inštitúciami Únie na účely uplatňovania služobného poriadku a podmienok zamestnávania.

2. Správna rada vykonáva vo vzťahu k zamestnancom kompetenčného centra právomoci zverené služobným poriadkom menovaciemu orgánu a právomoci zverené podmienkami zamestnávania orgánu splnomocnenému uzatvárať pracovné zmluvy (ďalej len „právomoci menovacieho orgánu“).

3. Správna rada v súlade s článkom 110 služobného poriadku prijíma rozhodnutie na základe článku 2 ods. 1 služobného poriadku a článku 6 podmienok zamestnávania, ktorým deleguje príslušné právomoci menovacieho orgánu na výkonného riaditeľa a ktorým vymedzuje podmienky, za ktorých možno toto delegovanie právomocí pozastaviť. Výkonný riaditeľ je oprávnený tieto právomoci subdelegovať.

4. Ak si to vyžadujú mimoriadne okolnosti, správna rada môže formou rozhodnutia dočasne pozastaviť delegovanie právomocí menovacieho orgánu na výkonného riaditeľa, ako aj právomocí, ktoré subdelegoval. V takýchto prípadoch správna rada vykonáva právomoci menovacieho orgánu sama alebo ich deleguje na jedného zo svojich členov alebo na iného zamestnanca kompetenčného centra, ktorý nie je výkonným riaditeľom.

5. Správna rada prijíma príslušné vykonávacie predpisy k služobnému poriadku a podmienkam zamestnávania v súlade s článkom 110 služobného poriadku.

6. Počet zamestnancov sa stanoví v pláne pracovných miest kompetenčného centra s uvedením počtu dočasných pracovných miest podľa funkčnej skupiny a platovej triedy a počtu zmluvných zamestnancov vyjadreného v ekvivalente plného pracovného úväzku v súlade s jeho ročným rozpočtom.

7. Medzi zamestnancov kompetenčného centra patria dočasní zamestnanci a zmluvní zamestnanci.

8. Všetky náklady na zamestnancov znáša kompetenčné centrum.

Článok 32

Vyslaní národní experti a ďalší pracovníci

1. Kompetenčné centrum môže využívať vyslaných národných expertov alebo ďalších pracovníkov, ktorých nezamestnáva.

2. Správna rada prijme v súlade s Komisiou rozhodnutie, v ktorom stanoví pravidlá vysielania národných expertov do kompetenčného centra.

Článok 33

Výsady a imunity

Na kompetenčné centrum a jeho zamestnancov sa vzťahuje Protokol č. 7 o výsadách a imunitách Európskej únie, ktorý je pripojený k Zmluve o Európskej únii a k Zmluve o fungovaní Európskej únie.

KAPITOLA V
SPOLOČNÉ USTANOVENIA

Článok 34

Bezpečnostné pravidlá

1. Účasť na všetkých akciách financovaných kompetenčným centrom podlieha článku 12 ods. 7 nariadenia (EÚ) XXX [program Digitálna Európa].

2. Akcie financované z programu Európsky horizont sa riadia týmito osobitnými bezpečnostnými pravidlami:

   a) na účely článku 34 ods. 1 [Vlastníctvo a ochrana] nariadenia (EÚ) XXX [Európsky horizont], ak sa tak stanovuje v pracovnom pláne, môže byť udelenie nevýhradných licencií obmedzené na tretie strany, ktoré sú usadené alebo sa považujú za usadené v členských štátoch, a/alebo na štátnych príslušníkov členských štátov;

   a) na účely článku 36 ods. 4 písm. b) [Prevod a udelenie licencie] nariadenia (EÚ) XXX [Európsky horizont] je prevod alebo udelenie licencie právnemu subjektu usadenému v pridruženej krajine alebo usadenému v Únii ale kontrolovanému z tretích krajín tiež dôvodom namietať proti prevodu vlastníctva výsledkov, resp. proti udeľovaniu výhradných licencií na výsledky;

   b) na účely článku 37 ods. 3 písm. a) [Prístupové práva] nariadenia (EÚ) XXX [Európsky horizont], ak sa tak stanovuje v pracovnom pláne, môže byť udelenie prístupu k výsledkom alebo podkladom obmedzené iba na právne subjekty, ktoré sú usadené alebo sa považujú za usadené v členských štátoch, a/alebo na štátnych príslušníkov členských štátov;

Článok 35

Transparentnosť

1. Kompetenčné centrum vykonáva svoje činnosti s vysokým stupňom transparentnosti.

2. Kompetenčné centrum zabezpečí, aby verejnosť a všetky zainteresované strany dostávali náležité, objektívne, spoľahlivé a ľahko dostupné informácie, najmä o výsledkoch jeho práce. Kompetenčné centrum takisto zverejňuje vyhlásenia o záujmoch predkladané podľa článku 41.

3. Správna rada konajúc na návrh výkonného riaditeľa môže subjektom, ktoré majú záujem, povoliť pozorovanie postupov niektorých činností kompetenčného centra.

4. Kompetenčné centrum vo svojom rokovacom poriadku stanoví praktické opatrenia na vykonávanie pravidiel transparentnosti uvedených v odsekoch 1 a 2. V prípade akcií financovaných z programu Európsky horizont sa pri tom náležite zohľadnia ustanovenia prílohy III k nariadeniu o Európskom horizonte.

Článok 36

Bezpečnostné pravidlá v oblasti ochrany utajovaných skutočností a citlivých neutajovaných skutočností

1. Bez toho, aby bol dotknutý článok 35, kompetenčné centrum nesmie poskytovať tretím stranám informácie, ktoré spracúva alebo získava a v súvislosti s ktorými bola podaná odôvodnená žiadosť o úplné alebo čiastočné dôverné zaobchádzanie.

2. Členovia správnej rady, výkonný riaditeľ, členovia odvetvovej a vedeckej poradnej rady, externí experti zúčastňujúci sa *ad hoc* pracovných skupín a zamestnanci centra

musia aj po skončení povinností spĺňať požiadavky na dôvernosť informácií podľa článku 339 Zmluvy o fungovaní Európskej únie.

3. Správna rada kompetenčného centra na základe schválenia Komisiou prijme bezpečnostné pravidlá kompetenčného centra, ktoré vychádzajú zo zásad a pravidiel stanovených v bezpečnostných predpisoch Komisie na ochranu utajovaných skutočností Európskej únie (EUCI) a citlivých neutajovaných skutočností, okrem iného vrátane ustanovení o spracovaní a uchovávaní takýchto informácií v zmysle rozhodnutí Komisie (EÚ, Euratom) 2015/443[33] a 2015/444[34].

4. Kompetenčné centrum môže prijať všetky opatrenia potrebné na uľahčenie výmeny informácií týkajúcich sa jej úloh s Komisiou a členskými štátmi a prípadne aj s príslušnými agentúrami a orgánmi Únie. Všetky administratívne dohody uzatvorené na tento účel, ktoré sa týkajú výmeny EUCI, alebo ak takéto dohody neexistujú, všetky výnimočné prípady poskytnutia EUCI *ad hoc* musí vopred schváliť Komisia.

Článok 37

Prístup k dokumentom

1. Na dokumenty v držbe kompetenčného centra sa vzťahuje nariadenie (ES) č. 1049/2001.

2. Správna rada prijme opatrenia na vykonanie nariadenia (ES) č. 1049/2001 do šiestich mesiacov od zriadenia kompetenčného centra.

3. Rozhodnutia kompetenčného centra podľa článku 8 nariadenia (ES) č. 1049/2001 môžu byť predmetom sťažnosti podanej ombudsmanovi podľa článku 228 Zmluvy o fungovaní Európskej únie alebo konania pred Súdnym dvorom Európskej únie podľa článku 263 Zmluvy o fungovaní Európskej únie.

Článok 38

Monitorovanie, hodnotenie a preskúmanie

1. Kompetenčné centrum zabezpečí, aby sa jeho činnosti vrátane tých, ktoré sa spravujú prostredníctvom národných koordinačných centier a siete, priebežne a systematicky monitorovali a aby sa pravidelne hodnotili. Kompetenčné centrum zabezpečí efektívny, účinný a včasný zber údajov na monitorovanie vykonávania programu a jeho výsledkov, pričom príjemcom prostriedkov Únie a členským štátom sa uložia primerané oznamovacie povinnosti. Výsledky hodnotenia sa zverejnia.

2. Keď bude k dispozícii dostatok informácií o vykonávaní tohto nariadenia, najneskôr však tri a pol roka po začatí jeho vykonávania, Komisia kompetenčné centrum priebežne vyhodnotí. Komisia vypracuje o tomto hodnotení správu, ktorú predloží Európskemu parlamentu a Rade do 31. decembra 2024. Kompetenčné centrum a členské štáty poskytnú Komisii informácie potrebné na vypracovanie tejto správy.

3. Hodnotenie uvedené v odseku 2 zahŕňa posúdenie výsledkov kompetenčného centra so zreteľom na jeho ciele, mandát a úlohy. Ak Komisia dospeje k záveru, že z

[33] Rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii (Ú. v. EÚ L 72, 17.3.2015, s. 41).

[34] Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

hľadiska pridelených cieľov, mandátu a úloh kompetenčného centra je pokračovanie jeho činnosti odôvodnené, môže navrhnúť predĺženie mandátu kompetenčného centra stanoveného v článku 46.

4. Na základe záverov priebežného hodnotenia uvedeného v odseku 2 Komisia môže konať v súlade s [článkom 22 ods. 5], alebo prijať iné primerané opatrenia.

5. Monitorovanie, hodnotenie, postupné ukončovanie a obnova príspevku z programu Európsky horizont sa bude riadiť ustanoveniami článkov 8, 45 a 47 nariadenia o Európskom horizonte a prílohy III k nemu, ako aj dohodnutými implementačnými pravidlami.

6. Monitorovanie, podávanie správ a hodnotenie príspevku z programu Digitálna Európa sa bude riadiť ustanoveniami článkov 24 a 25 programu Digitálna Európa.

7. V prípade likvidácie kompetenčného centra Komisia vykoná jeho záverečné hodnotenie do šiestich mesiacov po jeho likvidácii, najneskôr však dva roky od začatia postupu likvidácie uvedeného v článku 46 tohto nariadenia. Výsledky tohto záverečného hodnotenia sa predložia Európskemu parlamentu a Rade.

Článok 39

Zodpovednosť kompetenčného centra

1. Zmluvnú zodpovednosť kompetenčného centra upravuje rozhodné právo pre danú dohodu, rozhodnutie alebo zmluvu.

2. V prípade mimozmluvnej zodpovednosti kompetenčné centrum nahradí v súlade so všeobecnými zásadami spoločnými pre právne poriadky členských štátov všetky škody, ktoré spôsobilo kompetenčné centrum alebo jeho zamestnanci pri vykonávaní svojich povinností.

3. Všetky platby kompetenčného centra vykonané v súvislosti so zodpovednosťou uvedenou v odsekoch 1 a 2 a náklady a výdavky vzniknuté v tejto súvislosti sa považujú za výdavok kompetenčného centra a uhradia sa z jeho zdrojov.

4. Kompetenčné centrum nesie výlučnú zodpovednosť za plnenie svojich záväzkov.

Článok 40

Právomoc Súdneho dvora Európskej únie a rozhodné právo

1. Súdny dvor Európskej únie má právomoc:

    1. podľa akejkoľvek rozhodcovskej doložky obsiahnutej v dohodách, rozhodnutiach alebo zmluvách uzatvorených kompetenčným centrom;

    2. v sporoch týkajúcich sa náhrady škody spôsobenej zamestnancami kompetenčného centra pri výkone ich funkcií;

    3. v každom spore medzi kompetenčným centrom a jeho zamestnancami v rámci obmedzení a za podmienok stanovených v služobnom poriadku.

2. Na všetky záležitosti, na ktoré sa nevzťahuje toto nariadenie alebo iné právne akty Únie, sa uplatňuje právo členského štátu, v ktorom sa nachádza sídlo kompetenčného centra.

Článok 41

Zodpovednosť členov a poistenie

1. Finančná zodpovednosť členov za dlhy kompetenčného centra je obmedzená na výšku ich už poskytnutého príspevku na administratívne náklady.
2. Kompetenčné centrum uzavrie a udržiava vhodné poistenie.

Článok 42

Konflikty záujmov

Správna rada kompetenčného centra prijme pravidlá predchádzania a riadenia konfliktu záujmov so zreteľom na jeho členov, orgány a zamestnancov. Tieto pravidlá musia zahŕňať ustanovenia zamerané na zabránenie konfliktu záujmov zástupcov členov v správnej rade, ako aj v odvetvovej a vedeckej poradnej rade, v súlade s nariadením XXX [nové nariadenie o rozpočtových pravidlách].

Článok 43

Ochrana osobných údajov

1. Spracovávanie osobných údajov kompetenčným centrom podlieha nariadeniu Európskeho parlamentu a Rady (EÚ) XXX/2018.
2. Správna rada prijme vykonávacie opatrenia uvedené v článku xx ods. 3 nariadenia (EÚ) xxx/2018. Správna rada môže prijať dodatočné opatrenia potrebné na uplatňovanie nariadenia (EÚ) xxx/2018 kompetenčným centrom.

Článok 44

Podpora zo strany hostiteľského členského štátu

Medzi kompetenčným centrom a členským štátom [Belgickom], v ktorom sa nachádza jeho sídlo, sa môže uzatvoriť administratívna dohoda o výsadách a imunitách a inej podpore, ktorú tento členský štát poskytne kompetenčnému centru.

KAPITOLA VII

ZÁVEREČNÉ USTANOVENIA

Článok 45

Počiatočné opatrenia

1. Komisia je zodpovedná za zriadenie a počiatočnú prevádzku kompetenčného centra, kým nedosiahne prevádzkovú kapacitu na plnenie vlastného rozpočtu. Komisia podnikne v súlade s právom Únie všetky potrebné kroky so zapojením príslušných orgánov kompetenčného centra.

2. Na účely odseku 1, kým sa výkonný riaditeľ po svojom vymenovaní správnou radou v súlade s článkom 16 neujme výkonu funkcie, môže Komisia vymenovať dočasného výkonného riaditeľa, ktorý plní povinnosti náležiace výkonnému riaditeľovi a ktorému môže pomáhať obmedzený počet úradníkov Komisie. Komisia môže dočasne prideliť obmedzený počet svojich úradníkov.

3. Dočasný výkonný riaditeľ môže povoľovať všetky platby pokryté rozpočtovými prostriedkami z ročného rozpočtu kompetenčného centra po schválení správnou radou a môže prijímať rozhodnutia a uzatvárať dohody a zmluvy vrátane zamestnaneckých zmlúv po prijatí plánu pracovných miest kompetenčného centra.

4. Dočasný výkonný riaditeľ po vzájomnej dohode s výkonným riaditeľom kompetenčného centra a na základe súhlasu správnej rady stanoví dátum, keď kompetenčné centrum dosiahne kapacitu na plnenie vlastného rozpočtu. Od uvedeného dátumu Komisia prestane prijímať záväzky a vykonávať platby súvisiace s činnosťami kompetenčného centra.

Článok 46

Trvanie

1. Kompetenčné centrum sa zriaďuje na obdobie od 1. januára 2021 do 31. decembra 2029.

2. Na konci tohto obdobia, pokiaľ sa nerozhodne inak na základe preskúmania tohto nariadenia, sa spustí proces likvidácie. Postup likvidácie sa spustí automaticky, ak z kompetenčného centra vystúpi Únia alebo všetky zúčastnené členské štáty.

3. Na účely vykonania postupu likvidácie kompetenčného centra správna rada vymenuje jedného alebo viacerých likvidátorov, ktorí sa musia riadiť rozhodnutiami správnej rady.

4. Pri likvidácii kompetenčného centra sa jeho aktíva použijú na pokrytie jeho záväzkov a výdavkov spojených s likvidáciou. Prípadný prebytok sa rozdelí medzi Úniu a zúčastnené členské štáty úmerne k ich finančnému príspevku na kompetenčné centrum. Akýkoľvek prebytok pridelený Únii sa vráti do rozpočtu Únie.

Článok 47

Nadobudnutie účinnosti

Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

Za Európsky parlament	*Za Radu*
predseda	*predseda*

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

1.2. Príslušné oblasti politiky v rámci ABM/ABB

1.3. Druh návrhu/iniciatívy

1.4. Ciele

1.5. Dôvody návrhu/iniciatívy

1.6. Trvanie a finančný vplyv

1.7. Plánovaný spôsob riadenia

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

2.2. Systémy riadenia a kontroly

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušné okruhy viacročného finančného rámca a rozpočtové riadky výdavkov

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

3.2.2. Odhadovaný vplyv na operačné rozpočtové prostriedky

3.2.3. Odhadovaný vplyv na administratívne rozpočtové prostriedky

3.2.4. Súlad s platným viacročným finančným rámcom

3.2.5. Príspevky od tretích strán

3.3. Odhadovaný vplyv na príjmy

LEGISLATÍVNY FINANČNÝ VÝKAZ

1. RÁMEC NÁVRHU/INICIATÍVY

1.1. Názov návrhu/iniciatívy

Nariadenie, ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti

1.2. Príslušné oblasti politiky v rámci ABM/ABB[35]

Výskum a inovácia

Európske strategické investície

1.3. Druh návrhu/iniciatívy

☒ Návrh/iniciatíva sa týka **novej akcie**

☐ Návrh/iniciatíva sa týka **novej akcie, ktorá nadväzuje na pilotný projekt/prípravnú akciu**[36]

☐ Návrh/iniciatíva sa týka **predĺženia trvania existujúcej akcie**

☐ Návrh/iniciatíva sa týka **akcie presmerovanej na novú akciu**

1.4. Ciele

1.4.1. Viacročné strategické ciele Komisie, ktoré sú predmetom návrhu/iniciatívy

1. Prepojený digitálny jednotný trh

2. Ďalšie posilnenie zamestnanosti, rastu a investícií

1.4.2. Príslušné špecifické ciele

Špecifické ciele

1.3. Digitálne hospodárstvo môže plne využiť svoj potenciál na základe iniciatív, ktoré umožňujú plný rast digitálnych a dátových technológií.

2.1. Európa si zachováva postavenie svetového lídra v digitálnom hospodárstve, kde európske spoločnosti môžu globálne rásť, vychádzajúc zo silného digitálneho podnikania, fungujúcich startupov a využitia digitálnej transformácie v priemysle i verejných službách.

2.2. Európsky výskum nájde investičné príležitosti pre potenciálne prelomové technológie a hlavné iniciatívy, najmä z programov program Horizont 2020/Európsky horizont a s využitím verejno-súkromných partnerstiev.

[35] ABM: riadenie podľa činností – ABB: zostavovanie rozpočtu podľa činností.

[36] Podľa článku 54 ods. 2 písm. a) alebo b) nariadenia o rozpočtových pravidlách.

1.4.3. Očakávané výsledky a vplyv

Uveďte, aký vplyv by mal mať návrh/iniciatíva na prijímateľov/cieľové skupiny.

Kompetenčné centrum spolu so sieťou a komunitou sa budú snažiť dosiahnuť tieto ciele:

1. prispievať k vykonávaniu kyberneticko-bezpečnostnej zložky programu Digitálna Európa zriadeného nariadením XXX, a najmä akcií súvisiacich s článkom 6 nariadenia (EÚ) XXX [program Digitálna Európa], ako aj programu Európsky horizont zriadeného nariadením XXX, a najmä oddielu 2.2.6 prílohy I k rozhodnutiu XXX, ktorým sa zriaďuje špecifický program na vykonávanie programu Európsky horizont – rámcový program pre výskum a inovácie, ako aj ďalších programov Únie, ak sa tak stanoví v právnych aktoch Únie];

2. posilňovať kyberneticko-bezpečnostné spôsobilosti, znalosti a infraštruktúru k dispozícii jednotlivým odvetviam, verejnému sektoru a výskumnej obci;

3. prispievať k plošnému zavádzaniu najmodernejších kyberneticko-bezpečnostných produktov a riešení v celom hospodárstve;

4. zlepšovať chápanie kybernetickej bezpečnosti a prispievať k dopĺňaniu chýbajúcich zručností v Únii v oblasti kybernetickej bezpečnosti;

5. prispievať k posilňovaniu kyberneticko-bezpečnostného výskumu a vývoja v Únii;

6. posilniť spoluprácu medzi civilnou a obrannou sférou v oblasti technológií a aplikácií dvojakého použitia;

7. posilniť synergie medzi civilným a obranným rozmerom kybernetickej bezpečnosti;

8. pomáhať pri koordinácii a podporovať činnosti siete národných koordinačných centier (ďalej len „sieť“) uvedenej v článku 10 a komunity kyberneticko-bezpečnostných kompetencií uvedenej v článku 12.

1.4.4. Ukazovatele výsledkov a vplyvu

Uveďte ukazovatele, pomocou ktorých je možné sledovať uskutočňovanie návrhu/iniciatívy.

· Počet spoločne obstaraných kyberneticko-bezpečnostných infraštruktúr/nástrojov.

· Prístup európskych výskumníkov a odvetví v rámci siete a centra k možnostiam testovania a experimentovania. Ak už zariadenia existujú, zvýšený počet hodín dostupných pre tieto komunity v porovnaní s počtom hodín, ktoré sú v súčasnosti k dispozícii.

· Počet podporených skupín používateľov a počet výskumných pracovníkov, ktorí získali prístup k európskym zariadeniam kybernetickej bezpečnosti, sa zvyšuje v porovnaní s počtom tých, ktorí musia hľadať takéto zdroje mimo Európy.

· Konkurencieschopnosť európskych dodávateľov sa začína zvyšovať – z hľadiska podielu na celosvetovom trhu (cieľ je 25 % trhový podiel do roku 2027) a z hľadiska podielu európskych výskumných a vývojových výsledkov zavedených v priemysle.

· Prínos pre nové kyberneticko-bezpečnostné technológie meraný na základe autorských práv, patentov, vedeckých publikácií a komerčných produktov.

· Počet hodnotených a zosúladených plánov zručností v oblasti kybernetickej bezpečnosti, počet posudzovaných programov kyberneticko-bezpečnostnej profesionálnej certifikácie.

· Počet vyškolených vedcov, študentov, používateľov (z priemyslu a verejnej správy).

1.5. Dôvody návrhu/iniciatívy

1.5.1. Potreby, ktoré sa majú uspokojiť v krátkodobom alebo dlhodobom horizonte

Dosiahnuť kritický objem investícií do technologického a priemyselného vývoja v oblasti kybernetickej bezpečnosti a prekonať roztrieštenosť príslušných kapacít v celej EÚ.

1.5.2. Prínos zapojenia Európskej únie

Kybernetická bezpečnosť je otázkou spoločného záujmu Únie, ako sa potvrdzuje vo vyššie uvedených záveroch Rady. Dokazuje to aj rozsah a cezhraničný charakter incidentov ako WannaCry alebo NonPetya. Povaha a rozsah technologických výziev v oblasti kybernetickej bezpečnosti, ako aj nedostatočná koordinácia úsilia v rámci odvetvia, verejného sektora a výskumných komunít a medzi nimi si vyžadujú, aby EÚ ďalej podporovala úsilie o koordináciu s cieľom zhromaždiť kritické množstvo zdrojov a zabezpečiť lepšiu správu znalostí a aktív. Je to potrebné vzhľadom na požiadavky na zdroje pri určitých spôsobilostiach pre výskum, vývoj a zavádzanie v oblasti kybernetickej bezpečnosti; potrebu zabezpečiť prístup k interdisciplinárnemu know-how v oblasti kybernetickej bezpečnosti (ten je na vnútroštátnej úrovni často dostupný len čiastočne); globálny charakter odvetvových hodnotových reťazcov, ako aj činnosť svetových konkurentov pracujúcich na rôznych trhoch.

To si vyžaduje zdroje a odborné znalosti v rozsahu, ktorý sotva zodpovedá jednotlivým opatreniam ktoréhokoľvek členského štátu. Napríklad celoeurópska kvantová komunikačná sieť by mohla vyžadovať investície EÚ vo výške približne 900 miliónov EUR v závislosti od investícií členských štátov (ktoré sa majú prepojiť/doplniť) a od toho, do akej miery táto technológia umožní využitie existujúcich infraštruktúr.

1.5.3. Poznatky získané z podobných skúseností v minulosti

Aj v priebežnom hodnotení programu Horizont 2020 sa potvrdil pretrvávajúci význam podpory EÚ na výskum, vývoj a spoločenské výzvy (vrátane cieľa „bezpečné spoločnosti“, z ktorého sa podporuje kyberneticko-bezpečnostný výskum a vývoj). Zároveň sa v hodnotení potvrdzuje, že posilnenie vedúceho postavenia priemyslu je stále výzvou a že pretrváva inovačný deficit, pričom EÚ na poli prelomových trhových inovácií zaostáva.

Zdá sa, že hodnotenie Nástroja na prepájanie Európy (NPE) v polovici trvania potvrdzuje pridanú hodnotu intervencie EÚ nad rámec výskumu a vývoja, hoci kybernetická bezpečnosť v rámci NPE mala trochu iné zameranie (na prevádzkovú bezpečnosť) a intervenčnú logiku. Zároveň si väčšina príjemcov grantov z NPE v oblasti kybernetickej bezpečnosti – komunita vnútroštátnych jednotiek CSIRT – v nasledujúcom VFR želá osobitný program podpory.

Vytvorenie verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti v Únii v roku 2016 bolo výrazným prvým krokom k spájaniu komunít výskumu, priemyslu a verejného sektora s cieľom uľahčiť výskum a inovácie v oblasti

kybernetickej bezpečnosti, a v medziach finančného rámca na roky 2014 – 2020 by malo viesť k dobrým, cielenejším výsledkom vo výskume a inováciách. Toto verejno-súkromné partnerstvo umožnilo partnerom z odvetvia vyjadriť svoje záväzky týkajúce sa jednotlivých výdavkov na oblasti vymedzené v strategickom výskumnom a inovačnom programe partnerstva.

1.5.4. Zlučiteľnosť a možná synergia s inými vhodnými nástrojmi

Kompetenčná sieť kybernetickej bezpečnosti a Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti budú pôsobiť ako dodatočná podpora existujúcich politických ustanovení a aktérov na poli kybernetickej bezpečnosti. Mandát Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti bude dopĺňať úsilie agentúry ENISA, ale má iné zameranie a vyžaduje si odlišný súbor zručností. Hoci ENISA zohrá rolu z hľadiska poradenstva v oblasti kyberneticko-bezpečnostného výskumu a inovácie v EÚ, jej navrhovaný mandát sa v prvom rade zameriava na iné úlohy, ktoré sú rozhodujúce pre posilnenie odolnosti kybernetickej bezpečnosti v EÚ. Centrum by malo stimulovať vývoj a zavádzanie technológií v oblasti kybernetickej bezpečnosti a dopĺňať úsilie o budovanie kapacít v tejto oblasti na úrovni EÚ a na vnútroštátnej úrovni.

Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti spolu s kompetenčnou sieťou kybernetickej bezpečnosti bude takisto pracovať na podpore výskumu s cieľom uľahčiť a urýchliť procesy normalizácie a certifikácie, najmä v oblasti systémov certifikácie kybernetickej bezpečnosti v zmysle aktu o kybernetickej bezpečnosti.

Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti bude pôsobiť ako spoločný implementačný mechanizmus pre dva európske programy na podporu kybernetickej bezpečnosti (program Digitálna Európa a program Európsky horizont) a posilnenie koherentnosti a synergií medzi nimi.

Táto iniciatíva umožňuje doplniť úsilie členských štátov poskytovaním primeraných vstupov tvorcom politiky vzdelávania s cieľom posilniť vzdelávanie v oblasti kybernetickej bezpečnosti (napr. vypracovaním učebných osnov v oblasti kybernetickej bezpečnosti v civilných a vojenských vzdelávacích systémoch, ale aj v oblasti základného kyberneticko-bezpečnostného vzdelania). Zároveň by to umožnilo podporiť zosúladenie a nepretržité hodnotenie programov kyberneticko-bezpečnostnej profesionálnej certifikácie – všetky činnosti potrebné na preklenutie nedostatku zručností v oblasti kybernetickej bezpečnosti a na uľahčenie prístupu odvetvových a iných komunít k odborníkom v oblasti kybernetickej bezpečnosti. Zosúladenie vzdelávania a zručností prispeje k rozvoju kyberneticky-bezpečnostne kvalifikovanej pracovnej sily v EÚ, ktorá je kľúčovým aktívom pre spoločnosti pôsobiace v tejto oblasti, ale aj pre iné odvetvia, ktorých sa dotýka.

1.6. Trvanie a finančný vplyv

☒ Návrh/iniciatíva s **obmedzeným trvaním**

– ☒ Návrh/iniciatíva bude v platnosti od 1. 1. 2021 do 31. 12. 2029.

– ☒ Finančný vplyv na viazané rozpočtové prostriedky trvá od roku 2021 do roku 2027 a na platobné rozpočtové prostriedky od roku 2021 do roku 2031.

☐ Návrh/iniciatíva s **neobmedzeným trvaním**

– Počiatočná fáza implementácie bude trvať od RRRR do RRRR,

– a potom bude implementácia pokračovať v plnom rozsahu.

1.7. Plánovaný spôsob riadenia[37]

☐ **Priame riadenie** na úrovni Komisie

– ☐ prostredníctvom jej útvarov vrátane zamestnancov v delegáciách Únie

– ☐ prostredníctvom výkonných agentúr

☐ **Zdieľané riadenie** s členskými štátmi

☒

Nepriame riadenie s delegovaním úloh súvisiacich s plnením rozpočtu na:

– ☐ tretie krajiny alebo subjekty, ktoré tieto krajiny určili,

– ☐ medzinárodné organizácie a ich agentúry (uveďte),

– ☐ Európsku investičnú banku (EIB) a Európsky investičný fond,

– ☒ subjekty uvedené v článkoch 70 a 71 nariadenia o rozpočtových pravidlách,

– ☐ verejnoprávne subjekty,

– ☐ súkromnoprávne subjekty poverené vykonávaním verejnej služby, pokiaľ tieto subjekty poskytujú dostatočné finančné záruky,

– ☐ súkromnoprávne subjekty spravované právom členského štátu, ktoré sú poverené vykonávaním verejno-súkromného partnerstva a ktoré poskytujú dostatočné finančné záruky,

– ☐ osoby poverené vykonávaním osobitných činností v oblasti SZBP podľa hlavy V Zmluvy o Európskej únii a určené v príslušnom základnom akte.

– *V prípade viacerých spôsobov riadenia uveďte v oddiele „Poznámky“ presnejšie vysvetlenie.*

[37] Vysvetlenie spôsobov riadenia a odkazy na nariadenie o rozpočtových pravidlách sú k dispozícii na webovej stránke BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. OPATRENIA V OBLASTI RIADENIA

2.1. Opatrenia týkajúce sa monitorovania a predkladania správ

Uveďte časový interval a podmienky, ktoré sa vzťahujú na tieto opatrenia.

Podrobné ustanovenia o monitorovaní a podávaní správ obsahuje článok 28.

2.2. Systémy riadenia a kontroly

2.2.1. Zistené riziká

Na zmiernenie rizík súvisiacich s prevádzkou kompetenčného centra po jeho zriadení a so zdržaniami Komisia v tejto fáze kompetenčné centrum podporí, aby sa zabezpečilo rýchle prijímanie kľúčových pracovníkov a zavedenie efektívneho systému vnútornej kontroly a náležitých postupov.

2.2.2. Údaje o zavedenom systéme vnútornej kontroly

Výkonný riaditeľ zodpovedá za prevádzku a každodenné riadenie kompetenčného centra a je jeho právnym zástupcom. Riaditeľ sa zodpovedá správnej rade a priebežne ju informuje o vývoji činností kompetenčného centra.

Správna rada nesie celkovú zodpovednosť za strategické zameranie a prevádzku kompetenčného centra a vykonáva dohľad nad realizáciou jeho činností.

Finančné pravidlá uplatniteľné na kompetenčné centrum prijíma správna rada po porade s Komisiou. Nesmú sa odchyľovať od nariadenia (EÚ) č. 1271/2013, pokiaľ si takúto odchýlku osobitne nevyžaduje prevádzka kompetenčného centra a Komisia vopred neudelila súhlas.

Vnútorný audítor Komisie má vo vzťahu ku kompetenčnému centru rovnaké právomoci, aké má vo vzťahu ku Komisii. Dvor audítorov má právomoc vykonávať na základe dokumentov a na mieste audit u všetkých príjemcov grantov, dodávateľov a subdodávateľov, ktorým boli poskytnuté finančné prostriedky Únie z kompetenčného centra.

2.2.3. Odhad nákladov a prínosov kontrol a posúdenie očakávanej úrovne rizika chyby

Náklady a prínosy kontrol

Náklady na kontrolu v rámci Európskeho centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti sa delia medzi náklady na dohľad na úrovni Komisie a prevádzkové kontroly nákladov na úrovni implementujúceho orgánu.

Náklady na kontroly na úrovni kompetenčného centra sa odhadujú približne na 1,19 % operačných platobných rozpočtových prostriedkov vynaložených na úrovni kompetenčného centra.

Náklady na dohľad na úrovni Komisie sa odhadujú na 1,20 % operačných platobných rozpočtových prostriedkov vynaložených na úrovni kompetenčného centra.

Ak by činnosti v plnom rozsahu riadila Komisia bez podpory implementujúceho orgánu, náklady na kontrolu by boli podstatne vyššie a mohli by predstavovať približne 7,7 % platobných rozpočtových prostriedkov.

Cieľom plánovaných kontrol je zabezpečiť bezproblémový a účinný dohľad nad vykonávacími subjektmi zo strany Komisie a zabezpečiť potrebný stupeň uistenia na úrovni Komisie.

Prínosy kontrol:

– zabránenie výberu slabších alebo neprimeraných návrhov,

– optimalizácia plánovania a využívania finančných prostriedkov EÚ na zachovanie pridanej hodnoty EÚ,

– zabezpečenie kvality dohôd o grantoch, predchádzanie chybám pri identifikácii právnych subjektov, zabezpečenie správneho výpočtu príspevkov EÚ a prijatie potrebných záruk na správne fungovanie grantov,

– zistenie neoprávnených nákladov vo fáze platby,

– zistenie chýb, ktoré ovplyvňujú zákonnosť a regulárnosť operácií vo fáze auditu.

Odhadovaná chybovosť

Cieľom je udržať zvyškovú chybovosť za celý program pod hranicou 2 %, a pritom obmedziť zaťaženie príjemcov kontrolami s cieľom dosiahnuť správne vyváženie cieľa zákonnosti a regulárnosti s ostatnými cieľmi, ako je atraktívnosť programu, najmä pre MSP, a náklady na kontroly.

2.3. Opatrenia na predchádzanie podvodom a nezrovnalostiam

Uveďte existujúce a plánované preventívne a ochranné opatrenia.

Úrad OLAF môže vykonávať vyšetrovania vrátane kontrol a inšpekcií na mieste v súlade s ustanoveniami a postupmi stanovenými v nariadení Európskeho parlamentu a Rady (ES) č. 883/2013 a nariadení Rady (Euratom, ES) č. 2185/9640 z 11. novembra 1996 o kontrolách a inšpekciách na mieste, vykonávaných Komisiou s cieľom ochrany finančných záujmov Únie pred spreneverou a inými podvodmi s úmyslom zistiť, či v súvislosti s grantom alebo zmluvou financovanou kompetenčným centrom nedošlo k podvodu, korupcii alebo akémukoľvek inému protiprávnemu konaniu poškodzujúcemu finančné záujmy Únie.

Dohody, rozhodnutia a zmluvy vyplývajúce z vykonávania tohto nariadenia musia obsahovať ustanovenia, ktorými sa výslovne udeľuje Komisii, kompetenčnému centru, Dvoru audítorov a úradu OLAF právomoc na vykonávanie auditov a vyšetrovaní v súlade s ich príslušnými právomocami.

Kompetenčné centrum zabezpečí, aby sa finančné záujmy jeho členov primerane chránili vykonávaním alebo zadávaním náležitých interných a externých kontrol.

Kompetenčné centrum pristúpi k medziinštitucionálnej dohode z 25. mája 1999 medzi Európskym parlamentom, Radou Európskej únie a Komisiou Európskych spoločenstiev, ktorá sa týka vnútorných vyšetrovaní vykonávaných Európskym úradom pre boj proti podvodom (OLAF). Kompetenčné centrum prijme potrebné opatrenia na uľahčenie vnútorných vyšetrovaní vykonávaných úradom OLAF.

Kompetenčné centrum prijme stratégiu boja proti podvodom na základe analýzy rizika podvodu a posúdenia nákladov a prínosov. Bude chrániť finančné záujmy Únie uplatňovaním preventívnych opatrení na zamedzenie podvodom, korupcii a iným protiprávnym činnostiam, účinnými kontrolami, vymáhaním neoprávnene vyplatených súm pri odhalení nezrovnalostí a v prípade potreby aj ukladaním účinných, primeraných a odrádzajúcich administratívnych a finančných sankcií.

3. ODHADOVANÝ FINANČNÝ VPLYV NÁVRHU/INICIATÍVY

3.1. Príslušný okruh viacročného finančného rámca a navrhované rozpočtové riadky výdavkov

- Požadované nové rozpočtové riadky

V poradí, v akom za sebou nasledujú okruhy viacročného finančného rámca a rozpočtové riadky:

Okruh viacročného finančného rámca	Rozpočtový riadok	Druh výdavkov	Príspevky			
	Číslo	DRP/NRP[38].	krajín EZVO[39]	kandidátskych krajín[40]	tretích krajín	v zmysle článku [21 ods. 2 písm. b)] nariadenia o rozpočtových pravidlách
Okruh 1: Jednotný trh, inovácie a digitálna ekonomika	01 02 XX XX Európsky horizont Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti – podporné výdavky 01 02 XX XX Európsky horizont Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti 02 06 01 XX program Digitálna Európa Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti – podporné výdavky 02 06 01 XX program Digitálna Európa Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti	DRP	ÁNO	ÁNO (ak sa uvádza v ročnom pracovnom programe)	ÁNO (obmedzené na niektoré časti programu)	NIE

[38] DRP = diferencované rozpočtové prostriedky / NRP = nediferencované rozpočtové prostriedky.
[39] EZVO: Európske združenie voľného obchodu.
[40] Kandidátske krajiny a prípadne potenciálni kandidáti zo západného Balkánu.

- Očakáva sa, že príspevky na tieto rozpočtové riadky budú pochádzať z:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok	Rok 2021	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**Spolu**
01 01 01 01 Výdavky vzťahujúce sa na dočasných zamestnancov v oblasti výskumu – Európsky horizont	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Externí zamestnanci implementujúci výskumné programy – Európsky horizont	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Ostatné výdavky na riadenie v oblasti výskumu – Európsky horizont	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globálne výzvy a konkurencieschopnosť priemyslu	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Administratívna podpora – program Digitálna Európa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Kybernetická bezpečnosť – Program Digitálna Európa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Výdavky spolu	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Príspevok z finančného krytia klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 21 ods. 1 písm. b) navrhne Komisia počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody. Návrh bude vychádzať z výsledkov procesu strategického plánovania vymedzeného v článku 6 ods. 6 nariadenia XXX [rámcový program Európsky horizont].

Uvedené sumy nezahŕňajú príspevok členských štátov na prevádzkové a administratívne náklady kompetenčného centra, ktorý zodpovedá finančnému príspevku Únie.

3.2. Odhadovaný vplyv na výdavky

3.2.1. Zhrnutie odhadovaného vplyvu na výdavky

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Okruh viacročného finančného rámca	**1**	Jednotný trh, inovácie a digitálna ekonomika

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***po roku 2027***	**SPOLU**
Hlava 1 (výdavky na zamestnancov)	Záväzky = Platby	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Hlava 2 (infraštruktúra a prevádzkové výdavky)	Záväzky = Platby	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Hlava 3 (operačné výdavky)	Záväzky	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	Platby	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
Rozpočtové prostriedky na finančné krytie programov SPOLU[42]	Záväzky	= 1 + 2 + 3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**
	Platby	= 1 + 2 + 4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

41 Rozpočtové prostriedky na zamestnancov sú v roku 2021 účtované len na pol roka.

42 Uvedené finančné krytie sa týka len finančných zdrojov EÚ vyhradených na kybernetickú bezpečnosť v rámci programu Digitálna Európa. Príspevok z finančného krytia klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 5 ods. 1 písm. b) navrhne Komisia počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody. Návrh bude vychádzať z výsledkov procesu strategického plánovania vymedzeného v článku 6 ods. 6 nariadenia XXX [rámcový program Európsky horizont].

Okruh viacročného finančného rámca	7	„Administratívne výdavky“

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***po roku 2027***	**SPOLU**
Ľudské zdroje		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Ostatné administratívne výdavky		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
Rozpočtové prostriedky OKRUHU 7 viacročného finančného rámca SPOLU	(Záväzky spolu = Platby spolu)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***po roku 2027***	**SPOLU**
Rozpočtové prostriedky OKRUHOV viacročného finančného rámca **SPOLU**	Záväzky	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	Platby	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 ²061,715**	**2 005,637**

3.2.2. Zhrnutie odhadovaného vplyvu na administratívne rozpočtové prostriedky

– ☐ Návrh/iniciatíva si nevyžaduje použitie administratívnych rozpočtových prostriedkov.

– ☒ Návrh/iniciatíva si vyžaduje použitie administratívnych rozpočtových prostriedkov, ako je uvedené v nasledujúcej tabuľke:

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rok	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**SPOLU**
OKRUH 7 viacročného finančného rámca								
Ľudské zdroje	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Ostatné administratívne výdavky	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Medzisúčet OKRUHU 7 viacročného finančného rámca	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Mimo OKRUHU 7[43] viacročného finančného rámca								
Ľudské zdroje								
Ostatné administratívne výdavky	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Medzisúčet mimo OKRUHU 7 viacročného finančného rámca	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

SPOLU	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky budú pokryté rozpočtovými prostriedkami GR, ktoré už boli pridelené na riadenie akcie a/alebo boli prerozdelené v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov a v závislosti od rozpočtových obmedzení.

Uvedené rozpočtové prostriedky potrebné na ľudské zdroje a ostatné administratívne výdavky mimo okruhu 7 zodpovedajú sumám, na ktoré sa vzťahuje finančný príspevok Únie z programu Digitálna Európa.

Rozpočtové prostriedky potrebné na ľudské zdroje a na ostatné administratívne výdavky mimo okruhu 7 sa zvýšia o sumy pokryté finančným príspevkom Únie z programu Európsky horizont, keď Komisia navrhne príspevok z finančného krytia klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 21 ods. 1 písm. b) počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody.

[43] Technická a/alebo administratívna pomoc a výdavky určené na financovanie implementácie programov a/alebo akcií Európskej únie (pôvodné rozpočtové riadky „BA“), nepriamy výskum, priamy výskum.

Uvedené sumy rozpočtových prostriedkov, ktoré sú potrebné na ľudské zdroje a na ostatné administratívne výdavky mimo okruhu 7, nezahŕňajú príspevok členských štátov na administratívne náklady kompetenčného centra, ktorý zodpovedá finančnému príspevku Únie.

3.2.2.1. Odhadované potreby ľudských zdrojov v Komisii

– ☐ Návrh/iniciatíva si nevyžaduje použitie ľudských zdrojov.

– ■ Návrh/iniciatíva si vyžaduje použitie ľudských zdrojov, ako je uvedené v nasledujúcej tabuľke:

odhady sa vyjadrujú v jednotkách ekvivalentu plného pracovného času

Rok		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Plán pracovných miest (úradníci a dočasní zamestnanci)								
Ústredie a zastúpenia Komisie		20	21	21	21	21	21	22
Delegácie								
Výskum								
• Externí zamestnanci (ekvivalent plného pracovného času) – ZZ, MZ, VNE, DAZ a PED [44] Okruh 7								
Financované z OKRUHU 7 viacročného finančného rámca	– ústredie	3	3	3	3	3	3	3
	– delegácie							
Financované z balíka prostriedkov určených na implementáciu programu [45]	– ústredie							
	– delegácie							
Výskum								
Iné (uveďte)								
SPOLU		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Potreby ľudských zdrojov budú pokryté úradníkmi GR, ktorí už boli pridelení na riadenie akcie a/alebo boli interne prerozdelení v rámci GR, a v prípade potreby budú doplnené zdrojmi, ktoré sa môžu prideliť riadiacemu GR v rámci ročného postupu prideľovania zdrojov v závislosti od rozpočtových obmedzení.

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	Koordinácia, monitorovanie a riadenie úloh zverených Európskemu centru odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti vrátane nákladov na podporu a koordináciu. Rozvoj politiky a koordinácia v oblasti kybernetickej bezpečnosti v súvislosti s úlohami zverenými Európskemu centru odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti, napr. so zreteľom na stanovovanie priorít pre výskumnú a priemyselnú politiku, všeobecnú spoluprácu medzi členskými štátmi a hospodárskymi subjektmi, konzistentnosť s budúcim rámcom kybernetickobezpečnostnej certifikácie EÚ, otázky zodpovednosti a náležitej starostlivosti alebo koordináciu s politikami týkajúcimi sa vysokovýkonnej výpočtovej techniky, umelej inteligencie a digitálnych zručností. .
Externí zamestnanci	Koordinácia, monitorovanie a riadenie úloh zverených Európskemu centru odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti vrátane

[44] ZZ = zmluvný zamestnanec; MZ = miestny zamestnanec; VNE = vyslaný národný expert; DAZ = dočasný agentúrny zamestnanec; PED = pomocný expert v delegácii.

[45] Čiastkový strop pre externých zamestnancov financovaných z operačných rozpočtových prostriedkov (pôvodné rozpočtové riadky „BA“).

	nákladov na podporu a koordináciu. Rozvoj politiky a koordinácia v oblasti kybernetickej bezpečnosti v súvislosti s úlohami zverenými Európskemu centru odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti, napr. so zreteľom na stanovovanie priorít pre výskumnú a priemyselnú politiku, všeobecnú spoluprácu medzi členskými štátmi a hospodárskymi subjektmi, konzistentnosť s budúcim rámcom kybernetickobezpečnostnej certifikácie EÚ, otázky zodpovednosti a náležitej starostlivosti alebo koordináciu s politikami týkajúcimi sa vysokovýkonnej výpočtovej techniky, umelej inteligencie a digitálnych zručností. .

3.2.2.2. Odhadované potreby ľudských zdrojov v centre odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti

	2021	2022	2023	2024	2025	2026	2027
Úradníci Komisie							
Z toho AD							
Z toho AST							
Z toho AST-SC							
Dočasní zamestnanci							
Z toho AD	10	11	13	13	13	13	13
Z toho AST							
Z toho AST-SC							
Zmluvní zamestnanci	26	32	39	39	39	39	39
VNE	1	1	1	1	1	1	1
Spolu	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Opis úloh, ktoré sa majú vykonať:

Úradníci a dočasní zamestnanci	Operačný výkon úloh zverených Európskemu centru odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti v zmysle článku 4 tohto nariadenia vrátane nákladov na podporu a koordináciu.
Externí zamestnanci	Operačný výkon úloh zverených Európskemu centru odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti v zmysle článku 4 tohto nariadenia vrátane nákladov na podporu a koordináciu.

Uvedené odhadované požiadavky na ľudské zdroje v centre odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti zodpovedajú odhadovaným požiadavkám na implementáciu finančného príspevku Únie v rámci programu Digitálna Európa.

Uvedené odhadované požiadavky na ľudské zdroje v centre odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti sa zvýšia na základe odhadovaných požiadaviek na čerpanie finančného príspevku Únie v rámci programu Európsky horizont, keď Komisia navrhne príspevok z finančného krytia klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 21 ods. 1 písm. b) počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody.

3.2.2.3. Plán pracovných miest centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti

Funkčná skupina a trieda	2021	2022	2023	2024	2025	2025	2025

AD 16							
AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD spolu	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST spolu							
AST/SC 6							
AST/SC 5							
AST/SC 4							

AST/SC 3							
AST/SC 2							
AST/SC 1							
AST/SC spolu							
CELKOVÝ SÚČET	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Odhadovaný vplyv na zamestnancov (dodatočný) – externí zamestnanci centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti

Zmluvní zamestnanci	2021	2022	2023	2024	2025	2026	2027
Funkčná skupina IV	20	22	29	29	29	29	29
Funkčná skupina III	2	4	4	4	4	4	4
Funkčná skupina II	4	6	6	6	6	6	6
Funkčná skupina I							
Spolu	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Na zabezpečenie neutrality počtu zamestnancov sa dodatočné personálne obsadenie v centre odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti bude čiastočne kompenzovať znížením počtu úradníkov a externých zamestnancov (t. j. v súčasnosti platného plánu pracovných miest a externých zamestnancov) v relevantných útvaroch Komisie.

Počet zamestnancov centra odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti v bodoch 3.2.2.2 až 4 sa bude kompenzovať takto[46]:

SPOLU	2021	2022	2023	2024	2025	2026	2027
Úradníci Komisie	5	5	6	6	6	6	6
Dočasní zamestnanci							
Zmluvní zamestnanci	14	17	20	20	20	20	20
VNE							
Celkový počet ekvivalentov plného pracovného času	19	22	26	26	26	26	26

[46] Podľa konečnej sumy rozpočtu, ktorej plnenie bude delegované na kompetenčné centrum

Počet pracovníkov	19	22	26	26	26	26	26

Kompenzácia ľudských zdrojov v centre odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti bude úmerná podielu finančného príspevku Únie, t. j. 50 %.

Uvedená kompenzácia sa týka odhadovaných požiadaviek na ľudské zdroje v centre odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti na implementáciu finančného príspevku Únie z programu Digitálna Európa.

Uvedená kompenzácia sa zvýši na základe odhadovaných požiadaviek na čerpanie finančného príspevku Únie v rámci programu Európsky horizont, keď Komisia navrhne príspevok z finančného krytia klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 21 ods. 1 písm. b) počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody.

3.2.3. Príspevky od tretích strán

Návrh/iniciatíva:

– ☐ nestanovuje spolufinancovanie tretími stranami

– ☒ stanovuje spolufinancovanie tretími stranami[47] odhadnuté ďalej v texte:

rozpočtové prostriedky v mil. EUR (zaokrúhlené na tri desatinné miesta)

Rok	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**SPOLU**
Členské štáty – príspevok na výdavky na zamestnancov	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Členské štáty – príspevok na infraštruktúru a prevádzkové výdavky	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Členské štáty – príspevok na operačné výdavky	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Prostriedky zo spolufinancovania SPOLU	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Uvedený príspevok tretích strán sa vzťahuje iba na spolufinancovanie zodpovedajúce finančným zdrojom EÚ vyhradeným na kybernetickú bezpečnosť v rámci programu Digitálna Európa. Uvedený príspevok tretích strán sa zvýši, keď Komisia navrhne finančný príspevok z klastra „Inkluzívna a bezpečná spoločnosť“ II. piliera „Globálne výzvy a konkurencieschopnosť priemyslu“ programu Európsky horizont (celková suma krytia je 2 800 000 000 EUR) uvedený v článku 21 ods. 1 písm. b) počas legislatívneho procesu a v každom prípade pred dosiahnutím politickej dohody. Návrh bude vychádzať z výsledkov procesu strategického plánovania vymedzeného v článku 6 ods. 6 nariadenia XXX [rámcový program Európsky horizont].

3.3. Odhadovaný vplyv na príjmy

– ☒ Návrh/iniciatíva nemá finančný vplyv na príjmy.

– ☐ Návrh/iniciatíva má finančný vplyv na príjmy, ako je uvedené v nasledujúcej tabuľke:

☐ vplyv na vlastné zdroje

☐ vplyv na iné príjmy

uveďte, či sú príjmy pripísané rozpočtovým riadkom výdavkov ☐

v mil. EUR (zaokrúhlené na 3 desatinné miesta)

Rozpočtový riadok príjmov:	Vplyv návrhu/iniciatívy[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**

[47] Odhadovaný nepeňažný príspevok členských štátov.

[48] Pokiaľ ide o tradičné vlastné zdroje (clá, odvody z produkcie cukru), uvedené sumy musia predstavovať čisté sumy, t. j. hrubé sumy po odčítaní 20 % na náklady na výber.

Článok …….							

V prípade pripísaných príjmov uveďte príslušné rozpočtové riadky výdavkov.

Ďalšie poznámky (napr. spôsob/vzorec použitý na výpočet vplyvu na príjmy alebo akékoľvek ďalšie informácie).