

Brusel 14. září 2018
(OR. en)

12104/18

Interinstitucionální spis:
2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

PRŮVODNÍ POZNÁMKA

Odesílatel:	Jordi AYET PUIGARNAU, ředitel, za generálního tajemníka Evropské komise
Datum přijetí:	12. září 2018
Příjemce:	Jeppe TRANHOLM-MIKKELSEN, generální tajemník Rady Evropské unie
Č. dok. Komise:	COM(2018) 630 final
Předmět:	Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center

Delegace naleznou v příloze dokument COM(2018) 630 final.

Příloha: COM(2018) 630 final



EVROPSKÁ
KOMISE

V Bruselu dne 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

**kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí
pro kybernetickou bezpečnost a síť národních koordinačních center**

*Příspěvek Evropské komise k zasedání vedoucích představitelů
v Salcburku ve dnech 19.–20. září 2018*

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

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

• Odůvodnění a cíle návrhu

Jak se naše každodenní životy a ekonomiky stávají závislejší na digitálních technologiích, jsou občané čím dál více vystaveni závažným kybernetickým incidentům. Budoucí bezpečnost závisí na zlepšování schopností chránit Unii před kybernetickými hrozbami, jelikož o bezpečné digitální systémy se opírá jak civilní infrastruktura, tak i vojenské schopnosti.

S cílem čelit rostoucím výzvám Unie neustále zintenzivňuje svoje činnosti v této oblasti, přičemž vychází ze strategie kybernetické bezpečnosti z roku 2013¹ a jejích cílů a zásad, totiž podporovat spolehlivý, bezpečný a otevřený kybernetický ekosystém. V roce 2016 Unie přijala první opatření v oblasti kybernetické bezpečnosti prostřednictvím směrnice Evropského parlamentu a Rady (EU) 2016/1148² o bezpečnosti sítí a informačních systémů.

Vzhledem k rychlému vývoji v oblasti kybernetické bezpečnosti představily Komise a Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku v září 2017 společné sdělení³ nazvané „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“ s cílem dále posílit odolnost, odrazování a reakci Unie v souvislosti s kybernetickými útoky. V uvedeném společném sdělení, které rovněž vychází z předchozích iniciativ, je nastíněn soubor navrhovaných opatření, mimo jiné posílení Agentury Evropské unie pro bezpečnost sítí a informací (ENISA), vytvoření dobrovolného celounijního rámce pro certifikaci kybernetické bezpečnosti za účelem zvýšení kybernetické bezpečnosti produktů a služeb v digitálním světě, jakož i plán na rychlou a koordinovanou reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize.

Ve společném sdělení se uznává, že je též strategickým zájmem Unie zajistit, aby si udržela a rozvíjela důležité technické kapacity v oblasti kybernetické bezpečnosti, aby mohla zajistit bezpečnost svého jednotného digitálního trhu a zejména chránit kritické sítě a informační systémy a poskytovat klíčové služby v oblasti kybernetické bezpečnosti. Unie musí být schopna sama zabezpečit svá digitální aktiva a být konkurenceschopná na celosvětovém trhu kybernetické bezpečnosti.

V současné době je Unie čistým dovozcem produktů a řešení v oblasti kybernetické bezpečnosti a je do velké míry závislá na neevropských dodavatelích⁴. Trh kybernetické bezpečnosti celosvětově dosahuje 600 miliard EUR a předpokládá se, že v příštích pěti letech poroste přibližně o 17 %, pokud jde o objem prodeje, počet společností a zaměstnanost. Z tržního pohledu je však mezi dvaceti předními zeměmi v oblasti kybernetické bezpečnosti pouze šest členských států EU⁵.

¹ SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ: Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, JOIN(2013) 1 final.

² Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

³ SPOLEČNÉ SDĚLENÍ EVROPSKÉMU PARLAMENTU A RADĚ: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“, JOIN(2017) 450 final.

⁴ Návrh závěrečné zprávy o studii trhu kybernetické bezpečnosti, 2018.

⁵ Návrh závěrečné zprávy o studii trhu kybernetické bezpečnosti, 2018.

Zároveň ale Unie disponuje bohatými odbornými znalostmi a zkušenostmi v oblasti kybernetické bezpečnosti – do nedávného mapování odborných středisek v oblasti kybernetické bezpečnosti provedeného Komisí se přihlásilo více než 660 organizací z celé EU⁶. Pokud budou tyto odborné znalosti přeměněny v produkty a řešení uplatnitelné na trhu, mohla by být Unie schopna pokrýt celý hodnotový řetězec kybernetické bezpečnosti. Avšak snahy výzkumných a průmyslových komunit jsou roztržštěné, nedostatečně propojené a chybí jim společný cíl, čímž je omezena konkurenceschopnost EU v této oblasti i její schopnost zabezpečit svá digitální aktiva. Příslušným odvětvím kybernetické bezpečnosti (jako jsou energetika, vesmír, obrana, doprava) a dílčím odvětvím se dnes nedostává dostatečné podpory⁷. V Evropě dále nejsou plně využívány možnosti, které nabízejí synergie mezi civilními a obrannými odvětvími kybernetické bezpečnosti.

Vytvoření smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost v Unii v roce 2016 bylo prvním významným krokem pro větší propojení výzkumných komunit, průmyslu a veřejného sektoru v zájmu usnadnění výzkumu a inovací v oblasti kybernetické bezpečnosti a v mezích daných finančním rámcem na roky 2014–2020 by mělo vést k dobrým a lépe cíleným výsledkům v oblasti výzkumu a inovací. Uvedené partnerství umožnilo průmyslovým partnerům vyjádřit závazek o jejich individuálních výdajích v oblastech vymezených v jeho programu strategického výzkumu a inovací.

Unie však může usilovat o daleko rozsáhlejší investice a potřebuje efektivnější mechanismus, který by vytvořil dlouhotrvající kapacity, spojil úsilí a kompetence a stimuloval rozvoj inovativních řešení, která by byla schopna reagovat na výzvy v průmyslových odvětvích související s kybernetickou bezpečností v oblasti nových víceúčelových technologií (např. umělá inteligence, kvantová výpočetní technika, technologie blockchain a bezpečné digitální identity) a v kritických odvětvích (např. doprava, energetika, zdravotnictví, finančnictví, státní správa, telekomunikace, výroba, obrana, vesmír).

Ve společném sdělení byla zvažována možnost posílit schopnosti Unie v oblasti kybernetické bezpečnosti prostřednictvím sítě odborných středisek v oblasti kybernetické bezpečnosti, jejímž ústředním prvkem by bylo Evropské výzkumné a odborné středisko pro kybernetickou bezpečnost. Tím by se doplnilo stávající úsilí zaměřené na budování kapacit v této oblasti na úrovni Unie a na vnitrostátní úrovni. Ve společném sdělení byl vyjádřen záměr Komise zahájit v roce 2018 posouzení dopadů za účelem prozkoumání dostupných možností s cílem vytvořit tuto strukturu. Komise jako první krok a v zájmu získání informací pro budoucí úvahy zahájila v rámci programu Horizont 2020 pilotní fázi, která pomůže zapojit národní centra do sítě, a dodat tak nový impuls rozvoji kompetencí a technologií v oblasti kybernetické bezpečnosti.

V září 2017 hlavy států a předsedové vlád vyzvali na Tallinnském summitu k digitální problematice, že je třeba z Unie „do roku 2025 učinit vedoucí sílu v oblasti kybernetické bezpečnosti, abychom zajistili důvěru, jistotu a ochranu našich občanů, spotřebitelů a podniků online a umožnili svobodný internet respektující právo.“

⁶ Technické zprávy JRC: *European Cybersecurity Centres of Expertise* (Evropská odborná střediska pro kybernetickou bezpečnost), 2018.

⁷ Technická zpráva JRC: *Outcomes of the Mapping Exercise* (Výsledky mapování; podrobnosti viz přílohy 4 a 5).

V závěrech Rady⁸ přijatých v listopadu 2017 byla Komise vyzvána, aby urychleně zajistila posouzení dopadů různých možností a do poloviny roku 2018 navrhla příslušný právní nástroj pro provedení iniciativy.

Cílem *programu Digitální Evropa, který Komise předložila v červnu 2018*⁹, je rozšířit a maximalizovat výhody digitální transformace pro evropské občany a podniky ve všech příslušných oblastech politik EU, posílit tyto politiky a podporovat cíle jednotného digitálního trhu. Program navrhuje soudržný a jednotný přístup k zajištění nejlepšího využití pokročilých technologií a správnou kombinaci technických kapacit a lidských kompetencí pro digitální transformaci, a to nejenom v oblasti kybernetické bezpečnosti, ale také s ohledem na inteligentní datovou infrastrukturu, umělou inteligenci, pokročilé dovednosti a použití v průmyslu a v oblastech veřejného zájmu. Tyto prvky jsou na sobě závislé, vzájemně se posilují a budou-li podporovány současně, pak lze dosáhnout nezbytného rozsahu pro prosperující ekonomiku založenou na datech¹⁰. *Program Horizont Evropa*¹¹ – příští rámcový program EU pro výzkum a inovace – rovněž považuje kybernetickou bezpečnost za jednu z priorit.

V uvedeném kontextu toto nařízení navrhuje zřízení Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center. Tento model spolupráce vytvořený pro konkrétní účel by měl fungovat dále popsaným způsobem, a tak stimulovat evropský technologický a průmyslový ekosystém v oblasti kybernetické bezpečnosti: Kompetenční centrum usnadní a pomůže koordinovat práci sítě a bude podporovat komunitu kompetencí pro kybernetickou bezpečnost, aktivně prosazovat agendu technologií kybernetické bezpečnosti a usnadňovat přístup k takto shromážděným odborným znalostem. Za tímto účelem bude kompetenční centrum zejména provádět příslušné části programů Digitální Evropa a Horizont Evropa, a to přidělováním grantů a zadáváním veřejných zakázek. S ohledem na značné investice do kybernetické bezpečnosti vynakládané v jiných částech světa a na potřebu koordinovat a sdružit v Evropě příslušné prostředky je navrhovanou formou kompetenčního centra evropské partnerství¹², čímž se usnadní společné investice ze strany Unie, členských států a/nebo průmyslu. Návrh proto vyžaduje, aby členské státy přispěly na akce kompetenčního centra a sítě souměřitelnou částkou. Hlavním rozhodovacím orgánem je správní rada, v níž jsou zastoupeny všechny členské státy, ale hlasovací práva mají pouze členské státy, které se účastní finančně. Mechanismus hlasování ve správní radě se řídí zásadou dvojí většiny, která vyžaduje 75 % finančních příspěvků a 75 % hlasů. Komise, vzhledem ke své odpovědnosti za rozpočet Unie, má 50 % hlasů. Pro svou práci ve správní radě Komise v příslušných případech využije know-how Evropské služby pro vnější činnost. Správní radě je nápomocna průmyslová a vědecká poradní rada, která zajišťuje pravidelný dialog se soukromým sektorem, organizacemi spotřebitelů a dalšími relevantními zúčastněnými stranami.

⁸ Závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, přijaté Radou pro obecné záležitosti dne 20. listopadu 2017.

⁹ COM(2018) 434 Návrh nařízení Evropského parlamentu a Rady, kterým se zavádí program Digitální Evropa na období 2021–2027.

¹⁰ Viz SWD (2018) 305.

¹¹ COM(2018) 435 Návrh nařízení Evropského parlamentu a Rady, kterým se zavádí rámcový program pro výzkum a inovace Horizont Evropa a stanoví pravidla pro účast a šíření výsledků.

¹² Dle definice v návrhu nařízení Evropského parlamentu a Rady, kterým se zavádí rámcový program pro výzkum a inovace Horizont Evropa a stanoví pravidla pro účast a šíření výsledků, COM(2018) 435, a odkazu v návrhu nařízení Evropského parlamentu a Rady, kterým se zavádí program Digitální Evropa na období 2021–2027, COM(2018) 434.

Na základě úzké spolupráce se sítí národních koordinačních center a komunitou kompetencí pro kybernetickou bezpečnost (do níž je zapojeno velké množství různých hráčů zabývajících se vývojem technologií kybernetické bezpečnosti, například výzkumné subjekty, průmyslová odvětví působící na straně dodávky a na straně poptávky a veřejný sektor) zavedenými tímto nařízením by Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost bylo hlavním prováděcím subjektem pro finanční prostředky EU určené na kybernetickou bezpečnost v rámci navrhovaného programu *Digitální Evropa* a programu *Horizont Evropa*.

Takový komplexní přístup by umožnil podporovat kybernetickou bezpečnost v rámci celého hodnotového řetězce, od výzkumu přes podporu nasazení po šíření klíčových technologií. Finanční účast členských států by měla být souměřitelná s finančním příspěvkem EU na tuto iniciativu a je nezbytným předpokladem úspěchu.

Evropská organizace pro kybernetickou bezpečnost, která je protějškem Komise ve smluvním partnerství veřejného a soukromého sektoru o kybernetické bezpečnosti v rámci programu Horizont 2020, by s ohledem na své konkrétní odborné znalosti a široké a vhodné zastoupení zúčastněných stran měla být přizvána, aby přispěla k činnostem centra a sítě.

Dále by Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost mělo usilovat o posílení synergie mezi civilním a obranným rozměrem kybernetické bezpečnosti. Členským státům a dalším příslušným hráčům by mělo nabízet podporu poskytováním poradenství, sdílením odborných znalostí a usnadňováním spolupráce v souvislosti s projekty a akcemi. Bude-li o to požádáno členskými státy, mohlo by rovněž působit jako projektový manažer, zejména v souvislosti s Evropským obranným fondem. Cílem předkládané iniciativy je přispět k řešení následujících problémů:

- **Nedostatečná spolupráce mezi průmyslovými odvětvími na straně poptávky a na straně nabídky.** Evropské podniky čelí dvojí výzvě – zajistit si vlastní bezpečnost a nabízet bezpečné produkty a služby svým zákazníkům. Avšak často nejsou schopny vhodně zabezpečit své stávající produkty, služby a aktiva, nebo navrhnout bezpečné inovativní produkty a služby. Klíčová aktiva v oblasti kybernetické bezpečnosti jsou mnohdy příliš nákladná na to, aby mohla být vyvinuta a zavedena jednotlivými hráči, jejichž hlavní podnikatelská činnost s kybernetickou bezpečností nesouvisí. Zároveň nejsou dostatečně rozvinuty vazby mezi poptávkovou a nabídkovou stranou trhu kybernetické bezpečnosti, což vede k neoptimální nabídce evropských produktů a řešení přizpůsobených potřebám různých odvětví i k nedostatečné úrovni důvěry mezi hráči na trhu.
- **Chybějící účinný mechanismus spolupráce mezi členskými státy pro budování průmyslových kapacit.** V tuto chvíli neexistuje žádný účinný mechanismus spolupráce, díky němuž by členské státy mohly společně pracovat na budování nezbytných schopností podporujících inovace v oblasti kybernetické bezpečnosti v různých průmyslových odvětvích a zavádění špičkových evropských řešení v oblasti kybernetické bezpečnosti. Stávající mechanismy spolupráce pro členské státy v oblasti kybernetické bezpečnosti podle směrnice (EU) 2016/1148 ve svém mandátu s tímto druhem činností nepočítají.
- **Nedostatečná spolupráce uvnitř výzkumných a průmyslových komunit a mezi nimi navzájem.** Navzdory teoretické schopnosti Evropy pokrýt celý hodnotový řetězec kybernetické bezpečnosti existují relevantní odvětví kybernetické bezpečnosti (např. energetika, vesmír, obrana, doprava) a dílčí odvětví, která jsou dnes nedostatečně podporována výzkumnou komunitou, nebo podporována pouze omezeným počtem center

(např. postkvantová a kvantová kryptografie, důvěra a kybernetická bezpečnost v umělé inteligenci). Přestože tato spolupráce samozřejmě existuje, často je pouze krátkodobá a má podobu poradenství, což neumožňuje zapojení do dlouhodobých výzkumných plánů pro řešení průmyslových úkolů v oblasti kybernetické bezpečnosti.

- **Nedostatečná spolupráce mezi civilními a obrannými výzkumnými a inovačními komunitami v oblasti kybernetické bezpečnosti.** Nedostatečná míra spolupráce se týká rovněž civilních a obranných komunit. Stávající synergie nejsou využívány v plném rozsahu v důsledku chybějících účinných mechanismů, které by umožnily, aby tyto komunity mohly účinně spolupracovat a vybudovat si vzájemnou důvěru, jež je v tomto případě ještě více než v jiných oblastech předpokladem úspěšné spolupráce. Problém umocňují omezené finanční možnosti trhu kybernetické bezpečnosti v EU včetně nedostačujících prostředků na podporu inovací.
- **Soulad s platnými předpisy v této oblasti politiky**

Síť kompetencí pro kybernetickou bezpečnost a Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost budou působit jako doplňující podpora pro stávající právní předpisy a subjekty v oblasti kybernetické bezpečnosti. Mandát Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost bude doplňovat úsilí agentury ENISA, ale bude mít jiné zaměření a vyžaduje odlišný soubor schopností. Mandát agentury ENISA sice počítá s poradenskou rolí v rámci výzkumu a inovací v oblasti kybernetické bezpečnosti v EU, avšak její navrhovaný mandát se soustředí především na jiné úkoly nezbytné k posílení odolnosti EU v oblasti kybernetické bezpečnosti. Dále mandát agentury ENISA nezahrnuje druhy činností, které by měly být hlavními úkoly centra a sítě – podporovat rozvoj a zavádění technologií kybernetické bezpečnosti a doplnit stávající úsilí o budování kapacit v této oblasti na úrovni EU a na vnitrostátní úrovni.

Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost bude společně se sítí kompetencí pro kybernetickou bezpečnost také usilovat o podporu výzkumu s cílem usnadnit a zrychlit procesy standardizace a certifikace, zejména v souvislosti se systémy certifikace kybernetické bezpečnosti ve smyslu navrhovaného aktu o kybernetické bezpečnosti¹³¹⁴.

Tato iniciativa *de facto* rozšiřuje smluvní partnerství veřejného a soukromého sektoru o kybernetické bezpečnosti (cPPP), které představovalo první celounijní pokus o propojení odvětví kybernetické bezpečnosti, strany poptávky (kupující produktů a řešení v oblasti kybernetické bezpečnosti, včetně veřejné správy a kritických odvětví, jako jsou doprava, zdravotnictví, energetika, finančníctví) a výzkumné komunity s cílem vybudovat platformu pro udržitelný dialog a vytvořit podmínky pro dobrovolné společné investice. Toto partnerství vzniklo v roce 2016 a do roku 2020 podnítilo investice ve výši až 1,8 miliardy EUR. Rozsah investic vynakládaných v jiných částech světa (např. Spojené státy jen v roce 2017

¹³ Návrh nařízení Evropského parlamentu a Rady o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a zrušení nařízení (EU) č. 526/2013 a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („akt o kybernetické bezpečnosti“, COM(2017) 477 final/3).

¹⁴ Tím nejsou dotčeny mechanismy certifikace podle obecného nařízení o ochraně osobních údajů, v nichž hrají roli vnitrostátní orgány pro ochranu údajů, v souladu s nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („obecné nařízení o ochraně osobních údajů“).

investovaly do kybernetické bezpečnosti 19 miliard dolarů) však ukazuje, že EU musí udělat více, aby dosáhla kritického množství investic a překonala roztržičnost kapacit po celé EU.

- **Soulad s ostatními politikami Unie**

Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost bude působit jako jediný prováděcí subjekt pro různé unijní programy podporující kybernetickou bezpečnost (programy Digitální Evropa a Horizont Evropa) a zvýší jejich soudržnost a synergie mezi nimi.

Tato iniciativa také umožní doplnit úsilí členských států tím, že poskytne vhodné vstupy pro tvůrce politiky v oblasti vzdělávání s cílem zlepšit dovednosti v oblasti kybernetické bezpečnosti (např. vytvořením vzdělávacích programů v oblasti kybernetické bezpečnosti v rámci civilních a vojenských vzdělávacích systémů) a pomoci rozvíjet v EU kvalifikovanou pracovní sílu v oblasti kybernetické bezpečnosti, která bude klíčovým aktivem pro společnosti působící v této oblasti i další odvětví, která mají zájem na kybernetické bezpečnosti. Pokud jde o vzdělávání a odbornou přípravu v oblasti kybernetické obrany, bude tato iniciativa v souladu s probíhající prací na platformě pro vzdělávání, odbornou přípravu a cvičení v oblasti kybernetické obrany založené pod Evropskou bezpečnostní a obrannou školou.

Iniciativa doplní a podpoří úsilí center pro digitální inovace v rámci programu Digitální Evropa. Centra pro digitální inovace jsou neziskové organizace, které pomáhají společnostem – zejména začínajícím podnikům, malým a středním podnikům a společnostem se střední tržní kapitalizací – zlepšit svou konkurenceschopnost zlepšováním jejich podnikatelských/výrobních postupů a jejich produktů a služeb prostřednictvím inteligentních inovací umožněných digitálními technologiemi. Centra pro digitální inovace poskytují podnikatelsky zaměřené služby v oblasti inovací, jako například průzkum trhu, poradenství s financováním, přístup do relevantních testovacích a experimentálních zařízení nebo odbornou přípravu a rozvoj dovedností, s cílem pomoci úspěšně uvést na trh nové produkty či služby nebo zavést lepší výrobní postupy. Některá centra pro digitální inovace se zvláštními odbornými znalostmi v oblasti kybernetické bezpečnosti by se mohla přímo zapojit do komunity kompetencí pro kybernetickou bezpečnost zřízené touto iniciativou. Ve většině případů by však centra pro digitální inovace, která nejsou zaměřená konkrétně na kybernetickou bezpečnost, mohla usnadnit svým klientům přístup k odborným znalostem, informacím a kapacitám v oblasti kybernetické bezpečnosti dostupným v komunitě kompetencí pro kybernetickou bezpečnost, a to díky úzké spolupráci se sítí národních koordinačních center a Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost. Centra pro digitální inovace by také podpořila zavádění inovativních produktů a řešení v oblasti kybernetické bezpečnosti, která odpovídají potřebám společností a dalších konečných uživatelů, jimž jsou určeny. V neposlední řadě by centra pro digitální inovace specializovaná na dané odvětví mohla se sítí a centrem sdílet své znalosti reálných odvětvových potřeb, aby plán vývoje a inovací odpovídal požadavkům průmyslu.

Vyhledávány budou synergie s příslušnými znalostními a inovačními společenstvími Evropského inovačního a technologického institutu a zejména s EIT Digital.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

• Právní základ

Kompetenční centrum by vzhledem ke své povaze a specifickým cílům mělo být zřízeno na dvojím právním základě. Článek 187 Smlouvy o fungování EU, který upravuje zakládání struktur potřebných k účinnému uskutečnění výzkumných programů, programů technologického rozvoje a demonstrace prováděných Unií, umožňuje kompetenčnímu centru vytvářet synergie a spojit prostředky k investování do nezbytných kapacit na úrovni členských států a vytvořit společná evropská aktiva (např. společným zadáváním veřejných zakázek na nezbytnou infrastrukturu pro testování a experimenty v oblasti kybernetické bezpečnosti). V čl. 188 prvním pododstavci je upraveno přijímání uvedených opatření. Nicméně čl. 188 první pododstavec by jako jediný právní základ neumožnil, aby tyto činnosti přesahovaly rámec výzkumu a vývoje, což je třeba ke splnění všech cílů kompetenčního centra stanovených v tomto nařízení; mezi tyto činnosti patří podpora uvádění produktů a řešení v oblasti kybernetické bezpečnosti na trh, pomoc evropskému odvětví kybernetické bezpečnosti, aby se stalo konkurenceschopnějším a zvýšilo svůj podíl na trhu a přidávání hodnoty k vnitrostátnímu úsilí o řešení nedostatku dovedností v oblasti kybernetické bezpečnosti. Z tohoto důvodu je pro dosažení cílů nezbytné jako právní základ přidat čl. 173 odst. 3, který Unii umožňuje přijímat opatření na podporu konkurenceschopnosti průmyslu.

• Odůvodnění návrhu z pohledu zásad subsidiarity a proporcionality

Kybernetická bezpečnost představuje společný zájem Unie, jak dokládají závěry Rady zmíněné výše. Rozsah a přeshraniční charakter incidentů jako *WannaCry* nebo *NonPetya* to jenom dokazují. Povaha a rozsah technologických problémů v oblasti kybernetické bezpečnosti i nedostatečná koordinace úsilí mezi průmyslem, veřejným sektorem a výzkumnými komunitami, jakož i v rámci těchto skupin vyžaduje od EU další podporu koordinačních úsilí jak ke sloučení kritického množství prostředků, tak k zajištění lepších znalostí a správy aktiv. Je to nezbytné vzhledem k požadavkům na prostředky souvisejícím s některými schopnostmi potřebnými k výzkumu, vývoji a nasazování v oblasti kybernetické bezpečnosti; potřebě poskytnout přístup k interdisciplinárnímu know-how v oblasti kybernetické bezpečnosti z různých oborů (často dostupnému jen částečně na vnitrostátní úrovni); globálnímu charakteru průmyslových hodnotových řetězců i aktivitám globálních konkurentů napříč trhy.

To vše vyžaduje prostředky a odborné znalosti v rozsahu, kterého lze jen těžko dosáhnout opatřeními jakéhokoli jednotlivého členského státu. Například celoevropská kvantová komunikační síť by mohla vyžadovat investici EU ve výši přibližně 900 milionů EUR v závislosti na investicích členských států (zda budou propojené / budou se doplňovat) a také na tom, v jakém rozsahu bude technicky možné využít stávající infrastruktury. Tato iniciativa bude klíčem, který umožní spojit financování a umožnit uskutečnění takových investic v Unii.

Samotné členské státy nemohou cílů této iniciativy plně dosáhnout. Jak bylo ukázáno výše, lze jich lépe dosáhnout na úrovni Unie spojením úsilí a zabráněním jejich zbytečného zdvojení, pomocí s dosažením kritického množství investic a zajištěním, že veřejné financování je používáno optimálním způsobem. Zároveň v souladu se zásadou proporcionality nepřekračuje toto nařízení rámec toho, co je nezbytné k dosažení tohoto cíle. Na základě subsidiarity a proporcionality je proto opatření na úrovni EU odůvodněné.

Tento nástroj nepředpokládá žádné nové regulační povinnosti pro podniky. Zároveň by se podnikům, zejména malým a středním podnikům, měly snížit náklady související se snahou navrhovat inovativní produkty, které jsou kyberneticky bezpečné, protože iniciativa umožňuje

spojení prostředků k investování do nezbytných kapacit na úrovni členských států nebo vytvořit společná evropská aktiva (např. společným zadáváním veřejných zakázek na nezbytnou infrastrukturu pro testování a experimenty v oblasti kybernetické bezpečnosti). Tato aktiva by mohla využít průmyslová odvětví a malé a střední podniky v různých oborech, aby zajistily kybernetickou bezpečnost svých produktů a vytvořily z ní svoji konkurenční výhodu.

- **Výběr nástroje**

Navrhovaný nástroj zřizuje subjekt určený k provádění akcí v oblasti kybernetické bezpečnosti v rámci programu Digitální Evropa a programu Horizont Evropa. Je v něm stanoven jeho mandát, úkoly i struktura řízení. Ke zřízení takového subjektu EU je třeba přijmout nařízení.

3. KONZULTACE SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

Návrh na vytvoření sítě kompetencí pro kybernetickou bezpečnost a Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost je novou iniciativou. Představuje pokračování a rozšíření smluvního partnerství veřejného a soukromého sektoru o kybernetické bezpečnosti z roku 2016.

- **Konzultace se zúčastněnými stranami**

Kybernetická bezpečnost je široké téma dotýkající se mnoha různých odvětví. Komise použila různé metody konzultace, aby zajistila, že tato iniciativa dobře odráží zájmy široké veřejnosti Unie, nikoli zvláštní zájmy úzkého okruhu zúčastněných stran. Tato metoda zajišťuje transparentnost a odpovědnost při práci Komise. Přestože vzhledem k cílovému publiku (průmyslová a výzkumná komunita a členské státy) neproběhla žádná otevřená veřejná konzultace zaměřená konkrétně na tuto iniciativu, byla tato problematika pokryta několika jinými otevřenými veřejnými konzultacemi:

- všeobecná otevřená veřejná konzultace na téma investic, výzkumu a inovací, malých a středních podniků a jednotného trhu, která se konala v roce 2018,
- 12týdenní on-line veřejná konzultace zahájená v roce 2017 s cílem získat názory širší veřejnosti (přibližně 90 respondentů) na hodnocení a přezkum agentury ENISA,
- 12týdenní on-line veřejná konzultace, která proběhla v roce 2016 u příležitosti zahájení smluvního partnerství veřejného a soukromého sektoru o kybernetické bezpečnosti (přibližně 240 respondentů).

Komise také zorganizovala cílené konzultace o této iniciativě, včetně workshopů, setkání a cílených žádostí o vstupy (od agentury ENISA a Evropské obranné agentury). Období konzultací trvalo šest měsíců od listopadu 2017 do března 2018. Komise dále provedla mapování odborných středisek, čímž získala vstupy od 665 odborných středisek zaměřených na kybernetickou bezpečnost ohledně jejich know-how, činnosti, oblastí práce a mezinárodní spolupráce. Průzkum byl zahájen v lednu a při tvorbě zprávy o provedené analýze byly zohledněny dotazníky odevzdané do 8. března 2018.

Zúčastněné strany z řad průmyslových a vědeckých komunit se domnívaly, že kompetenční centrum a síť by mohly znamenat přidanou hodnotu pro současné snahy na vnitrostátní úrovni tím, že pomohou vytvořit celoevropský ekosystém kybernetické bezpečnosti, který by umožnil lepší spolupráci mezi výzkumnými a průmyslovými komunitami. Také považovaly za nutné, aby EU a členské státy zaujaly proaktivní, dlouhodobý a strategický přístup k průmyslové politice v oblasti kybernetické bezpečnosti, který překročí hranice výzkumu

a inovací. Zúčastněné strany vyjádřily potřebu získat přístup ke klíčovým schopnostem, mezi něž patří testovací a experimentální zařízení, a být ambicióznější při řešení nedostatku dovedností v oblasti kybernetické bezpečnosti, např. prostřednictvím rozsáhlých celoevropských projektů, které přilákají nejtalentovanější odborníky. Všechny výše uvedené skutečnosti byly také považovány za nutný předpoklad, aby se Unie mohla stát celosvětově uznávaným předním hráčem v oblasti kybernetické bezpečnosti.

Členské státy v rámci konzultačních činností, které začaly minulý září¹⁵, i ve zvláštních závěrech Rady¹⁶ uvítaly záměr zřídit síť kompetencí pro kybernetickou bezpečnost s cílem podpořit vývoj a zavádění technologií v oblasti kybernetické bezpečnosti a zdůraznily potřebu zahrnout všechny členské státy a jejich stávající centra excelence a kompetencí a věnovat zvláštní pozornost doplňkovosti. Zvláště s ohledem na budoucí kompetenční centrum členské státy zdůraznily důležitost jeho koordinační role pro podporu této sítě. Konkrétně s ohledem na vnitrostátní činnosti a potřeby v oblasti kybernetické obrany ukázalo mapování, které v březnu 2018 provedla Evropská služba pro vnější činnost, že většina členských států vidí přidanou hodnotu v podpoře EU, pokud jde o odbornou přípravu a vzdělávání v kybernetické oblasti, jakož i v podpoře průmyslu prostřednictvím výzkumu a vývoje¹⁷. Tato iniciativa by skutečně byla realizována společně se členskými státy nebo subjekty podporovanými členskými státy. Spolupráce mezi průmyslem, výzkumnou komunitou a/nebo veřejným sektorem by spojila a posílila stávající subjekty a úsilí a nevytvářela nové. Členské státy by se rovněž zapojily do definování konkrétních akcí zacílených na veřejný sektor jako přímého uživatele technologií a know-how v oblasti kybernetické bezpečnosti.

• **Posouzení dopadů**

Posouzení dopadů podporující tuto iniciativu bylo předloženo Výboru pro kontrolu regulace dne 11. dubna 2017 a získalo kladné stanovisko s výhradami. Posouzení dopadů bylo následně přezkoumáno s ohledem na připomínky Výboru. Stanovisko Výboru a příloha s vysvětlením, jak byly připomínky Výboru zohledněny, je zveřejněno společně s tímto návrhem.

V posouzení dopadů byla zvažována řada legislativních i nelegislativních možností politiky. Pro hloubkové posouzení byly ponechány následující možnosti:

- Základní scénář – možnost založená na spolupráci – předpokládá pokračování stávajícího přístupu k budování průmyslových a technických kapacit v oblasti kybernetické bezpečnosti v EU prostřednictvím podpory výzkumu a inovací a souvisejících mechanismů spolupráce v rámci 9. rámcového programu.
- Možnost 1: síť kompetencí pro kybernetickou bezpečnost s Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost s dvojím mandátem k provádění opatření na podporu průmyslových technologií i pro oblast výzkumu a vývoje.
- Možnost 2: síť kompetencí pro kybernetickou bezpečnost a Evropské výzkumné a kompetenční centrum pro kybernetickou bezpečnost zaměřené na činnosti v oblasti výzkumu a inovací.

¹⁵ Např. kulatý stůl na vysoké úrovni s členskými státy, jehož se účastnili místopředseda Ansip a komisařka Gabrielová, konaný 5. prosince 2017.

¹⁶ Rada pro obecné záležitosti: Závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU (20. listopadu 2017).

¹⁷ ESVČ, březen 2018.

Mezi možnosti, které byly zamítnuty již v počáteční fázi, patřily: 1) možnost žádného opatření, 2) možnost vytvoření pouze sítě kompetencí pro kybernetickou bezpečnost, 3) možnost vytvoření pouze centralizované struktury a 4) možnost využití stávající agentury (Agentura Evropské unie pro bezpečnost sítí a informací (ENISA), Výkonná agentura pro výzkum (REA) nebo Výkonná agentura pro inovace a sítě (INEA)).

Analýza dospěla k závěru, že k dosažení cílů iniciativy je nejvhodnější možnost 1, která zároveň bude mít nejpříznivější dopady na hospodářství, společnost a životní prostředí a zaručí zájmy Unie. Hlavní argumenty hovořící pro tuto možnost zahrnovaly schopnost vytvořit skutečnou průmyslovou politiku v oblasti kybernetické bezpečnosti podporováním činností spojených nejen s výzkumem a vývojem, ale i s uváděním na trh; flexibilitu umožňující různé modely spolupráce se sítí center kompetencí, aby byly optimálně využity stávající znalosti a prostředky; možnost strukturovat spolupráci a společné závazky veřejných a soukromých zúčastněných stran ze všech relevantních odvětví včetně obrany. V neposlední řadě možnost 1 také umožňuje posílit synergie a může fungovat jako prováděcí mechanismus pro dva různé zdroje financování pro kybernetickou bezpečnost v EU v rámci příštího víceletého finančního rámce (program Digitální Evropa, program Horizont Evropa).

- **Základní práva**

Tato iniciativa umožní orgánům veřejné moci a průmyslu v členských státech efektivněji zabráňovat kybernetických hrozbám a reagovat na ně tím, že jim nabídne a zpřístupní bezpečnější produkty a řešení. To je obzvláště důležité pro ochranu přístupu k základním službám (např. doprava, zdravotnictví, bankovní a finanční služby).

Zlepšení schopnosti Evropské unie samostatně zabezpečit své produkty a služby pravděpodobně pomůže jejím občanům uplatňovat svá demokratická práva a hodnoty (např. lépe chránit svá práva související s informacemi zakotvená v Listině základních práv Evropské unie, zejména právo na ochranu osobních údajů a soukromého života), a v důsledku tak zvýšit jejich důvěru v digitální společnost a ekonomiku.

4. ROZPOČTOVÉ DŮSLEDKY

Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost bude ve spolupráci se sítí kompetencí pro kybernetickou bezpečnost představovat hlavní prováděcí subjekt pro finanční prostředky EU určené na kybernetickou bezpečnost z programu Digitální Evropa a programu Horizont Evropa.

Rozpočtové důsledky související s prováděním programu Digitální Evropa jsou podrobně rozepsány v legislativním finančním výkazu připojeném k tomuto návrhu. Výši příspěvku z finančního krytí kladu „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 21 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody. Návrh bude vycházet z výsledku procesu strategického plánování podle definice v čl. 6 odst. 6 nařízení XXX [rámcový program Horizont Evropa].

5. DALŠÍ PRVKY

- **Plány provádění a monitorování, hodnocení a podávání zpráv**

Tento návrh počítá s výslovným ustanovením o hodnocení, na jehož základě Komise provede nezávislé hodnocení (článek 38). Komise následně o svém hodnocení podá zprávu

Evropskému parlamentu a Radě, případně spolu s návrhem na přezkum, za účelem změření dopadu nástroje a jeho přidané hodnoty. Na hodnocení se použije metodika Komise pro zlepšování právní úpravy.

Výkonný ředitel by měl každé dva roky správní radě předložit hodnocení *ex-post* činnosti Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost a sítě kompetencí, jak je stanoveno v článku 17 tohoto návrhu. Výkonný ředitel by rovněž měl vypracovat akční plán v návaznosti na závěry zpětných hodnocení a každé dva roky podat Komisi zprávu o pokroku. Správní rada by měla odpovídat za sledování odpovídajících opatření v návaznosti na tyto závěry, jak je stanoveno v článku 16 tohoto návrhu.

Údajné případy nesprávného úředního postupu při činnostech právního subjektu mohou být předmětem šetření evropského veřejného ochránce práv podle ustanovení článku 228 Smlouvy.

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost a síť národních koordinačních center

*Příspěvek Evropské komise k zasedání vedoucích představitelů
v Salcburku ve dnech 19.–20. září 2018*

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 173 odst. 3 a čl. 188 první pododstavec této smlouvy,

s ohledem na návrh Evropské komise,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru¹⁸,

s ohledem na stanovisko Výboru regionů¹⁹,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

- (1) Naše každodenní životy a ekonomiky se stávají závislejší na digitálních technologiích a občané jsou čím dál více vystaveni závažným kybernetickým incidentům. Budoucí bezpečnost závisí mimo jiné na zlepšování technických a průmyslových schopností chránit Unii před kybernetickými hrozbami, jelikož o bezpečné digitální systémy se opírá jak civilní infrastruktura, tak i vojenské schopnosti.
- (2) Unie v návaznosti na strategii kybernetické bezpečnosti z roku 2013²⁰ s cílem podporovat spolehlivý, bezpečný a otevřený kybernetický ekosystém neustále zintenzivňuje svoji činnost v reakci na rostoucí výzvy v oblasti kybernetické bezpečnosti. V roce 2016 Unie přijala první opatření v oblasti kybernetické bezpečnosti prostřednictvím směrnice Evropského parlamentu a Rady (EU) 2016/1148²¹ o bezpečnosti sítí a informačních systémů.

¹⁸ Úř. věst. C, s . .

¹⁹ Úř. věst. C , , s . .

²⁰ Společné sdělení Evropskému parlamentu a Radě: Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, JOIN(2013) 1 final.

²¹ Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

- (3) V září 2017 představily Komise a Vysoká představitelka Unie pro zahraniční věci a bezpečnostní politiku společné sdělení²² nazvané „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“ s cílem dále posílit odolnost, odrazování a reakci Unie v souvislosti s kybernetickými útoky.
- (4) V září 2017 hlavy států a předsedové vlád vyzvali na Tallinnském summitu k digitální problematice, že je třeba z Unie „do roku 2025 učinit vedoucí sílu v oblasti kybernetické bezpečnosti, abychom zajistili důvěru, jistotu a ochranu našich občanů, spotřebitelů a podniků online a umožnili svobodný internet respektující právo.“
- (5) Vážná narušení sítí a informačních systémů mohou mít dopady na jednotlivé členské státy i na Unii jako celek. Bezpečnost sítí a informačních systémů je proto základním předpokladem pro hladké fungování vnitřního trhu. V současnosti je Unie v oblasti kybernetické bezpečnosti závislá na neevropských dodavatelích. Strategickým zájmem Unie je však zajistit, aby si udržela a rozvíjela důležité technické kapacity v oblasti kybernetické bezpečnosti, aby mohla zajistit bezpečnost svého jednotného digitálního trhu a zejména chránit kritické sítě a informační systémy a poskytovat klíčové služby v oblasti kybernetické bezpečnosti.
- (6) Unie disponuje bohatými odbornými znalostmi a zkušenostmi, pokud jde o výzkum, technologie a průmyslový vývoj v oblasti kybernetické bezpečnosti, ale úsilí průmyslových a výzkumných komunit je roztříštěné, nedostatečně propojené a chybí mu společný cíl, čímž je omezena konkurenceschopnost v této oblasti. Je třeba toto úsilí a odborné znalosti sdílet, propojit a používat účinným způsobem, aby se podpořily a doplnily stávající výzkumné, technické a průmyslové kapacity na unijní i vnitrostátní úrovni.
- (7) V závěrech Rady přijatých v listopadu 2017 byla Komise vyzvána, aby urychleně zajistila posouzení dopadů různých možností vytvoření odborné sítě pro kybernetickou bezpečnost a Evropského výzkumného a odborného střediska a aby do poloviny roku 2018 předložila příslušný právní nástroj.
- (8) Kompetenční centrum by mělo být hlavním nástrojem Unie pro spojení investic do výzkumu, technologií a průmyslového vývoje v oblasti kybernetické bezpečnosti a pro realizaci relevantních projektů a iniciativ společně se sítí kompetencí pro kybernetickou bezpečnost. Mělo by poskytnout finanční podporu související s kybernetickou bezpečností z programů Horizont Evropa a Digitální Evropa a mělo by být otevřené Evropskému fondu pro regionální rozvoj a případně dalším programům. Takový přístup by měl přispět k vytvoření synergií a ke koordinaci finanční podpory související s výzkumem, inovacemi, technologiemi a průmyslovým vývojem v oblasti kybernetické bezpečnosti a zamezit zdvojování.
- (9) Vzhledem k tomu, že cílů této iniciativy lze nejlépe dosáhnout, pokud se jí zúčastní všechny členské státy nebo co možná nejvíce členských států, a rovněž jako motivace k účasti pro členské státy by hlasovací práva měly držet pouze členské státy, jež finančně přispívají na správní a provozní náklady kompetenčního centra.
- (10) Finanční příspěvek zúčastněných členských států by měl být souměřitelný s finančním příspěvkem Unie na tuto iniciativu.

²² Společné sdělení Evropskému parlamentu a Radě: „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“, JOIN(2017) 450 final.

- (11) Kompetenční centrum by mělo usnadnit a pomoci koordinovat práci sítě kompetencí pro kybernetickou bezpečnost (dále jen „sítě“) tvořené národními koordinačními centry v každém členském státě. Národní koordinační centra by pro účely provádění činností souvisejících s tímto nařízením měla dostávat přímou finanční podporu od Unie, včetně grantů udělovaných bez výzev k podávání návrhů.
- (12) Národní koordinační centra by měla být vybrána členskými státy. Kromě nezbytné správní kapacity by centra měla disponovat odbornými technickými znalostmi v oblasti kybernetické bezpečnosti nebo k nim mít přímý přístup, zejména v odvětvích, jako jsou kryptografie, bezpečnostní služby IKT, detekce narušení, bezpečnost systémů, bezpečnost sítí, bezpečnost softwaru a aplikací nebo lidské a společenské aspekty bezpečnosti a soukromí. Rovněž by měla mít kapacitu k efektivní práci a koordinaci s průmyslem, veřejným sektorem, včetně orgánů určených podle směrnice Evropského parlamentu a Rady (EU) 2016/1148²³, a výzkumnou komunitou.
- (13) Je-li národním koordinačním centřům poskytována finanční podpora s cílem podpořit třetí osoby na vnitrostátní úrovni, musí být příslušným zúčastněným stranám postoupena prostřednictvím kaskádových grantových dohod.
- (14) Nově vznikající technologie, jako jsou umělá inteligence, internet věcí, vysoce výkonná výpočetní technika (HPC) a kvantová výpočetní technika, technologie blockchain nebo koncepty typu bezpečné digitální identity, představují pro kybernetickou bezpečnost nové výzvy a zároveň i řešení. Posuzování a ověřování spolehlivosti stávajících nebo budoucích systémů IKT bude vyžadovat testování bezpečnostních řešení v souvislosti s útoky prováděnými prostřednictvím výkonné a kvantové počítačové techniky. Kompetenční centrum, síť a komunita kompetencí pro kybernetickou bezpečnost by měly pomáhat s vývojem a šířením nejnovějších řešení v oblasti kybernetické bezpečnosti. Zároveň by kompetenční centrum a síť měly sloužit vývojářům a provozovatelům v kritických odvětvích, jako jsou doprava, energetika, zdravotnictví, finančníctví, státní správa, telekomunikace, výroba, obrana a vesmír, a pomáhat jim s řešením výzev v oblasti kybernetické bezpečnosti.
- (15) Kompetenční centrum by mělo plnit několik hlavních funkcí. Zprvu by kompetenční centrum mělo usnadnit a pomoci koordinovat práci evropské sítě kompetencí pro kybernetickou bezpečnost a podporovat komunitu kompetencí pro kybernetickou bezpečnost. Mělo by aktivně prosazovat agendu technologií kybernetické bezpečnosti a usnadnit přístup k odborným znalostem shromážděným v rámci sítě a komunity kompetencí pro kybernetickou bezpečnost. Zadruhé by mělo provádět příslušné části programů Digitální Evropa a Horizont Evropa přidělováním grantů, zpravidla v návaznosti na konkurenční výzvy k podávání návrhů. Zatřetí by kompetenční centrum mělo usnadnit společné investice Unie, členských států a/nebo průmyslu.
- (16) Kompetenční centrum by mělo stimulovat a podporovat spolupráci a koordinaci činností komunity kompetencí pro kybernetickou bezpečnost, jež by zahrnovala rozsáhlou, otevřenou a různorodou skupinu aktérů zapojených do technologií kybernetické bezpečnosti. Zmíněná komunita by měla zahrnovat zejména výzkumné subjekty, průmyslová odvětví na straně dodávky i poptávky a veřejný sektor. Komunita kompetencí pro kybernetickou bezpečnost by měla kompetenčnímu centru poskytovat vstupy pro jeho činnost a pracovní plán a rovněž by měla těžit z činností

²³ Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

kompetenčního centra a sítě zaměřených na budování komunity, ale v jiných ohledech by neměla být upřednostňována, pokud jde o výzvy k podávání návrhů či nabídek.

- (17) S cílem reagovat na potřeby průmyslových odvětví na straně nabídky i poptávky by se úkol kompetenčního centra, totiž poskytovat znalosti a technickou pomoc průmyslovým odvětvím, měl vztahovat jak na produkty a služby IKT, tak na všechny ostatní průmyslové a technické produkty a řešení, do nichž je třeba začlenit kybernetickou bezpečnost.
- (18) Ačkoli by kompetenční centrum a síť měly usilovat o synergie mezi civilní a obrannou oblastí kybernetické bezpečnosti, budou projekty financované programem Horizont Evropa prováděny v souladu s nařízením XXX [nařízení o programu Horizont Evropa], které stanoví, že výzkumné a inovační činnosti prováděné v rámci programu Horizont Evropa musí být zaměřeny na civilní využití.
- (19) S cílem zajistit strukturovanou a udržitelnou spolupráci by vztah mezi kompetenčním centrem a národními koordinačními centry měl být založen na smluvní dohodě.
- (20) Vhodná ustanovení by měla zajistit odpovědnost a transparentnost kompetenčního centra.
- (21) Vzhledem k jejich odborným znalostem by Společné výzkumné středisko Komise i Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) měly hrát aktivní úlohu v rámci komunity kompetencí pro kybernetickou bezpečnost a v průmyslové a vědecké poradní radě.
- (22) V případech, kdy národní koordinační centra a subjekty, které jsou součástí komunity kompetencí pro kybernetickou bezpečnost, obdrží finanční příspěvek ze souhrnného rozpočtu Unie, měly by veřejně propagovat skutečnost, že příslušné činnosti probíhají v rámci této iniciativy.
- (23) Příspěvek Unie na kompetenční centrum by měl pokrýt polovinu nákladů vyplývajících ze zřízení a správních a koordinačních činností kompetenčního centra. S cílem předejít dvojímu financování by tyto činnosti neměly být zároveň podporovány příspěvky z jiných unijních programů.
- (24) Správní rada kompetenčního centra, složená z členských států a Komise, by měla vymezit obecné směřování činností kompetenčního centra a zajistit, aby své úkoly vykonávalo v souladu s tímto nařízením. Správní radě by měly být svěřeny pravomoci potřebné pro sestavování rozpočtu, ověřování jeho plnění, přijímání vhodných finančních pravidel, zavedení transparentních pracovních postupů pro přijímání rozhodnutí kompetenčního centra, schvalování pracovního plánu a víceletého strategického plánu kompetenčního centra, v nichž budou zohledněny priority týkající se dosahování jeho cílů a plnění jeho úkolů, přijímání jednacího řádu kompetenčního centra, jakož i pro jmenování výkonného ředitele a rozhodování o prodloužení jeho funkčního období a o jeho odvolání.
- (25) V zájmu řádného a účinného fungování kompetenčního centra by Komise a členské státy měly zajistit, aby osoby, které mají být jmenovány členy správní rady, měly patřičnou odbornou kvalifikaci a zkušenosti v daných oblastech činnosti. Komise a členské státy by rovněž měly usilovat o omezení obměny svých zástupců ve správní radě, aby byla zajištěna kontinuita její činnosti.
- (26) Řádné fungování kompetenčního centra vyžaduje, aby jeho výkonný ředitel byl jmenován na základě projevených kvalit a doložených administrativních a řídicích

schopností, jakož i kompetencí a praxe v oblasti kybernetické bezpečnosti, a aby vykonával své povinnosti zcela nezávisle.

- (27) Kompetenční centrum by mělo mít průmyslovou a vědeckou poradní radu, která bude působit jako poradní orgán zajišťující pravidelný dialog se soukromým sektorem, sdruženími spotřebitelů a dalšími příslušnými zúčastněnými stranami. Průmyslová a vědecká poradní rada by se měla zaměřit na záležitosti významné pro zúčastněné strany a upozorňovat na ně správně radu kompetenčního centra. Složení průmyslové a vědecké poradní rady a úkoly, které jsou jí přiděleny, například konzultování pracovního plánu, by měly zajistit dostatečné zastoupení zúčastněných stran v činnostech kompetenčního centra.
- (28) Kompetenční centrum by prostřednictvím své průmyslové a vědecké poradní rady mělo mít prospěch ze specifických odborných znalostí a širokého a relevantního zastoupení zúčastněných stran vybudovaných na základě smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost během trvání programu Horizont 2020.
- (29) Kompetenční centrum by mělo mít zavedena pravidla týkající se prevence a řešení střetu zájmů. Kompetenční centrum by rovněž mělo uplatňovat odpovídající ustanovení práva Unie týkající se přístupu veřejnosti k dokumentům podle nařízení Evropského parlamentu a Rady (ES) č. 1049/2001²⁴. Zpracování osobních údajů kompetenčním centrem se bude řídit nařízením Evropského parlamentu a Rady (EU) č. XXX/2018. Kompetenční centrum by mělo dodržovat předpisy vztahující se na orgány Unie, jakož i vnitrostátní předpisy o nakládání s informacemi, zejména s citlivými informacemi nepodléhajícími utajení a utajovanými informacemi Evropské unie.
- (30) Finanční zájmy Unie a členských států by měly být chráněny přiměřenými opatřeními v celém výdajovém cyklu, včetně prevence, odhalování a vyšetřování nesrovnalostí, zpětného získávání ztracených, neoprávněně vyplacených nebo nesprávně použitých finančních prostředků a případného použití správních a finančních sankcí v souladu s nařízením Evropského parlamentu a Rady (EU, Euratom) XXX²⁵ [finanční nařízení].
- (31) Kompetenční centrum by mělo fungovat otevřeným a transparentním způsobem, přičemž by mělo včas poskytovat všechny potřebné informace a propagovat své činnosti, včetně poskytování informací a jejich šíření mezi širší veřejnost. Jednací řád orgánů kompetenčního centra by měl být zveřejněn.
- (32) Interní auditor Komise by měl vykonávat vůči kompetenčnímu centru stejné pravomoci jako vůči Komisi.
- (33) Komise, kompetenční centrum, Účetní dvůr a Evropský úřad pro boj proti podvodům by měly mít přístup ke všem nezbytným informacím a do všech prostor, aby mohly provádět audity a vyšetřování týkající se grantů, smluv a dohod podepsaných kompetenčním centrem.
- (34) Vzhledem k tomu, že cílů tohoto nařízení, totiž udržování a rozvoje technických a průmyslových kapacit Unie v oblasti kybernetické bezpečnosti, zvyšování konkurenceschopnosti odvětví kybernetické bezpečnosti v Unii a přeměny

²⁴ Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).

²⁵ [doplňte název a odkaz na Úř. věst.]

kybernetické bezpečnosti v konkurenční výhodu ostatních průmyslových odvětví v Unii, nemůže být uspokojivě dosaženo členskými státy v důsledku rozptýlenosti stávajících omezených prostředků a rozsahu nezbytných investic, ale spíše jich vzhledem k potřebě vyhnout se zdvojování tohoto úsilí, pomoci dosáhnout kritického množství investic a zajistit optimální využití veřejného financování může být dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné k dosažení tohoto cíle,

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ A ZÁSADY KOMPETENČNÍHO CENTRA A SÍTĚ

Článek 1

Předmět

1. Tímto nařízením se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost (dále jen „kompetenční centrum“) a síť národních koordinačních center a stanoví pravidla pro nominaci národních koordinačních center a pro vytvoření komunity kompetencí pro kybernetickou bezpečnost.
2. Kompetenční centrum přispívá k provádění části zaměřené na kybernetickou bezpečnost v rámci programu Digitální Evropa zavedeného nařízením XXX, zejména opatření souvisejících s článkem 6 nařízení (EU) č. XXX [program Digitální Evropa], a v rámci programu Horizont Evropa zavedeného nařízením č. XXX, zejména bodu 2.2.6 pilíře II přílohy I rozhodnutí č. XXX o zavedení zvláštního programu, kterým se provádí rámcový program pro výzkum a inovace Horizont Evropa [ref. číslo zvláštního programu].
3. Sídlo kompetenčního centra se nachází v [Bruselu v Belgii.]
4. Kompetenční centrum má právní subjektivitu. V každém členském státě požívá nejširší způsobilost k právům a právním úkonům přiznanou právníkům osobám podle práva daného členského státu. Může zejména nabývat a zcizovat movitý a nemovitý majetek a být účastníkem soudních řízení.

Článek 2

Definice

Pro účely tohoto nařízení se použijí tyto definice:

- 1) „kybernetickou bezpečností“ se rozumí ochrana sítí a informačních systémů, jejich uživatelů a dalších osob proti kybernetickým hrozbám;
- 2) „produkty a řešeními v oblasti kybernetické bezpečnosti“ se rozumí produkty, služby a postupy v oblasti informačních a komunikačních technologií, jejichž konkrétním účelem je ochrana sítí a informačních systémů, jejich uživatelů a dotčených osob před kybernetickými hrozbami;

- 3) „orgánem veřejné moci“ se rozumí jakýkoli vládní či jiný orgán veřejné správy, včetně veřejných poradních orgánů, na vnitrostátní, regionální nebo místní úrovni či jakákoli fyzická či právnická osoba, které vykonává funkci ve veřejné správě podle vnitrostátního práva, včetně zvláštních povinností;
- 4) „zúčastněným členským státem“ se rozumí členský stát, který dobrovolně poskytuje finanční příspěvky na pokrytí správních a provozních nákladů kompetenčního centra.

Článek 3

Poslání kompetenčního centra a sítě

1. Kompetenční centrum a síť pomáhají Unii:
 - a) udržovat a rozvíjet nezbytné technologické a průmyslové schopnosti Unie v oblasti kybernetické bezpečnosti k zajištění jejího jednotného digitálního trhu;
 - b) zvyšovat konkurenceschopnost odvětví kybernetické bezpečnosti v Unii a přeměnit kybernetickou bezpečnost v konkurenční výhodu jiných průmyslových odvětví Unie.
2. Kompetenční centrum plní své úkoly v příslušných případech ve spolupráci se sítí národních koordinačních center a komunitou kompetencí pro kybernetickou bezpečnost.

Článek 4

Cíle a úkoly kompetenčního centra

Kompetenční centrum má následující cíle a související úkoly:

1. usnadňovat a pomáhat koordinovat práci sítě národních koordinačních center (dále jen „sítě“) podle článku 6 a komunity kompetencí pro kybernetickou bezpečnost podle článku 8;
2. přispívat k provádění části zaměřené na kybernetickou bezpečnost v rámci programu Digitální Evropa zavedeného nařízením č. XXX²⁶, zejména opatření souvisejících s článkem 6 nařízení (EU) č. XXX [program Digitální Evropa], a v rámci programu Horizont Evropa zavedeného nařízením č. XXX²⁷, zejména bodu 2.2.6 pilíře II přílohy I rozhodnutí č. XXX o zavedení zvláštního programu, kterým se provádí rámcový program pro výzkum a inovace Horizont Evropa [ref. číslo zvláštního programu], a v rámci dalších unijních programů, stanoví-li tak právní akty Unie];
3. zlepšovat schopnosti, znalosti a infrastruktury v oblasti kybernetické bezpečnosti ve prospěch průmyslových odvětví, veřejného sektoru a výzkumných komunit, a to plněním těchto úkolů:
 - a) s ohledem na nejmodernější průmyslové a výzkumné infrastruktury a související služby v oblasti kybernetické bezpečnosti získávat, aktualizovat, provozovat a zpřístupňovat takové infrastruktury a související služby širokému okruhu uživatelů v celé Unii z řad průmyslu, včetně malých a středních podniků, veřejného sektoru a výzkumné a vědecké komunity;

²⁶ [doplňte úplný název a odkaz na Úř. věst.]

²⁷ [doplňte úplný název a odkaz na Úř. věst.]

- b) s ohledem na nejmodernější průmyslové a výzkumné infrastruktury a související služby v oblasti kybernetické bezpečnosti poskytovat podporu dalším subjektům, včetně finanční podpory, při získávání, aktualizování, provozování a zpřístupňování takových infrastruktur a souvisejících služeb širokému okruhu uživatelů po celé Unii z řad průmyslu, včetně malých a středních podniků, veřejného sektoru a výzkumné a vědecké komunity;
 - c) poskytovat znalosti a technickou pomoc v oblasti kybernetické bezpečnosti průmyslu a orgánům veřejné moci, zejména podporováním opatření, jejichž cílem je usnadnit přístup k odborným znalostem sítě a komunity kompetencí pro kybernetickou bezpečnost;
- 4. přispívat k plošnému nasazení produktů a řešení v oblasti kybernetické bezpečnosti napříč celou ekonomikou, a to plněním následujících úkolů:
 - a) podporovat výzkum, vývoj a zavádění produktů a řešení v oblasti kybernetické bezpečnosti původem z Unie orgány veřejné moci a uživatelskými odvětvími;
 - b) pomáhat orgánům veřejné moci, průmyslu na straně poptávky a dalším uživatelům při zavádění a integrování nejnovějších řešení v oblasti kybernetické bezpečnosti;
 - c) podporovat zejména orgány veřejné moci při zadávání veřejných zakázek nebo zadávání zakázek na nejmodernější produkty a řešení v oblasti kybernetické bezpečnosti jménem orgánů veřejné moci;
 - d) poskytovat finanční podporu a technickou pomoc začínajícím podnikům a malým a středním podnikům v odvětví kybernetické bezpečnosti, pokud jde o propojení s potenciálními trhy a přilákání investic;
- 5. zlepšovat povědomí o kybernetické bezpečnosti a přispívat ke snižování nedostatku v oblasti dovedností souvisejících s kybernetickou bezpečností v Unii, a to plněním těchto úkolů:
 - a) podporovat další rozvoj schopností v oblasti kybernetické bezpečnosti, v příslušných případech společně s příslušnými agenturami a subjekty EU včetně agentury ENISA;
- 6. přispívat k posílení výzkumu a vývoje v oblasti kybernetické bezpečnosti v Unii, a to následovně:
 - a) poskytovat finanční podporu na výzkumné úsilí v oblasti kybernetické bezpečnosti na základě společného a průběžně posuzovaného a vylepšovaného víceletého strategického, průmyslového, technologického a výzkumného programu;
 - b) podporovat rozsáhlé výzkumné a demonstrační projekty zaměřené na technologické schopnosti příští generace v oblasti kybernetické bezpečnosti ve spolupráci s průmyslem a sítí;
 - c) podporovat výzkum a inovace pro účely standardizace technologií kybernetické bezpečnosti;
- 7. posilovat spolupráci mezi civilní a obranou oblastí s ohledem na technologie a aplikace dvojího užití v oblasti kybernetické bezpečnosti, a to plněním těchto úkolů:

- a) podporovat členské státy a zúčastněné strany ze sféry průmyslu a výzkumu, pokud jde o výzkum, vývoj a nasazení;
 - b) přispívat ke spolupráci mezi členskými státy podporováním vzdělávání, odborné přípravy a cvičení;
 - c) spojovat zúčastněné strany v zájmu podpory synergií mezi civilním a obranným výzkumem a trhy v oblasti kybernetické bezpečnosti;
8. posilovat synergie mezi civilním a obranným rozměrem kybernetické bezpečnosti v souvislosti s Evropským obranným fondem, a to plněním těchto úkolů:
- a) poskytovat poradenství, sdílet odborné znalosti a usnadňovat spolupráci mezi příslušnými zúčastněnými stranami;
 - b) řídit nadnárodní projekty kybernetické obrany na žádost členských států, a tak působit jako projektový manažer ve smyslu nařízení XXX [nařízení, kterým se zřizuje Evropský obranný fond].

Článek 5

Investice do infrastruktur, schopností, produktů nebo řešení a jejich využívání

1. Poskytuje-li kompetenční centrum financování infrastruktur, schopností, produktů nebo řešení podle čl. 4 odst. 3 a 4 ve formě grantu či ceny, může pracovní plán kompetenčního centra zejména stanovit:
 - a) pravidla upravující provoz infrastruktury či schopnosti, včetně případného svěření provozu hostujícímu subjektu na základě kritérií vymezených kompetenčním centrem;
 - b) pravidla upravující přístup k infrastruktuře či schopnosti a jejich využívání.
2. Kompetenční centrum může odpovídat za celkové provádění příslušného společného zadávání veřejných zakázek, včetně zadávání veřejných zakázek v předobchodní fázi jménem členů sítě, členů komunity kompetencí pro kybernetickou bezpečnost nebo třetích osob zastupujících uživatele produktů a řešení v oblasti kybernetické bezpečnosti. Pro tento účel může kompetenčnímu centru pomáhat jedno nebo více národních koordinačních center či členů komunity kompetencí pro kybernetickou bezpečnost.

Článek 6

Nominace národních koordinačních center

1. Do [datum] každý členský stát nominuje subjekt, který má působit jako národní koordinační centrum pro účely tohoto nařízení, a informuje o tom Komisi.
2. Na základě posouzení týkajícího se splnění kritérií stanovených v odstavci 4 ze strany uvedeného subjektu vydá Komise do šesti měsíců od nominace centra oznámené členským státem rozhodnutí, jímž subjekt akredituje jako národní koordinační centrum, nebo nominaci zamítne. Komise zveřejní seznam národních koordinačních center.
3. Členské státy mohou pro účely tohoto nařízení kdykoli nominovat nový subjekt jako národní koordinační centrum. V případě nominace jakéhokoli nového subjektu se použijí odstavce 1 a 2.

4. Nominované národní koordinační centrum musí být schopno podporovat kompetenční centrum a síť při plnění jejich poslání stanoveného v článku 3 tohoto nařízení. Musí disponovat odbornými technickými znalostmi v oblasti kybernetické bezpečnosti nebo k nim mít přímý přístup a musí být schopno účinné spolupráce a koordinace s průmyslem, veřejným sektorem a výzkumnou komunitou.
5. Vztah mezi kompetenčním centrem a národními koordinačními centry se zakládá na smluvní dohodě podepsané mezi kompetenčním centrem a každým národním koordinačním centrem. Dohoda upraví pravidla, kterými se řídí vztah a rozdělení úkolů mezi kompetenčním centrem a každým národním koordinačním centrem.
6. Síť národních koordinačních center je složena ze všech národních koordinačních center nominovaných členskými státy.

Článek 7

Úkoly národních koordinačních center

1. Národní koordinační centra mají tyto úkoly:
 - a) podporovat kompetenční centrum při dosahování jeho cílů, zejména při koordinování komunity kompetencí pro kybernetickou bezpečnost;
 - b) usnadňovat účast průmyslu a dalších hráčů na úrovni členských států v přeshraničních projektech;
 - c) společně s kompetenčním centrem přispívat k identifikování a řešení výzev v oblasti kybernetické bezpečnosti specifických pro jednotlivá průmyslová odvětví;
 - d) působit jako kontaktní místo na vnitrostátní úrovni pro komunitu kompetencí pro kybernetickou bezpečnost a kompetenční centrum;
 - e) usilovat o vytvoření synergií s příslušnými činnostmi na vnitrostátní a regionální úrovni;
 - f) provádět konkrétní akce, pro něž kompetenční centrum udělilo granty, též prostřednictvím poskytování finanční podpory třetím osobám v souladu s článkem 204 nařízení XXX [nové finanční nařízení] za podmínek stanovených v dotčených grantových dohodách;
 - g) podporovat a šířit příslušné výsledky práce sítě, komunity kompetencí pro kybernetickou bezpečnost a kompetenčního centra na vnitrostátní nebo regionální úrovni;
 - h) posuzovat žádosti subjektů usazených ve stejném členském státě jako koordinační centrum, které se chtějí stát součástí komunity kompetencí pro kybernetickou bezpečnost.
2. Pro účely písmena f) může být finanční podpora třetím osobám poskytována v kterékoli z forem uvedených v článku 125 nařízení XXX [nové finanční nařízení] včetně jednorázových částek.
3. Národní koordinační centra mohou získat grant z Unie v souladu s čl. 195 písm. d) nařízení XXX [nové finanční nařízení] v souvislosti s plněním úkolů stanovených v tomto článku.
4. Národní koordinační centra v příslušných případech spolupracují prostřednictvím sítě s cílem plnění úkolů uvedených v odst. 1 písm. a), b), c), e) a g).

Článek 8

Komunita kompetencí pro kybernetickou bezpečnost

1. Komunita kompetencí pro kybernetickou bezpečnost podporuje posílání kompetenčního centra stanovené v článku 3 a zlepšuje a šíří odborné znalosti v oblasti kybernetické bezpečnosti v celé Unii.
2. Komunita kompetencí pro kybernetickou bezpečnost zahrnuje průmysl, akademické a neziskové výzkumné organizace, sdružení a veřejné subjekty a další subjekty zabývající se provozními a technickými záležitostmi. Spojuje hlavní zúčastněné strany v souvislosti s technologickými a průmyslovými kapacitami Unie v oblasti kybernetické bezpečnosti. Zahrnuje národní koordinační centra i orgány a subjekty Unie s příslušnými odbornými znalostmi.
3. Akreditovanými členy komunity kompetencí pro kybernetickou bezpečnost se mohou stát pouze subjekty usazené v Unii. Doloží své odborné znalosti v oblasti kybernetické bezpečnosti v alespoň jedné z těchto oblastí:
 - a) výzkum;
 - b) průmyslový vývoj;
 - c) odborná příprava a vzdělávání.
4. Kompetenční centrum akredituje subjekty zřízené podle vnitrostátního práva jako členy komunity kompetencí pro kybernetickou bezpečnost po posouzení národním koordinačním centrem členského státu, v němž je daný subjekt usazen, zda splňuje kritéria stanovená v odstavci 3. Akreditace je časově neomezená, ale může být kdykoli kompetenčním centrem zrušena, pokud se kompetenční centrum nebo příslušné národní koordinační centrum domnívá, že subjekt nesplňuje kritéria stanovená v odstavci 3, nebo se na něj vztahují příslušná ustanovení článku 136 nařízení XXX [nové finanční nařízení].
5. Kompetenční centrum akredituje příslušné instituce a jiné subjekty Unie jako členy komunity kompetencí pro kybernetickou bezpečnost v návaznosti na posouzení, zda daný subjekt splňuje kritéria stanovená v odstavci 3. Akreditace je časově neomezená, ale může být kdykoli kompetenčním centrem zrušena, pokud se kompetenční centrum domnívá, že subjekt nesplňuje kritéria stanovená v odstavci 3, nebo se na něj vztahují příslušná ustanovení článku 136 nařízení XXX [nové finanční nařízení].
6. Do činností komunity se mohou zapojit zástupci Komise.

Článek 9

Úkoly členů komunity kompetencí pro kybernetickou bezpečnost

Členové komunity kompetencí pro kybernetickou bezpečnost:

- 1) podporují kompetenční centrum při dosahování jeho poslání a cílů stanovených v člancích 3 a 4 a za tímto účelem úzce spolupracují s kompetenčním centrem a příslušnými národními koordinačními centry;
- 2) účastní se činností podporovaných kompetenčním centrem a národními koordinačními centry;

- 3) případně se účastnit pracovních skupin zřízených správní radou kompetenčního centra za účelem provádění konkrétních činností uvedených v pracovním plánu kompetenčního centra;
- 4) v příslušných případech podporují kompetenční centrum a národní koordinační centra při propagování konkrétních projektů;
- 5) propagují a šíří relevantní výsledky činností a projektů prováděných v rámci komunity.

Článek 10

Spolupráce mezi kompetenčním centrem a orgány, institucemi a jinými subjekty Unie

1. Kompetenční centrum spolupracuje s příslušnými orgány, institucemi a jinými subjekty Unie, včetně Agentury Evropské unie pro bezpečnost sítí a informací, skupiny pro reakci na počítačové hrozby (CERT-EU), Evropské služby pro vnější činnost, Společného výzkumného střediska Komise, Výkonné agentury pro výzkum, Výkonné agentury pro inovace a sítě, Evropského centra pro boj proti kyberkriminalitě zřízeného při Europolu a Evropské obranné agentury.
2. Spolupráce probíhá na základě pracovních ujednání. Uvedená ujednání jsou předložena Komisi k předchozímu souhlasu.

KAPITOLA II

ORGANIZACE KOMPETENČNÍHO CENTRA

Článek 11

Členství a struktura

1. Členy kompetenčního centra jsou Unie, zastoupená Komisí, a členské státy.
2. Strukturu kompetenčního centra tvoří:
 - a) správní rada, která plní úkoly stanovené článkem 13;
 - b) výkonný ředitel, který plní úkoly stanovené článkem 16;
 - c) průmyslová a vědecká poradní rada, která plní úkoly stanovené článkem 20.

ODDÍL I

SPRÁVNÍ RADA

Článek 12

Složení správní rady

1. Správní radu tvoří jeden zástupce z každého členského státu a pět zástupců Komise jednajících jménem Unie.
2. Každý člen správní rady má náhradníka, který jej zastupuje v jeho nepřítomnosti.
3. Členové správní rady a jejich náhradníci jsou jmenováni na základě svých znalostí techniky i s ohledem na své dovednosti v oblasti řízení, správy a rozpočtu. Komise a členské státy usilují o to, aby se omezila fluktuace jejich zástupců ve správní radě, a

zajistila se tak kontinuita práce rady. Komise a členské státy usilují o dosažení vyváženého zastoupení mužů a žen ve správní radě.

4. Funkční období členů správní rady a jejich náhradníků je čtyři roky. Toto období lze prodloužit.
5. Členové správní rady jednají v zájmu kompetenčního centra a nezávislým a transparentním způsobem zajišťují jeho cíle, poslání, identitu, autonomii a soudržnost.
6. Komise může v příslušných případech přizvat na zasedání správní rady pozorovatele, včetně zástupců relevantních institucí a jiných subjektů Unie.
7. Agentura Evropské unie pro bezpečnost sítí a informací (ENISA) je ve správní radě stálým pozorovatelem.

Článek 13

Úkoly správní rady

1. Správní rada nese celkovou odpovědnost za strategickou orientaci a činnost kompetenčního centra a dohlíží na provádění jeho činností.
2. Správní rada přijme svůj jednací řád. Tento jednací řád zahrnuje zvláštní postupy pro zjišťování střetů zájmů a jejich prevenci a zajišťuje zachování důvěrnosti všech citlivých informací.
3. Správní rada přijímá nutná strategická rozhodnutí, zejména:
 - a) přijímá víceletý strategický plán, který obsahuje prohlášení o hlavních prioritách a plánovaných iniciativách kompetenčního centra, včetně odhadu jeho finančních potřeb a zdrojů;
 - b) přijímá pracovní plán kompetenčního centra, roční účetní závěrku a rozvahu a výroční zprávu o činnosti na základě návrhu výkonného ředitele;
 - c) přijímá zvláštní finanční pravidla kompetenčního centra v souladu s [článkem 70 finančního nařízení];
 - d) přijímá postup pro jmenování výkonného ředitele;
 - e) přijímá kritéria a postupy pro posuzování a akreditaci subjektů jako členů komunity kompetencí pro kybernetickou bezpečnost;
 - f) jmenuje, odvolává a prodlužuje funkční období výkonného ředitele, poskytuje mu pokyny a sleduje jeho výsledky a jmenuje účetního;
 - g) přijímá roční rozpočet kompetenčního centra, včetně příslušného plánu pracovních míst, v němž je uveden počet dočasných pracovních míst podle funkčních skupin a platových tříd a počet smluvních zaměstnanců a vyslaných národních odborníků vyjádřený v přepočtu na plné pracovní úvazky;
 - h) přijímá pravidla o střetech zájmů;
 - i) zřizuje pracovní skupiny s členy komunity kompetencí pro kybernetickou bezpečnost;
 - j) jmenuje členy průmyslové a vědecké poradní rady;

- k) zřizuje funkci interního auditora v souladu s nařízením Komise v přenesené pravomoci (EU) č. 1271/2013²⁸;
- l) propaguje kompetenční centrum po celém světě, aby zvýšila jeho přitažlivost a vytvořila z něj špičkové světové centrum excelence v oblasti kybernetické bezpečnosti;
- m) na doporučení výkonného ředitele stanoví komunikační politiku kompetenčního centra;
- n) odpovídá za sledování odpovídajících opatření v návaznosti na zpětná hodnocení;
- o) v příslušných případech stanoví prováděcí pravidla ke služebnímu řádu a pracovnímu řádu v souladu s čl. 31 odst. 3;
- p) v příslušných případech stanoví pravidla pro vysílání národních odborníků do kompetenčního centra a pro využívání stážistů v souladu s čl. 32 odst. 2;
- q) přijímá bezpečnostní pravidla kompetenčního centra;
- r) přijímá strategii proti podvodům, která je úměrná rizikům podvodu s ohledem na analýzu nákladů a přínosů opatření, jež mají být provedena;
- s) přijímá metodiku pro výpočet finančních příspěvků od členských států;
- t) odpovídá za všechny úkoly, které nejsou výslovně přiděleny určitému orgánu kompetenčního centra; takové úkoly může přidělit jakékoli osobě působící v kompetenčním centru.

Článek 14

Předseda a zasedání správní rady

1. Správní rada volí předsedu a místopředsedu na dvouleté funkční období z řad svých členů, kteří mají hlasovací právo. Funkční období předsedy a místopředsedy může být jednou prodlouženo na základě rozhodnutí správní rady. Pokud však kdykoli během svého funkčního období přestanou být členy správní rady, jejich funkční období automaticky skončí k témuž dni. Nemůže-li předseda vykonávat své povinnosti, zaujme jeho místo z moci úřední místopředseda. Předseda se účastní hlasování.
2. Řádná zasedání správní rady se konají alespoň třikrát ročně. Mimořádná zasedání se mohou konat na žádost Komise, na žádost jedné třetiny všech členů správní rady, na žádost předsedy nebo na žádost výkonného ředitele při výkonu jeho úkolů.
3. Pokud správní rada nerozhodne jinak, výkonný ředitel se účastní jednání, nemá však hlasovací právo. Správní rada může v jednotlivých případech pozvat další osoby, aby se jejich zasedání zúčastnily jako pozorovatelé.
4. Členové průmyslové a vědecké poradní rady se mohou na pozvání předsedy účastnit zasedání správní rady, nemají však hlasovací práva.

²⁸ Nařízení Komise v přenesené pravomoci (EU) č. 1271/2013 ze dne 30. září 2013 o rámcovém finančním nařízení pro subjekty uvedené v článku 208 nařízení Evropského parlamentu a Rady (EU, Euratom) č. 966/2012 (Úř. věst. L 328, 7.12.2013, s. 42).

5. Členům správní rady a jejich náhradníkům mohou být s výhradou ustanovení jejího jednacího řádu na zasedáních nápomocní poradci nebo odborníci.
6. Kompetenční centrum zajišťuje sekretariát správní rady.

Článek 15

Pravidla hlasování ve správní radě

1. Unie má 50 % hlasovacích práv. Hlasovací práva Unie jsou nedělitelná.
2. Každý zúčastněný členský stát má jeden hlas.
3. Správní rada přijímá rozhodnutí většinou tvořenou alespoň 75 % všech hlasů (včetně hlasů nepřítomných členů), které představují alespoň 75 % celkových finančních příspěvků kompetenčnímu centru. Finanční příspěvek se vypočte na základě odhadovaných výdajů navržených členskými státy podle čl. 17 odst. 2 písm. c) a na základě zprávy o výši příspěvků zúčastněných členských států podle čl. 22 odst. 5.
4. Hlasovací práva mají pouze zástupci Komise a zástupci zúčastněných členských států.
5. Předseda se účastní hlasování.

ODDÍL II

VÝKONNÝ ŘEDITEL

Článek 16

Jmenování a odvolání výkonného ředitele nebo prodloužení jeho funkčního období

1. Výkonný ředitel má odborné znalosti a dobrou pověst v oborech, jimiž se kompetenční centrum zabývá.
2. Výkonný ředitel je zaměstnán jako dočasný zaměstnanec kompetenčního centra podle čl. 2 písm. a) pracovního řádu ostatních zaměstnanců.
3. Výkonného ředitele jmenuje správní rada ze seznamu kandidátů navržených Komisí po otevřeném a transparentním výběrovém řízení.
4. Pro účely uzavření smlouvy s výkonným ředitelem zastupuje kompetenční centrum předseda správní rady.
5. Funkční období výkonného ředitele je čtyři roky. Do konce tohoto období Komise provede posouzení, které zohlední hodnocení výsledků výkonného ředitele a budoucí úkoly a výzvy kompetenčního centra.
6. Správní rada může na návrh Komise, v němž je zohledněno posouzení podle odstavce 5, funkční období výkonného ředitele jednou prodloužit o další období nejvýše čtyř let.
7. Výkonný ředitel, jehož funkční období bylo prodlouženo, se nesmí účastnit dalšího výběrového řízení na tutéž pozici.
8. Výkonný ředitel může být odvolán z funkce pouze na základě rozhodnutí správní rady jednající na návrh Komise.

Článek 17

Úkoly výkonného ředitele

1. Výkonný ředitel odpovídá za provoz a každodenní řízení kompetenčního centra a je jeho právním zástupcem. Výkonný ředitel je odpovědný správní radě a vykonává své povinnosti v rámci pravomocí, které jsou mu svěřeny, zcela nezávisle.
2. Výkonný ředitel plní nezávisle zejména tyto úkoly:
 - a) provádí rozhodnutí přijatá správní radou;
 - b) podporuje správní radu v její práci, poskytuje pro její zasedání sekretariát a dodává všechny informace nezbytné pro plnění jejích povinností;
 - c) po konzultaci se správní radou a Komisí připravuje a předkládá správní radě k přijetí návrh víceletého strategického plánu a návrh ročního pracovního plánu kompetenčního centra, včetně rozsahu výzev k podávání návrhů, výzev k vyjádření zájmu a výzev k podávání nabídek potřebných k provedení pracovního plánu a příslušných odhadovaných výdajů navržených členskými státy a Komisí;
 - d) připravuje a předkládá správní radě k přijetí návrh ročního rozpočtu, včetně příslušného plánu pracovních míst s uvedením počtu dočasných pracovních míst v každé platové třídě a funkční skupině a počtu smluvních zaměstnanců a vyslaných národních odborníků vyjádřeného v přepočtu na plné pracovní úvazky;
 - e) provádí pracovní plán a podává o tom zprávy správní radě;
 - f) připravuje návrh výroční zprávy o činnosti kompetenčního centra, včetně informací o příslušných výdajích;
 - g) zajišťuje zavedení účinných postupů pro sledování a hodnocení výkonů kompetenčního centra;
 - h) vypracovává akční plán v návaznosti na závěry zpětných hodnocení a každé dva roky předkládá Komisi zprávy o pokroku;
 - i) připravuje, vyjednává a uzavírá dohody s národními koordinačními centry;
 - j) odpovídá za správní, finanční a personální záležitosti, včetně plnění rozpočtu kompetenčního centra, přičemž řádně zohledňuje rady poskytnuté interním auditorem v mezích svého pověření správní radou;
 - k) schvaluje a řídí zahájení výzev k podávání návrhů podle pracovního plánu a spravuje grantové dohody a rozhodnutí;
 - l) schvaluje seznam akcí vybraných pro financování na základě seznamu s uvedením pořadí vypracovaného panelem nezávislých odborníků;
 - m) schvaluje a řídí zahájení výzev k podávání nabídek podle pracovního plánu a spravuje příslušné smlouvy;
 - n) schvaluje nabídky vybrané pro financování;
 - o) předkládá roční účetní závěrku a rozvahu internímu auditorovi a následně správní radě;
 - p) zajišťuje, aby bylo prováděno posouzení rizik a řízení rizik;
 - q) podepisuje jednotlivé grantové dohody, rozhodnutí a smlouvy;
 - r) podepisuje smlouvy na veřejné zakázky;

- s) vypracovává akční plán v návaznosti na závěry interních nebo externích auditních zpráv, jakož i na vyšetřování Evropského úřadu pro boj proti podvodům (OLAF), a podává zprávy o pokroku dvakrát ročně Komisi a pravidelně správní radě;
- t) připravuje návrh finančních pravidel použitelných na kompetenční centrum;
- u) zřídí efektivní a účinný systém vnitřní kontroly, zajišťuje jeho fungování a informuje správní radu o veškerých jeho podstatných změnách;
- v) zajišťuje efektivní komunikaci s orgány Unie;
- w) přijímá jakákoli opatření potřebná k posouzení pokroku kompetenčního centra v rámci plnění jeho poslání a cílů stanovených v člancích 3 a 4 tohoto nařízení;
- x) plní veškeré další úkoly, které mu správní rada svěřila nebo kterými ho pověřila.

ODDÍL III

PRŮMYSLOVÁ A VĚDECEKÁ PORADNÍ RADA

Článek 18

Složení průmyslové a vědecké poradní rady

1. Průmyslová a vědecká poradní rada má nejvýše 16 členů. Členové jsou jmenováni správní radou z řad zástupců subjektů v komunitě kompetencí pro kybernetickou bezpečnost.
2. Členové průmyslové a vědecké poradní rady mají odborné znalosti buď v oblasti výzkumu, průmyslového vývoje či profesionálních služeb v oblasti kybernetické bezpečnosti, nebo s jejich nasazováním. Požadavky na tyto odborné znalosti podrobněji stanoví správní rada.
3. Postupy týkající se jmenování jejích členů správní radou a činnost poradní rady jsou stanoveny v jednacím řádu kompetenčního centra a zveřejněny.
4. Funkční období členů průmyslové a vědecké poradní rady je tři roky. Toto období lze prodloužit.
5. Zástupci Komise a Agentury Evropské unie pro bezpečnost sítí a informací se mohou účastnit průmyslové a vědecké poradní rady a podporovat její práci.

Článek 19

Fungování průmyslové a vědecké poradní rady

1. Průmyslová a vědecká poradní rada zasedá alespoň dvakrát ročně.
2. Průmyslová a vědecká poradní rada může v případě potřeby poskytovat správní radě poradenství ohledně zřizování pracovních skupin zabývajících se konkrétními problémy týkajícími se práce kompetenčního centra, což celkově koordinuje jeden nebo více členů průmyslové a vědecké poradní rady.
3. Průmyslová a vědecká poradní rada volí svého předsedu.
4. Průmyslová a vědecká poradní rada přijme svůj jednací řád, včetně jmenování zástupců, kteří poradní radu v příslušných případech reprezentují, a délky jejich jmenování.

Článek 20

Úkoly průmyslové a vědecké poradní rady

Průmyslová a vědecká poradní rada poskytuje kompetenčnímu centru poradenství ohledně vykonávání jeho činností a:

- 1) poskytuje výkonnému řediteli a správní radě strategické poradenství a vstupy pro tvorbu pracovního plánu a víceletého strategického plánu ve lhůtách stanovených správní radou;
- 2) organizuje veřejné konzultace otevřené všem veřejným a soukromým zúčastněným stranám, které mají zájem v oblasti kybernetické bezpečnosti, s cílem shromáždit vstupy pro strategické poradenství uvedené v odstavci 1;
- 3) podporuje a shromažďuje zpětnou vazbu k pracovnímu plánu a víceletému strategickému plánu kompetenčního centra.

KAPITOLA III FINANČNÍ USTANOVENÍ

Článek 21

Finanční příspěvek Unie

1. Příspěvek Unie kompetenčnímu centru na pokrytí správních nákladů a provozních nákladů je složen z těchto částek:
 - a) 1 981 668 000 EUR z programu Digitální Evropa, včetně až 23 746 000 EUR na správní náklady;
 - b) částka z programu Horizont Evropa, včetně správních nákladů, která bude určena s ohledem na proces strategického plánování, jenž bude proveden podle čl. 6 odst. 6 nařízení XXX [nařízení o programu Horizont Evropa].
2. Maximální příspěvek Unie bude vyplacen z prostředků souhrnného rozpočtu Unie přidělených na [program Digitální Evropa] a na zvláštní program, kterým se provádí program Horizont Evropa, zavedený rozhodnutím XXX.
3. Kompetenční centrum provádí akce v oblasti kybernetické bezpečnosti v rámci [programu Digitální Evropa] a [programu Horizont Evropa] v souladu s čl. 62 písm. c) bodem iv) nařízení (EU, Euratom) XXX²⁹ [finanční nařízení].
4. Finanční příspěvek Unie nepokrývá úkoly stanovené v čl. 4 odst. 8 písm. b).

Článek 22

Příspěvky zúčastněných členských států

1. Zúčastněné členské státy poskytnou celkový příspěvek na provozní a správní náklady kompetenčního centra přinejmenším ve stejných výších, jaké jsou uvedeny v čl. 21 odst. 1 tohoto nařízení.
2. Pro účely posouzení příspěvků uvedených v odstavci 1 a v čl. 23 odst. 3 písm. b) bodě ii) se náklady stanoví pomocí obvyklých postupů účtování nákladů dotčených členských států, platných účetních standardů členského státu a platných

²⁹ [doplňte úplný název a odkaz na Úř. věst.]

mezinárodních účetních standardů a mezinárodních standardů finančního výkaznictví. Náklady ověří nezávislý externí auditor jmenovaný dotčeným členským státem. Pokud na základě ověření vznikne nejistota, může kompetenční centrum ověřit metodu oceňování.

3. Pokud jakýkoli zúčastněný členský stát neplní své závazky týkající se finančního příspěvku, výkonný ředitel tuto skutečnost písemně zaznamená a stanoví přiměřenou lhůtu, v níž musí být tento nedostatek napraven. Není-li situace v této lhůtě napravena, výkonný ředitel svolá zasedání správní rady, aby rozhodla, zda má být zúčastněnému členskému státu neplnícímu své závazky odebráno hlasovací právo nebo zda mají být do doby, než splní své povinnosti, přijata jiná opatření. Hlasovací práva členského státu neplnícího své závazky jsou pozastavena do doby, než dojde k nápravě ve věci neplnění závazků.
4. Komise může ukončit, úměrně snížit či pozastavit poskytování finančního příspěvku Unie na kompetenční centrum, pokud zúčastněné členské státy nepřispívají, přispívají pouze částečně nebo přispívají pozdě, pokud jde o příspěvky uvedené v odstavci 1.
5. Zúčastněné členské státy podají do 31. ledna každého roku správní radě zprávu o výši příspěvků uvedených v odstavci 1 učiněných v každém předchozím rozpočtovém roce.

Článek 23

Náklady a prostředky kompetenčního centra

1. Kompetenční centrum je financováno společně Uníí a členskými státy prostřednictvím finančních příspěvků placených ve splátkách a příspěvků tvořených náklady vzniklými národním koordinačním centřum a příjemcům při provádění akcí, které nejsou propláceny kompetenčním centrem.
2. Správní náklady kompetenčního centra nepřekročí [částka] EUR a jsou hrazeny formou finančních příspěvků rozdělených každoročně rovným dílem mezi Unii a zúčastněné členské státy. Pokud se část příspěvku na správní náklady nevyužije, lze ji použít na pokrytí provozních nákladů kompetenčního centra.
3. Provozní náklady kompetenčního centra se hradí prostřednictvím:
 - a) finančního příspěvku Unie;
 - b) příspěvků zúčastněných členských států ve formě:
 - i) finančních příspěvků a
 - ii) v příslušných případech věcných příspěvků zúčastněných členských států v podobě nákladů vzniklých národním koordinačním centřum a příjemcům při provádění nepřímých akcí po odečtení příspěvku kompetenčního centra a jakéhokoli jiného příspěvku Unie na tyto náklady.
4. Prostředky kompetenčního centra, které jsou zahrnuty do jeho rozpočtu, tvoří tyto příspěvky:
 - a) finanční příspěvky zúčastněných členských států na správní náklady;
 - b) finanční příspěvky zúčastněných členských států na provozní náklady;
 - c) veškeré příjmy vytvářené kompetenčním centrem;

- d) veškeré další finanční příspěvky, prostředky a příjmy.
5. Veškeré úrokové výnosy z příspěvků hrazených kompetenčnímu centru zúčastněnými členskými státy jsou považovány za jeho příjmy.
 6. Cílem veškerých prostředků kompetenčního centra a jeho činností je dosažení cílů stanovených v článku 4.
 7. Kompetenční centrum vlastní veškerá aktiva, která vytvoří nebo která jsou na něj převedena pro plnění jeho cílů.
 8. S výjimkou zrušení kompetenčního centra nejsou zúčastněným členským státům vypláceny žádné příjmy převyšující výdaje.

Článek 24

Finanční závazky

Finanční závazky kompetenčního centra nesmějí překročit částku dostupných finančních prostředků nebo prostředků, k jejichž poskytnutí do rozpočtu se jeho členové zavázali.

Článek 25

Rozpočtový rok

Rozpočtový rok začíná 1. ledna a končí 31. prosince.

Článek 26

Sestavování rozpočtu

1. Výkonný ředitel každý rok vypracuje návrh odhadu příjmů a výdajů kompetenčního centra pro následující rozpočtový rok a spolu s návrhem plánu pracovních míst jej předá správní radě. Příjmy a výdaje musí být vyrovnané. Výdaje kompetenčního centra zahrnují výdaje na zaměstnance, správu, infrastrukturu a provoz. Výdaje na správu musí být co nejnižší.
2. Správní rada každý rok sestaví na základě návrhu odhadu příjmů a výdajů uvedeného v odstavci 1 odhad příjmů a výdajů kompetenčního centra pro následující rozpočtový rok.
3. Správní rada do 31. ledna každého roku zašle Komisi odhad uvedený v odstavci 2, který bude součástí návrhu jednotného programového dokumentu.
4. Komise na základě tohoto odhadu zanesle do návrhu rozpočtu Unie odhady, které považuje za nezbytné pro plán pracovních míst, a výši příspěvku ze souhrnného rozpočtu a předloží je Evropskému parlamentu a Radě v souladu s články 313 a 314 Smlouvy o fungování EU.
5. Evropský parlament a Rada schvalují prostředky na příspěvek pro kompetenční centrum.
6. Evropský parlament a Rada přijmou plán pracovních míst pro kompetenční centrum.
7. Správní rada přijme rozpočet kompetenčního centra společně s pracovním plánem. Rozpočet kompetenčního centra se stává konečným po přijetí souhrnného rozpočtu Unie. Správní rada v příslušných případech přizpůsobí rozpočet a pracovní plán kompetenčního centra podle souhrnného rozpočtu Unie.

Článek 27

Předkládání účetních závěrek a absolutorium

Předkládání předběžných a konečných účetních závěrek kompetenčního centra a udělení absolutoria se řídí pravidly a časovým harmonogramem stanovenými finančním nařízením a finančními pravidly přijatými v souladu s článkem 29.

Článek 28

Provozní a účetní výkaznictví

1. Výkonný ředitel každoročně v souladu s finančními pravidly kompetenčního centra předkládá správní radě zprávu o plnění svých povinností.
2. Do dvou měsíců od uzávěrky každého rozpočtového roku předloží výkonný ředitel správní radě ke schválení výroční zprávu o činnosti týkající se pokroku dosaženého kompetenčním centrem v předchozím kalendářním roce, a to zejména ve vztahu k pracovnímu plánu pro daný rok. Tato zpráva mimo jiné obsahuje informace o:
 - a) provedených operativních akcích a příslušných výdajích;
 - b) předložených akcích s rozpisem podle typu účastníků, včetně malých a středních podniků, a podle členských států;
 - c) akcích vybraných k financování s rozpisem podle typu účastníků, včetně malých a středních podniků, a podle členských států a s uvedením příspěvku kompetenčního centra jednotlivým účastníkům a na jednotlivé akce;
 - d) pokroku ohledně dosažení cílů uvedených v článku 4 a návrzích na to, co je pro dosažení těchto cílů dále třeba udělat.
3. Po schválení správní radou se výroční zpráva o činnosti zveřejní.

Článek 29

Finanční pravidla

Kompetenční centrum přijme svá zvláštní finanční pravidla v souladu s článkem 70 nařízení XXX [nové finanční nařízení].

Článek 30

Ochrana finančních zájmů

1. Kompetenční centrum přijme vhodná opatření k zajištění toho, aby při provádění akcí financovaných podle tohoto nařízení byly finanční zájmy Unie chráněny preventivními opatřeními proti podvodům, korupci a jinému protiprávnímu jednání účinnými kontrolami, a jsou-li zjištěny nesrovnalosti, zpětným získáním neoprávněně vyplacených částek a v příslušných případech účinnými, přiměřenými a odrazujícími správními sankcemi.
2. Kompetenční centrum poskytne zaměstnancům Komise a jiným osobám pověřeným Komisí, jakož i Účetnímu dvoru, přístup do svých míst a prostor a ke všem informacím, včetně informací v elektronickém formátu, které jsou potřebné k tomu, aby mohli provádět audity.
3. Evropský úřad pro boj proti podvodům (OLAF) může provádět vyšetřování, včetně kontrol na místě a inspekci, v souladu s pravidly a postupy stanovenými v nařízení

Rady (Euratom, ES) č. 2185/96³⁰ a nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013³¹ s cílem zjistit, zda nedošlo k podvodu, korupci či jiné protiprávní činnosti ovlivňující finanční zájmy Unie v souvislosti s grantovou dohodou nebo smlouvou financovanou, přímo či nepřímo, podle tohoto nařízení.

4. Aniž jsou dotčeny odstavce 1, 2 a 3 tohoto článku, musí smlouvy a grantové dohody vyplývající z provádění tohoto nařízení obsahovat ustanovení, která Komisi, kompetenční centrum, Účetní dvůr a úřad OLAF výslovně zmocňují k provádění těchto auditů a vyšetřování v souladu s jejich příslušnými pravomocemi. Je-li provádění akce zcela nebo zčásti zadáno externím dodavatelům či je-li jím někdo dále pověřen, nebo vyžaduje-li zadání veřejné zakázky nebo poskytnutí finanční podpory třetí straně, musí smlouva nebo grantová dohoda obsahovat smluvní povinnost dodavatele nebo příjemce uložit jakékoli zúčastněné třetí straně výslovné přijetí těchto pravomocí Komise, kompetenčního centra, Účetního dvora a úřadu OLAF.

KAPITOLA IV

ZAMĚSTNANCI KOMPETENČNÍHO CENTRA

Článek 31

Zaměstnanci

1. Na zaměstnance kompetenčního centra se vztahuje služební řád úředníků Evropské unie a pracovní řád ostatních zaměstnanců Evropské unie stanovený nařízením Rady (EHS, Euratom, ESUO) č. 259/68³² (dále jen „služební řád“ a „pracovní řád“) a pravidla přijatá společně orgány Unie pro účely provádění služebního řádu s pracovního řádu.
2. Správní rada vykonává ve vztahu k zaměstnancům kompetenčního centra pravomoci, které služební řád svěřuje orgánu oprávněnému ke jmenování a které pracovní řád svěřuje orgánu oprávněnému uzavírat smlouvy (dále jen „pravomoci orgánu oprávněného ke jmenování“).
3. Správní rada v souladu s článkem 110 služebního řádu přijme rozhodnutí na základě čl. 2 odst. 1 služebního řádu a na základě článku 6 pracovního řádu, kterým přeneše příslušné pravomoci orgánu oprávněného ke jmenování na výkonného ředitele a kterým stanoví podmínky, za nichž může být toto přenesení pozastaveno. Výkonný ředitel je oprávněn tyto pravomoci přenášet na další osoby.
4. Ve výjimečných případech může správní rada svým rozhodnutím dočasně pozastavit přenesení pravomocí orgánu oprávněného ke jmenování na výkonného ředitele a

³⁰ Nařízení Rady (Euratom, ES) č. 2185/96 ze dne 11. listopadu 1996 o kontrolách a inspekcích na místě prováděných Komisí za účelem ochrany finančních zájmů Evropských společenství proti podvodům a jiným nesrovnalostem (Úř. věst. L 292, 15.11.1996, s. 2).

³¹ Nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 ze dne 11. září 2013 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1073/1999 a nařízení Rady (Euratom) č. 1074/1999 (Úř. věst. L 248, 18.9.2013, s. 1).

³² Nařízení Rady (EHS, Euratom, ESUO) č. 259/68 ze dne 29. února 1968, kterým se stanoví služební řád úředníků Evropských společenství a pracovní řád ostatních zaměstnanců Evropských společenství a kterým se zavádějí zvláštní opatření dočasně použitelná na úředníky Komise (Úř. věst. L 56, 4.3.1968, s. 1).

jakékoli následné převedení pravomocí na jiné osoby provedené výkonným ředitelem. V takovém případě správní rada vykonává pravomoci orgánu oprávněného ke jmenování sama, nebo je přenesa na jednoho ze svých členů nebo na jiného zaměstnance kompetenčního centra, než je výkonný ředitel.

5. Správní rada v souladu s článkem 110 služebního řádu přijme prováděcí pravidla pro provádění služebního řádu a pracovního řádu.
6. Personální zdroje se určí v plánu pracovních míst kompetenčního centra, s uvedením počtu dočasných pracovních míst podle funkčních skupin a platových tříd a počtu smluvních pracovníků vyjádřeného v přepočtu na plné pracovní úvazky, v souladu s jeho ročním rozpočtem.
7. Zaměstnanci kompetenčního centra jsou dočasní zaměstnanci a smluvní zaměstnanci.
8. Veškeré náklady související se zaměstnanci nese kompetenční centrum.

Článek 32

Vyslaní národní odborníci a jiní zaměstnanci

1. Kompetenční centrum může využívat vyslané národní odborníky nebo jiné pracovníky, kteří nejsou zaměstnanci kompetenčního centra.
2. Správní rada po dohodě s Komisí přijme rozhodnutí, kterým se stanoví pravidla pro vysílání národních odborníků do kompetenčního centra.

Článek 33

Výsady a imunity

Na kompetenční centrum a jeho zaměstnance se vztahuje Protokol č. 7 o výsadách a imunitách Evropské unie připojený ke Smlouvě o Evropské unii a Smlouvě o fungování Evropské unie.

KAPITOLA V SPOLEČNÁ USTANOVENÍ

Článek 34

Bezpečnostní pravidla

1. Na účast ve všech akcích financovaných kompetenčním centrem se použije čl. 12 odst. 7 nařízení (EU) č. XXX [program Digitální Evropa].
2. Na akce financované z programu Horizont Evropa se použijí tato zvláštní bezpečnostní pravidla:
 - a) pro účely čl. 34 odst. 1 [Vlastnictví a ochrana výsledků] nařízení (EU) č. XXX [program Horizont Evropa] může být udělování nevýhradních licencí omezeno na třetí strany usazené nebo považované za usazené v členských státech a kontrolované členskými státy a/nebo občany členských států, je-li to stanoveno v pracovním plánu;
 - b) pro účely čl. 36 odst. 4 písm. b) [Převod vlastnictví a udělování licencí] nařízení (EU) č. XXX [program Horizont Evropa] je převod vlastnictví nebo udělení licence právnímu subjektu usazenému v přidružené zemi, nebo

usazenému v Unii, ale kontrolovanému z třetích zemí, rovněž důvodem pro vznesení námitky proti převodu vlastnictví výsledků nebo udělení výhradní licence k výsledkům;

- c) pro účely čl. 37 odst. 3 písm. a) [Přístupová práva] nařízení (EU) č. XXX [program Horizont Evropa] může být udělení přístupu k výsledkům a stávajícím znalostem omezeno pouze na právní subjekt usazený nebo považovaný za usazený v členských státech a kontrolovaný členskými státy a/nebo občany členských států, je-li to stanoveno v pracovním plánu.

Článek 35

Transparentnost

1. Kompetenční centrum vykonává své činnosti s vysokou mírou transparentnosti.
2. Kompetenční centrum zajistí, aby veřejnost a všechny zainteresované strany měly k dispozici náležitě, objektivní, spolehlivé a snadno dostupné informace, zejména pokud jde o výsledky jeho činnosti. Zveřejní rovněž prohlášení o zájmech učiněná v souladu s článkem 41.
3. Správní rada může na návrh výkonného ředitele zainteresovaným stranám umožnit, aby se účastnily některých činností kompetenčního centra jako pozorovatelé.
4. Kompetenční centrum ve svém jednacím řádu stanoví praktická opatření pro provádění pravidel transparentnosti podle odstavců 1 a 2. V rámci akcí financovaných z programu Horizont Evropa náležitě zohlední ustanovení přílohy III nařízení o programu Horizont Evropa.

Článek 36

Bezpečnostní pravidla týkající se ochrany utajovaných informací a citlivých neutajovaných informací

1. Aniž je dotčen článek 35, kompetenční centrum nesděluje třetím osobám informace, které zpracovává nebo obdrží a pro které bylo odůvodněně vyžádáno zcela či částečně důvěrné zacházení.
2. Členové správní rady, výkonný ředitel, členové průmyslové a vědecké poradní rady, externí odborníci, jenž se účastní *ad hoc* pracovních skupin, a zaměstnanci kompetenčního centra dodržují povinnost zachovávat důvěrnost podle článku 339 Smlouvy o fungování Evropské unie, a to i po skončení svých funkcí.
3. Správní rada kompetenčního centra přijme bezpečnostní pravidla kompetenčního centra po schválení Komisí na základě zásad a pravidel stanovených v bezpečnostních pravidlech Komise pro ochranu utajovaných informací Evropské unie a citlivých neutajovaných informací, včetně mimo jiné ustanovení upravujících zpracování a uchovávání těchto informací, jak stanoví rozhodnutí Komise (EU, Euratom) 2015/443³³ a 2015/444³⁴.

³³ Rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi (Úř. věst. L 72, 17.3.2015, s. 41).

³⁴ Rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 72, 17.3.2015, s. 53).

4. Kompetenční centrum může přijmout veškerá opatření nezbytná k usnadnění výměny informací týkajících se jeho úkolů s Komisí a členskými státy a v příslušných případech s relevantními subjekty Unie. Jakékoli správní ujednání za tímto účelem ohledně sdílení utajovaných informací EU, nebo v případě neexistence takového opatření případně výjimečné *ad hoc* uvolnění těchto informací musí být předem schváleno Komisí.

Článek 37

Přístup k dokumentům

1. Na dokumenty v držení kompetenčního centra se vztahuje nařízení (ES) č. 1049/2001.
2. Správní rada přijme do šesti měsíců od zřízení kompetenčního centra prováděcí pravidla k nařízení (ES) č. 1049/2001.
3. Rozhodnutí učiněná kompetenčním centrem podle článku 8 nařízení (ES) č. 1049/2001 mohou být předmětem stížnosti předložené veřejnému ochránci práv podle článku 228 Smlouvy o fungování Evropské unie nebo Soudnímu dvoru Evropské unie podle článku 263 Smlouvy o fungování Evropské unie.

Článek 38

Sledování, hodnocení a přezkum

1. Kompetenční centrum zajistí, aby jeho činnosti, včetně činností řízených prostřednictvím národních koordinačních center a sítě, byly předmětem průběžného a systematického sledování a pravidelného přezkumu. Kompetenční centrum zajistí, aby údaje týkající se sledování provádění programu a výsledků byly shromažďovány účinným, efektivním a včasným způsobem a aby na příjemce unijních prostředků a na členské státy byly uloženy přiměřené požadavky na podávání zpráv. Výsledky hodnocení se zveřejňují.
2. Jakmile jsou k dispozici dostačující informace o provádění tohoto nařízení, avšak nejpozději tři a půl roku po zahájení provádění tohoto nařízení, provede Komise průběžné hodnocení kompetenčního centra. O tomto hodnocení vypracuje Komise zprávu a do 31. prosince 2024 ji předloží Evropskému parlamentu a Radě. Kompetenční centrum a členské státy poskytnou Komisi informace potřebné pro přípravu uvedené zprávy.
3. Součástí hodnocení uvedeného v odstavci 2 bude posouzení výsledků, kterých kompetenční centrum s ohledem na své cíle, mandát a úkoly dosáhlo. Pokud se Komise domnívá, že pokračování činnosti kompetenčního centra je vzhledem k jeho určeným cílům, mandátu a úkolům odůvodněné, může navrhnout, aby byl mandát kompetenčního centra stanovený v článku 46 prodloužen.
4. Na základě závěrů průběžného hodnocení uvedeného v odstavci 2 může Komise jednat v souladu s [čl. 22 odst. 5] nebo přijmout jiná vhodná opatření.
5. Sledování, hodnocení, ukončování a obnovování příspěvku z programu Horizont Evropa se bude řídit ustanoveními článků 8, 45 a 47 a přílohy III nařízení o programu Horizont Evropa a sjednanými způsoby provádění.
6. Sledování, podávání zpráv a hodnocení týkající se příspěvku z programu Digitální Evropa se bude řídit ustanoveními článků 24 a 25 programu Digitální Evropa.

7. V případě zrušení kompetenčního centra provede Komise závěrečné hodnocení kompetenčního centra do šesti měsíců po jeho zrušení, avšak nejpozději do dvou let po zahájení likvidačního řízení uvedeného v článku 46 tohoto nařízení. Výsledky závěrečného hodnocení se předloží Evropskému parlamentu a Radě.

Článek 39

Odpovědnost kompetenčního centra

1. Smluvní odpovědnost kompetenčního centra se řídí právními předpisy, kterými se řídí dotčená dohoda, rozhodnutí nebo smlouva.
2. V případě mimosmluvní odpovědnosti nahradí kompetenční centrum v souladu s obecnými zásadami společnými právním řádům členských států škodu způsobenou jeho zaměstnanci při plnění jejich povinností.
3. Veškeré platby kompetenčního centra týkající se odpovědnosti uvedené v odstavcích 1 a 2 a náklady a výdaje vzniklé ve spojitosti s touto odpovědností jsou považovány za výdaje kompetenčního centra a hrazeny z jeho prostředků.
4. Za plnění svých závazků odpovídá výhradně kompetenční centrum.

Článek 40

Pravomoc Soudního dvora Evropské unie a rozhodné právo

1. Soudní dvůr Evropské unie má pravomoc:
 - 1) na základě jakékoliv rozhodčí doložky obsažené v dohodách, rozhodnutích nebo smlouvách uzavřených kompetenčním centrem;
 - 2) ve sporech týkajících se náhrady škody způsobené zaměstnanci kompetenčního centra při plnění jejich povinností;
 - 3) v jakémkoli sporu mezi kompetenčním centrem a jeho zaměstnanci v mezích a za podmínek stanovených ve služebním řádu.
2. Ve věcech, na které se nevztahuje toto nařízení nebo jiné právní akty Unie, se použije právo členského státu, v němž se nachází sídlo kompetenčního centra.

Článek 41

Odpovědnost členů a pojištění

1. Finanční odpovědnost členů za závazky kompetenčního centra je omezena výší již poskytnutého příspěvku na správní náklady.
2. Kompetenční centrum uzavře a udržuje vhodné pojištění.

Článek 42

Střety zájmů

Správní rada kompetenčního centra přijme pravidla k zabránění vzniku střetů zájmů u svých členů, orgánů a zaměstnanců a k řešení takových střetů. Tato pravidla obsahují ustanovení

určená k zabránění střetů zájmů, pokud jde o zástupce členů ve správní radě a v průmyslové a vědecké poradní radě, v souladu s nařízením XXX [nové finanční nařízení].

Článek 43

Ochrana osobních údajů

1. Zpracování osobních údajů kompetenčním centrem se řídí nařízením Evropského parlamentu a Rady (EU) č. XXX/2018.
2. Správní rada přijme prováděcí opatření uvedená v čl. xx odst. 3 nařízení (EU) č. xxx/2018. Správní rada může přijmout dodatečná opatření nezbytná pro použití nařízení (EU) č. xxx/2018 kompetenčním centrem.

Článek 44

Podpora ze strany hostitelského členského státu

Kompetenční centrum a členský stát [Belgie], kde se nachází jeho sídlo, mohou uzavřít správní dohodu o výsadách a imunitách a další podpoře, jež tento stát kompetenčnímu centru poskytne.

KAPITOLA VII

ZÁVĚREČNÁ USTANOVENÍ

Článek 45

Počáteční opatření

1. Komise je odpovědná za zřízení a počáteční provoz kompetenčního centra až do doby, než bude mít kompetenční centrum provozní kapacitu k plnění vlastního rozpočtu. Komise v souladu s právem Unie provede veškerá nezbytná opatření ve spolupráci s příslušnými orgány kompetenčního centra.
2. Do doby, než se výkonný ředitel po jmenování správní radou v souladu s článkem 16 stanov ujme svých povinností, může Komise pro účely odstavce 1 určit dočasného výkonného ředitele a vykonávat úkoly svěřené výkonnému řediteli, případně za pomoci omezeného počtu úředníků Komise. Komise může dočasně přidělit omezený počet svých úředníků.
3. Dočasný výkonný ředitel může schvalovat všechny platby kryté prostředky stanovenými v ročním rozpočtu kompetenčního centra, pokud jej schválila správní rada, a může uzavírat dohody a smlouvy a přijímat rozhodnutí, včetně smluv se zaměstnanci, pokud byl přijat plán pracovních míst kompetenčního centra.
4. Dočasný výkonný ředitel po vzájemné dohodě s výkonným ředitelem kompetenčního centra a s výhradou schválení správní radou stanoví datum, kdy bude mít kompetenční centrum kapacitu k plnění vlastního rozpočtu. Od tohoto data se Komise zdrží přijímání závazků a provádění plateb týkajících se činností kompetenčního centra.

Článek 46

Doba trvání

1. Kompetenční centrum se zřizuje na období od 1. ledna 2021 do 31. prosince 2029.
2. Není-li prostřednictvím přezkumu tohoto nařízení rozhodnuto jinak, na konci uvedeného období se zahájí likvidační řízení. Likvidační řízení se zahájí automaticky, pokud od kompetenčního centra odstoupí Unie nebo všechny zúčastněné členské státy.
3. Pro účely likvidačního řízení kompetenčního centra jmenuje správní rada jednoho nebo několik likvidátorů, kteří postupují podle jejích rozhodnutí.
4. Při likvidaci kompetenčního centra se jeho aktiva použijí k pokrytí jeho závazků a výdajů souvisejících s jeho likvidací. Případný přebytek se rozdělí mezi Unii a zúčastněné členské státy úměrně k jejich finančnímu příspěvku na kompetenční centrum. Veškeré takové přebytky, které obdrží Unie, se vrátí do rozpočtu Unie.

Článek 47

Vstup v platnost

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament
předseda/předsedkyně

Za Radu
předseda/předsedkyně

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

- 1.1. Název návrhu/podnětu
- 1.2. Příslušné oblasti politik podle členění ABM/ABB
- 1.3. Povaha návrhu/podnětu
- 1.4. Cíle
- 1.5. Odůvodnění návrhu/podnětu
- 1.6. Doba trvání akce a finanční dopad
- 1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

- 2.1. Pravidla pro sledování a podávání zpráv
- 2.2. Systém řízení a kontroly
- 2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

- 3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky
- 3.2. Odhadovaný dopad na výdaje
 - 3.2.1. *Odhadovaný souhrnný dopad na výdaje*
 - 3.2.2. *Odhadovaný dopad na operační prostředky*
 - 3.2.3. *Odhadovaný dopad na prostředky správní povahy*
 - 3.2.4. *Soulad se stávajícím víceletým finančním rámcem*
 - 3.2.5. *Příspěvky třetích stran*
- 3.3. Odhadovaný dopad na příjmy

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Nařízení, kterým se zřizuje Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost

1.2. Příslušné oblasti politik podle členění ABM/ABB³⁵

Výzkum a inovace

Evropské strategické investice

1.3. Povaha návrhu/podnětu

☒ Návrh/podnět se týká **nové akce**

☐ Návrh/podnět se týká **nové akce následující po pilotním projektu / přípravné akci**³⁶

☐ Návrh/podnět se týká **prodloužení stávající akce**

☐ Návrh/podnět se týká **akce přesměrované na jinou akci**

1.4. Cíle

1.4.1. Víceleté strategické cíle Komise sledované návrhem/podnětem

1. Propojený jednotný digitální trh

2. Nový impuls pro zaměstnanost, růst a investice

1.4.2. Dotčené specifické cíle

Specifické cíle

1.3 Digitální ekonomika může plně využít svůj potenciál, bude-li podporována iniciativami umožňujícími plný rozvoj digitálních a datových technologií.

2.1 Evropa si drží své vedoucí světové postavení v digitální ekonomice, v níž mohou evropské společnosti díky silnému digitálnímu podnikatelskému duchu a úspěšným začínajícím podnikům růst v celosvětovém měřítku a v níž průmysl i veřejné služby úspěšně prošly digitální transformací.

2.2 Evropský výzkum nalézá investiční příležitosti pro potenciálně průlomové a stěžejní technologie, zejména prostřednictvím programu Horizont 2020 / Horizont Evropa a za použití partnerství veřejného a soukromého sektoru.

³⁵ ABM: řízení podle činností (*activity-based management*); ABB: sestavování rozpočtu podle činností (*activity-based budgeting*).

³⁶ Podle čl. 54 odst. 2 písm. a) nebo b) finančního nařízení.

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Kompetenční centrum bude společně se sítí a komunitou usilovat o dosažení těchto cílů:

- 1) přispívat k provádění části zaměřené na kybernetickou bezpečnost v rámci programu Digitální Evropa zavedeného nařízením č. XXX, zejména opatření souvisejících s článkem 6 nařízení (EU) č. XXX [program Digitální Evropa], a v rámci programu Horizont Evropa zavedeného nařízením č. XXX, zejména bodu 2.2.6 přílohy I rozhodnutí č. XXX o zavedení zvláštního programu, kterým se provádí rámcový program pro výzkum a inovace Horizont Evropa, pro provádění programu Horizont Evropa – rámcového programu pro výzkum a inovace, a v rámci dalších unijních programů, stanoví-li tak právní akty Unie];
- 2) zlepšovat schopnosti, znalosti a infrastruktury v oblasti kybernetické bezpečnosti ve prospěch průmyslových odvětví, veřejného sektoru a výzkumných komunit;
- 3) přispívat k plošnému nasazení nejnovějších produktů a řešení v oblasti kybernetické bezpečnosti napříč celou ekonomikou;
- 4) zlepšovat povědomí o kybernetické bezpečnosti a přispívat ke snižování nedostatku dovedností v oblasti kybernetické bezpečnosti v Unii;
- 5) přispívat k posílení výzkumu a vývoje v oblasti kybernetické bezpečnosti v Unii;
- 6) posilovat spolupráci mezi civilní a obranou oblastí s ohledem na technologie a aplikace dvojího užití;
- 7) posilovat synergie mezi civilním a obranným rozměrem kybernetické bezpečnosti;
- 8) pomáhat koordinovat a usnadňovat práci sítě národních koordinačních center (dále jen „sítě“) podle článku 10 a komunity kompetencí pro kybernetickou bezpečnost podle článku 12.

1.4.4. Ukazatele výsledků a dopadů

Upřesněte ukazatele, podle kterých je možno uskutečňování návrhu/podnětu sledovat.

- Počet společně zadáných veřejných zakázek na infrastruktury/nástroje v oblasti kybernetické bezpečnosti.
- Možnost evropských výzkumných pracovníků a průmyslu v rámci sítě a centra využívat čas na testovacích a experimentálních zařízeních. Pokud zařízení již existují, vyšší počet hodin, který je těmto komunitám k dispozici, v porovnání se stávající situací.
- Růst počtu uživatelských komunit, kterým byly poskytnuty služby, a počtu výzkumných pracovníků, kteří získali přístup k evropským zařízením v oblasti kybernetické bezpečnosti, v porovnání s počtem komunit a výzkumných pracovníků, kteří musejí tyto prostředky hledat mimo Evropu.
- Začne se zvyšovat konkurenceschopnost evropských dodavatelů, měřeno podílem na světovém trhu (cílem je 25% podíl na trhu do roku 2027) a podílem výsledků evropského výzkumu a vývoje využívaných v průmyslu.

- Přispívání k budoucím technologiím kybernetické bezpečnosti, měřeno z hlediska autorských práv, patentů, vědeckých publikací a komerčních produktů.
- Počet posouzených a sladěných vzdělávacích programů v oblasti kybernetické bezpečnosti, počet posouzených odborných certifikačních programů v oblasti kybernetické bezpečnosti.
- Počet vyškolených vědců, studentů a uživatelů (v rámci průmyslu a veřejné správy).

1.5. Odůvodnění návrhu/podnětu

1.5.1. *Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu*

Je třeba dosáhnout kritického množství investic do technologií a průmyslového vývoje v oblasti kybernetické bezpečnosti a překonat roztržičnost příslušných kapacit po celé EU.

1.5.2. *Přidaná hodnota ze zapojení EU*

Kybernetická bezpečnost představuje společný zájem Unie, jak dokládají závěry Rady zmíněné výše. Rozsah a přeshraniční charakter incidentů jako *WannaCry* nebo *NonPetya* to jenom dokazují. Povaha a rozsah technologických problémů v oblasti kybernetické bezpečnosti i nedostatečná koordinace úsilí mezi průmyslem, veřejným sektorem a výzkumnými komunitami, jakož i v rámci těchto skupin vyžaduje od EU další podporu koordinačních úsilí jak ke sloučení kritického množství prostředků, tak k zajištění lepších znalostí a správy aktiv. Je to nezbytné vzhledem k požadavkům na prostředky souvisejícím s některými schopnostmi potřebnými k výzkumu, vývoji a nasazování v oblasti kybernetické bezpečnosti; potřebě poskytnout přístup k interdisciplinárnímu know-how v oblasti kybernetické bezpečnosti z různých oborů (často dostupnému jen částečně na vnitrostátní úrovni); globálnímu charakteru průmyslových hodnotových řetězců i aktivitám globálních konkurentů napříč trhy.

To vše vyžaduje prostředky a odborné znalosti v rozsahu, kterého lze jen těžko dosáhnout opatřeními jakéhokoli jednotlivého členského státu. Například celoevropská kvantová komunikační síť by mohla vyžadovat investici EU v řádu 900 milionů EUR v závislosti na investicích členských států (zda budou propojené / budou se doplňovat) a také na tom, v jakém rozsahu bude technicky možné využít stávající infrastruktury.

1.5.3. *Závěry vyvozené z podobných zkušeností v minulosti*

Průběžné hodnocení programu Horizont 2020 mimo jiné potvrdilo trvalý význam podpory EU v oblasti výzkumu a vývoje a společenských výzev (včetně „bezpečných společností“, z nichž je podporován výzkum a vývoj kybernetické bezpečnosti). Zároveň hodnocení potvrzuje, že posílení vedoucího postavení v průmyslu zůstává výzvou a i nadále přetrvávají rozdíly v inovacích, přičemž EU zaostává, pokud jde o průlomové inovace vytvářející nové trhy.

Hodnocení v polovině období Nástroje pro propojení Evropy zřejmě potvrzuje přidanou hodnotu zapojení EU nad rámec výzkumu a vývoje, ačkoli kybernetická bezpečnost měla v rámci Nástroje pro propojení Evropy trochu jiné zaměření (na provozní bezpečnost) a logiku intervence. Zároveň se většina příjemců grantů v oblasti kybernetické bezpečnosti v rámci Nástroje pro propojení Evropy, tedy komunita národních týmů CSIRT, vyjádřila v tom smyslu, že by si v rámci příštího víceletého finančního rámce přála zvláštní program podpory.

Vytvoření smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost v EU v roce 2016 bylo prvním významným krokem pro větší propojení výzkumných komunit, průmyslu a veřejného sektoru v zájmu usnadnění výzkumu a inovací v oblasti kybernetické bezpečnosti a v rámci mezí daných finančním rámcem na období 2014–2020 by mělo vést k dobrým a lépe cíleným výsledkům v oblasti výzkumu a inovací. Uvedené partnerství umožnilo průmyslovým partnerům vyjádřit závazek o jejich individuálních výdajích v oblastech vymezených v jeho programu strategického výzkumu a inovací.

1.5.4. Soulad a možná synergie s dalšími vhodnými nástroji

Sít kompetencí pro kybernetickou bezpečnost a Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost budou působit jako doplňující podpora pro stávající právní předpisy a subjekty v oblasti kybernetické bezpečnosti. Mandát Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost bude doplňovat úsilí agentury ENISA, ale bude mít jiné zaměření a vyžaduje odlišný soubor schopností. Agentura ENISA sice hraje roli v poradenské činnosti v rámci výzkumu a inovací v oblasti kybernetické bezpečnosti v EU, avšak její navrhovaný mandát se soustředí především na jiné úkoly nezbytné k posílení odolnosti EU v oblasti kybernetické bezpečnosti. Kompetenční centrum by mělo stimulovat rozvoj a zavádění technologií v oblasti kybernetické bezpečnosti a doplnit úsilí zaměřené na budování kapacit v této oblasti na úrovni EU a na vnitrostátní úrovni.

Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost bude společně se sítí kompetencí pro kybernetickou bezpečnost také usilovat o podporu výzkumu s cílem usnadnit a zrychlit procesy standardizace a certifikace, zejména v souvislosti se systémy certifikace kybernetické bezpečnosti ve smyslu aktu o kybernetické bezpečnosti.

Evropské průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost bude působit jako jediný prováděcí mechanismus pro dva evropské programy na podporu kybernetické bezpečnosti (programy Digitální Evropa a Horizont Evropa) a zvýší jejich soudržnost a synergie mezi nimi.

Tato iniciativa umožňuje doplnit snahy členských států tím, že poskytne vhodné vstupy pro tvůrce politiky v oblasti vzdělávání s cílem zlepšit vzdělávání v oblasti kybernetické bezpečnosti (např. vytvořením vzdělávacích programů v oblasti kybernetické bezpečnosti v rámci civilních a vojenských vzdělávacích systémů, ale rovněž poskytováním vstupů pro základní vzdělávání v oblasti kybernetické bezpečnosti). Dále by umožnila podpořit sladění a průběžné posuzování odborných certifikačních programů v oblasti kybernetické bezpečnosti, což jsou všechno nezbytné činnosti přispívající k řešení nedostatku dovedností v oblasti kybernetické bezpečnosti a usnadňující přístup průmyslu i dalších komunit k odborníkům v oblasti kybernetické bezpečnosti. Sladění vzdělávání a dovedností pomůže v EU vytvořit kvalifikovanou pracovní sílu v oblasti kybernetické bezpečnosti, která bude představovat klíčovou výhodu pro společnosti v oblasti kybernetické bezpečnosti i v dalších odvětvích, která mají zájem na kybernetické bezpečnosti.

1.6. Doba trvání akce a finanční dopad

☒ **Časově omezený návrh/podnět**

- ☒ Návrh/podnět s platností od 1. 1. 2021 do 31. 12. 2029
- ☒ Finanční dopad od roku 2021 do roku 2027 pro prostředky na závazky a od roku 2021 do roku 2031 pro prostředky na platby.

☐ **Časově neomezený návrh/podnět**

- Provádění s obdobím rozběhu od RRRR do RRRR,
- poté plné fungování.

1.7. Předpokládaný způsob řízení³⁷

☐ **Přímé řízení Komisí**

- ☐ prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie;
- ☐ prostřednictvím výkonných agentur;

☐ **Sdílené řízení s členskými státy**



Nepřímé řízení, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

- ☐ třetí země nebo subjekty určené těmito zeměmi;
- ☐ mezinárodní organizace a jejich agentury (upřesněte);
- ☐ EIB a Evropský investiční fond;
- ☒ subjekty uvedené v článcích 70 a 71 finančního nařízení;
- ☐ veřejnoprávní subjekty;
- ☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky;
- ☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství soukromého a veřejného sektoru a poskytující dostatečné finanční záruky;
- ☐ osoby pověřené prováděním zvláštních činností v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.
- *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

³⁷

Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Článek 28 obsahuje podrobná ustanovení o sledování a podávání zpráv.

2.2. Systém řízení a kontroly

2.2.1. Zjištěná rizika

S cílem zmírnit rizika související s provozem kompetenčního centra po jeho zřízení a prodlevách bude Komise v této fázi kompetenční centrum podporovat, aby byl zajištěn rychlý nábor klíčového personálu a zavedení účinného systému vnitřní kontroly a řádných postupů.

2.2.2. Informace o zavedeném systému vnitřní kontroly

Výkonný ředitel odpovídá za provoz a každodenní řízení kompetenčního centra a je jeho právním zástupcem. Ředitel je odpovědný správní radě a podává jí průběžně zprávy o vývoji činností kompetenčního centra.

Správní rada nese celkovou odpovědnost za strategickou orientaci a činnost kompetenčního centra a dohlíží na provádění jeho činností.

Správní rada přijme po konzultaci s Komisí finanční pravidla použitelná pro kompetenční centrum. Tato finanční pravidla se mohou odchýlit od nařízení (EU) č. 1271/2013, pouze pokud je to specificky vyžadováno pro provoz kompetenčního centra a s předchozím souhlasem Komise.

Interní auditor Komise vykonává vůči kompetenčnímu centru stejné pravomoci jako vůči Komisi. Účetní dvůr je oprávněn provádět formou kontroly dokumentů a kontroly na místě audit u všech příjemců grantů, dodavatelů a subdodavatelů, kteří od kompetenčního centra obdrželi finanční prostředky Unie.

2.2.3. Odhad nákladů a přínosů kontrol a posouzení očekávané míry rizika výskytu chyb

Náklady na kontroly a jejich přínos

Náklady na kontrolu Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost se dělí na náklady na dohled na úrovni Komise a náklady na provozní kontroly na úrovni provádějícího subjektu.

Náklady na kontroly na úrovni kompetenčního centra se odhadují přibližně na 1,19 % z prostředků na provozní platby prováděné na úrovni kompetenčního centra.

Náklady na dohled na úrovni Komise se odhadují na přibližně 1,20 % z prostředků na provozní platby použitých na úrovni kompetenčního centra.

Za předpokladu, že by tyto činnosti byly v plném rozsahu řízeny Komisí bez podpory provádějícího subjektu, by náklady na kontrolu byly výrazně vyšší a mohly by se pohybovat okolo 7,7 % z prostředků na platby.

Cílem předpokládaných kontrol je zajistit bezproblémový a účinný dohled Komise nad provádějícími subjekty a nezbytnou míru jistoty na úrovni Komise.

Přínosy kontrol jsou tyto:

- vyvarování se výběru slabších či nedostatečných návrhů,

- optimalizace plánování a využití finančních prostředků EU, aby se zachovala přidaná hodnota EU,
- zajištění kvality grantových dohod, vyvarování se chyb v označení právních subjektů, zajištění správného výpočtu příspěvků EU a přijetí potřebných záruk pro správné poskytování grantů,
- odhalení nezpůsobilých nákladů ve fázi platby,
- odhalení chyb, které mají vliv na legalitu a správnost operací ve fázi auditu.

Odhadovaná míra chyb

Cílem je udržovat zbytkovou chybovost pod hranicí 2 % pro celý program a zároveň omezovat zátěž představovanou kontrolami pro příjemce, aby bylo dosaženo správné rovnováhy mezi cílem legality a správnosti a dalšími cíli, například přitažlivostí programu zejména pro malé a střední podniky a náklady na kontroly.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření.

Úřad OLAF smí provádět vyšetřování, včetně kontrol a inspekcí na místě, v souladu s ustanoveními a postupy stanovenými nařízením Evropského parlamentu a Rady č. 883/2013 a nařízením Rady (Euratom, ES) č. 2185/9640 ze dne 11. listopadu 1996 o kontrolách a inspekcích na místě prováděných Komisí za účelem ochrany finančních zájmů Unie proti podvodům a jiným nesrovnalostem, aby se zjistilo, zda v souvislosti s grantem nebo smlouvou financovanými ze strany kompetenčního centra nedošlo k podvodu, korupci nebo jinému protiprávnímu jednání s dopadem na finanční zájmy Unie.

Dohody, rozhodnutí a smlouvy vyplývající z provádění tohoto nařízení musí obsahovat ustanovení, která Komisi, kompetenční centrum, Účetní dvůr a úřad OLAF výslovně zmocňují k provádění auditů a vyšetřování v souladu s jejich příslušnými pravomocemi.

Kompetenční centrum zajistí, aby finanční zájmy jeho členů byly přiměřeně chráněny prostřednictvím provádění nebo zadávání vhodných vnitřních a vnějších kontrol.

Kompetenční centrum přistoupí k interinstitucionální dohodě ze dne 25. května 1999 mezi Evropským parlamentem, Radou Evropské unie a Komisí Evropských společenství o vnitřním vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF). Kompetenční centrum přijme nezbytná opatření pro usnadnění vnitřního vyšetřování vedeného úřadem OLAF.

Kompetenční centrum přijme strategii pro boj proti podvodům na základě analýz a zvážení rizika podvodu a nákladů a přínosů. Chrání finanční zájmy Unie uplatňováním preventivních opatření proti podvodům, korupci a jakýmkoli jiným protiprávním jednáním, účinnými kontrolami a zpětným získáním nesprávně vyplacených částek v případech, kdy jsou zjištěny nesrovnalosti, a případně účinnými, přiměřenými a odrazujícími správními a finančními sankcemi.

--

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruh víceletého finančního rámce a nově navržené výdajové rozpočtové položky

- Nové rozpočtové položky, jejichž vytvoření se požaduje

V pořadí okruhů víceletého finančního rámce a rozpočtových položek:

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	číslo	RP/NRP ³⁸	zemí ESVO ³⁹	kandidátských zemí ⁴⁰	třetích zemí	ve smyslu čl. [21 odst. 2 písm. b)] finančního nařízení
Okruh 1: Jednotný trh, inovace a digitální ekonomika	01 02 XX XX Horizont Evropa – průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost – podpůrné výdaje	RP	ANO	ANO (je-li stanoven v ročním pracovním programu)	ANO (pouze u některých částí programu)	NE
	01 02 XX XX Horizont Evropa – průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost					
	02 06 01 XX program Digitální Evropa – průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost – podpůrné výdaje					
	02 06 01 XX program Digitální Evropa – průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost					

- Očekává se, že příspěvky k těmto rozpočtovým položkám budou pocházet z:

³⁸ RP = rozlišené prostředky / NRP = nerozlišené prostředky.

³⁹ ESVO: Evropské sdružení volného obchodu.

⁴⁰ Kandidátské země a případně potenciální kandidátské země západního Balkánu.

v milionech EUR (zaokrouhleno na tři desetinná místa)

Rozpočtová položka	Rok 2021	Rok 2022	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	Celkem
01 01 01 01 Výdaje související s úředníky a dočasnými zaměstnanci ve výzkumu – Horizont Evropa	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 02 Externí zaměstnanci provádějící výzkumné programy – Horizont Evropa	pm	pm	pm	pm	pm	pm	pm	pm
01 01 01 03 Další výdaje na řízení výzkumu – Horizont Evropa	pm	pm	pm	pm	pm	pm	pm	pm
01 02 02 Globální výzvy a konkurenceschopnost průmyslu	pm	pm	pm	pm	pm	pm	pm	pm
02 01 04 Administrativní podpora – program Digitální Evropa	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
02 06 01 Kybernetická bezpečnost – program Digitální Evropa	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
Výdaje celkem	286,130	325,274	331,320	252,200	257,189	262,186	267,368	1 981,668

Výši příspěvku z finančního krytí klastru „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 21 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody. Návrh bude vycházet z výsledku procesu strategického plánování podle definice v čl. 6 odst. 6 nařízení XXX [rámcový program Horizont Evropa].

Výše uvedené částky nezahrnují příspěvek od členských států na provozní a správní náklady kompetenčního centra, souměřitelný s finančním příspěvkem Unie.

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce			1	Jednotný trh, inovace a digitální ekonomika							
			2021 ⁴¹	2022	2023	2024	2025	2026	2027	Po roce 2027	CELKEM
Hlava 1 (Výdaje na zaměstnance)	Závazky = platby	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
Hlava 2 (Infrastruktura a provozní výdaje)	Závazky = platby	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		11,873
Hlava 3 (Provozní výdaje)	Závazky	(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
Prostředky na krytí programů CELKEM⁴²	Závazky	= 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 Prostředky na zaměstnance jsou uvedeny pouze na půl roku v roce 2021.

⁴² Uvedené prostředky na krytí se vztahují pouze na finanční prostředky EU určené na kybernetickou bezpečnost v rámci programu Digitální Evropa. Výši příspěvku z finančního krytí klastru „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 5 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody. Návrh bude vycházet z výsledku procesu strategického plánování podle definice v čl. 6 odst. 6 nařízení XXX [rámcový program Horizont Evropa].

Okruh víceletého finančního rámce	7	„Správní výdaje“
--	----------	------------------

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2021	2022	2023	2024	2025	2026	2027	Po roce 2027	CELKEM
Lidské zdroje		3,090	3,233	3,233	3,233	3,233	3,233	3,805		23,060
Ostatní správní výdaje		0,105	0,100	0,104	0,141	0,147	0,153	0,159		0,909
CELKEM prostředky na OKRUH 7 víceletého finančního rámce	(Závazky celkem = platby celkem)	3,195	3,333	3,337	3,374	3,380	3,386	3,964		23,969

v milionech EUR (zaokrouhleno na tři desetinná místa)

		2021	2022	2023	2024	2025	2026	2027	Po roce 2027	CELKEM
CELKEM prostředky z OKRUHŮ víceletého finančního rámce	Závazky	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 ² 061,715	2 005,637

3.2.2. Odhadovaný souhrnný dopad na prostředky správní povahy

- ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.
- ☒ Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

Roky	2021	2022	2023	2024	2025	2026	2027	CELKEM
------	------	------	------	------	------	------	------	--------

OKRUH 7 víceletého finančního rámce								
Lidské zdroje	3,090	3,233	3,233	3,233	3,233	3,233	3,805	23,060
Ostatní správní výdaje	0,105	0,100	0,104	0,141	0,147	0,153	0,159	0,909
Mezisoučet za OKRUH 7 víceletého finančního rámce	3,195	3,333	3,337	3,374	3,380	3,386	3,964	23,969

Mimo OKRUH 7⁴³ víceletého finančního rámce								
Lidské zdroje								
Ostatní výdaje správní povahy	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Mezisoučet mimo OKRUH 7 víceletého finančního rámce	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746

CELKEM	4,433	6,363	7,079	7,192	7,274	7,358	8,016	47,715
---------------	--------------	--------------	--------------	--------------	--------------	--------------	--------------	---------------

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GŘ, a případně doplněny z dodatečného přidělu, který lze řídicímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Výše uvedené potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy mimo okruh 7 odpovídají částkám pokrytým finančním příspěvkem Unie z programu Digitální Evropa.

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy mimo okruh 7 budou povýšeny o částky pokryté finančním příspěvkem Unie z programu Horizont Evropa, jakmile výši příspěvku z finančního krytí klastru „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 21 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody.

Výše uvedené potřebné prostředky na oblast lidských zdrojů a na další výdaje správní povahy mimo okruh 7 nezahrnují příspěvek od členských států na správní náklady kompetenčního centra, souměřitelný s finančním příspěvkem Unie.

⁴³ Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.2.1. Odhadované potřeby v oblasti lidských zdrojů v Komisi

- ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.
- ☒ Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

Roky		2021	2022	2023	2024	2025	2026	2027
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
v ústředí a v zastoupeních Komise		20	21	21	21	21	21	22
při delegacích								
ve výzkumu								
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE) - SZ, MZ, VNO, ZAP a MOD ⁴⁴								
Okruh 7								
Financováno z OKRUHU 7 víceletého finančního rámce	- v ústředí	3	3	3	3	3	3	3
	- při delegacích							
Financováno z krytí programu ⁴⁵	- v ústředí							
	- při delegacích							
ve výzkumu								
Jiná (upřesněte)								
CELKEM		23	23	24	24	24	25	25

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GR, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GR, a případně doplněny z dodatečného přidělu, který lze řídicímu GR poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Popis úkolů:

Úředníci a dočasní zaměstnanci	Koordinace, monitorování a řízení úkolů svěřených Evropskému průmyslovému, technologickému a výzkumnému centru kompetencí pro kybernetickou bezpečnost, včetně nákladů na podporu a koordinaci. Tvorba politiky a koordinace v oblasti kybernetické bezpečnosti v souvislosti s úkoly svěřenými Evropskému průmyslovému, technologickému a výzkumnému centru kompetencí pro kybernetickou bezpečnost, např. s ohledem na určení priorit výzkumné a průmyslové politiky, obecnou spolupráci mezi členskými státy a hospodářskými subjekty, soulad s budoucím rámcem EU pro certifikaci kybernetické bezpečnosti, činnost související s odpovědností a povinnostmi péče nebo koordinace s politikami, které upravují HPC, umělou inteligenci a digitální dovednosti. .
Externí zaměstnanci	Koordinace, monitorování a řízení úkolů svěřených Evropskému průmyslovému, technologickému a výzkumnému centru kompetencí pro kybernetickou bezpečnost, včetně nákladů na podporu a koordinaci. Tvorba politiky a koordinace v oblasti kybernetické bezpečnosti v souvislosti s úkoly svěřenými Evropskému průmyslovému, technologickému a výzkumnému centru kompetencí pro kybernetickou bezpečnost, např. s ohledem na určení priorit výzkumné a průmyslové politiky, obecnou spolupráci mezi členskými státy a hospodářskými subjekty, soulad s budoucím rámcem EU pro certifikaci kybernetické bezpečnosti, činnost související s odpovědností a povinnostmi péče nebo koordinace s politikami, které upravují HPC, umělou inteligenci a digitální dovednosti. .

⁴⁴ SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

⁴⁵ Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.2.2. Odhadované potřeby v oblasti lidských zdrojů na průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost

	2021	2022	2023	2024	2025	2026	2027
Úředníci Komise							
z toho AD							
z toho AST							
z toho AST-SC							
Dočasní zaměstnanci							
z toho AD	10	11	13	13	13	13	13
z toho AST							
z toho AST-SC							
Smluvní zaměstnanci	26	32	39	39	39	39	39
Vyslaní národní odborníci	1	1	1	1	1	1	1
Celkem	37	44	53	53	53	53	53

Popis úkolů:

Úředníci a dočasní zaměstnanci	Provozní provádění úkolů svěřených Evropskému průmyslovému, technologickému a výzkumnému centru kompetencí pro kybernetickou bezpečnost podle článku 4 tohoto nařízení, včetně nákladů na podporu a koordinaci.
Externí zaměstnanci	Provozní provádění úkolů svěřených Evropskému průmyslovému, technologickému a výzkumnému centru kompetencí pro kybernetickou bezpečnost podle článku 4 tohoto nařízení, včetně nákladů na podporu a koordinaci.

Výše uvedené odhadované potřeby v oblasti lidských zdrojů pro průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost odpovídají odhadovaným potřebám na provedení finančního příspěvku Unie v rámci programu Digitální Evropa.

Výše uvedené odhadované potřeby v oblasti lidských zdrojů pro průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost budou navýšeny o odhadované potřeby na provedení finančního příspěvku Unie v rámci programu Horizont Evropa, jakmile vyšší příspěvku z finančního krytí klastru „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 21 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody.

3.2.2.3. Plán pracovních míst průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost

	2021	2022	2023	2024	2025	2025	2025
Funkční skupina a platová třída							
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
Celkem AD	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							
Celkem AST							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							
Celkem AST/SC							
CELKOVÝ SOUČET	10	11	13	13	13	13	13

3.2.2.4. Odhadovaný dopad na zaměstnance (dodatečné) – externí zaměstnanci průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost

	2021	2022	2023	2024	2025	2026	2027
Smluvní zaměstnanci							
Funkční skupina IV	20	22	29	29	29	29	29
Funkční skupina III	2	4	4	4	4	4	4
Funkční skupina II	4	6	6	6	6	6	6
Funkční skupina I							
Celkem	26	32	39	39	39	39	39

Za účelem zajištění neutrality, pokud jde o počet zaměstnanců, budou dodatečné počty zaměstnanců průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost částečně kompenzovány snížením počtu úředníků a externích zaměstnanců (tj. plán pracovních míst a aktuální externí personál) v příslušných útvarech Komise.

Počet zaměstnanců průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost uvedený v bodech 3.2.2.2–4 bude kompenzován následovně⁴⁶:

CELKEM	2021	2022	2023	2024	2025	2026	2027
Úředníci Komise	5	5	6	6	6	6	6
Dočasní zaměstnanci							
Smluvní zaměstnanci	14	17	20	20	20	20	20
Vyslání národní odborníci							
FTE celkem	19	22	26	26	26	26	26
Počet zaměstnanců	19	22	26	26	26	26	26

Kompenzace lidských zdrojů průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost bude souměřitelná s podílem finančního příspěvku Unie, tj. 50 %.

Výše uvedená kompenzace se vztahuje na odhadované potřeby v oblasti lidských zdrojů pro průmyslové, technologické a výzkumné centrum kompetencí pro kybernetickou bezpečnost na provedení finančního příspěvku Unie z programu Digitální Evropa.

⁴⁶ V závislosti na konečné výši rozpočtu, jehož plněním bude kompetenční centrum pověřeno.

Výše uvedená kompenzace bude navýšena o odhadované potřeby na provedení finančního příspěvku Unie z programu Horizont Evropa, jakmile výši příspěvku z finančního krytí klastru „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 21 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody.

3.2.3. Příspěvky třetích stran

Návrh/podnět:

- ☐ nepočítá se spolufinancováním od třetích stran.
- ☒ počítá se spolufinancováním od třetích stran⁴⁷ podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

Roky	2021	2022	2023	2024	2025	2026	2027	CELKEM
Členské státy – příspěvky na výdaje na zaměstnance	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Členské státy – příspěvky na výdaje na infrastrukturu a provozní výdaje	0,619	1,515	1,871	1,909	1,947	1,986	2,026	11,873
Členské státy – příspěvky na provozní výdaje	284,892	322,244	327,578	248,382	253,295	258,214	263,316	1 957,922
Spolufinancované prostředky CELKEM	286,130	325,274	331,320	252,200	257,189	262,186	267,368	1 981,668

Výše uvedený příspěvek třetích stran se vztahuje pouze na spolufinancování souměřitelné s finančními prostředky EU určenými na kybernetickou bezpečnost z programu Digitální Evropa. Výše uvedený příspěvek třetích stran bude navýšen, jakmile výši příspěvku z finančního krytí klastru „Inkluzivní a bezpečná společnost“ v rámci pilíře II „Globální výzvy a konkurenceschopnost průmyslu“ programu Horizont Evropa (celkové krytí 2 800 000 000 EUR) podle čl. 21 odst. 1 písm. b) navrhne Komise během legislativního procesu a v každém případě před dosažením politické dohody. Návrh bude vycházet z výsledku procesu strategického plánování podle definice v čl. 6 odst. 6 nařízení XXX [rámcový program Horizont Evropa].

3.3. Odhadovaný dopad na příjmy

- ☒ Návrh/podnět nemá žádný finanční dopad na příjmy.
- ☐ Návrh/podnět má tento finanční dopad:

☐ dopad na vlastní zdroje

☐ dopad na různé příjmy

uved'te, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová položka:	rozpočtová	Dopad návrhu/podnětu ⁴⁸						
		2021	2022	2023	2024	2025	2026	2027
Článek								

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

⁴⁷ Odhad věcných příspěvků od členských států

⁴⁸ Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).