EVROPSKÁ
KOMISE

V Bruselu dne 12.9.2018
SWD(2018) 404 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN POSOUZENÍ DOPADŮ

Průvodní dokument k

NÁVRHU NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

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

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Souhrnný přehled

Posouzení dopadů pro: návrh na vytvoření sítě kompetenčních center a Evropského průmyslového, technologického a výzkumného centra kompetencí pro kybernetickou bezpečnost

A. Potřeba opatření

Proč? Jaký problém se řeší?

V současnosti EU stále chybí dostačující technické a průmyslové kapacity, aby mohla samostatně zabezpečit svou ekonomiku a kritické infrastruktury a získala vedoucí postavení v oblasti kybernetické bezpečnosti v celosvětovém měřítku. Cílem předkládané iniciativy je přispět k řešení následujících problémů a souvisejících faktorů, které k současnému stavu přispívají:

Problém č. 1: Nedostačující úroveň strategické a udržitelné koordinace a spolupráce mezi průmyslovými odvětvími, výzkumnými komunitami v oblasti kybernetické bezpečnosti a vládami, pokud jde o ochranu ekonomiky, společnosti a demokracie nejmodernějšími evropskými řešeními v oblasti kybernetické bezpečnosti.

Problém č. 2: Nedostačující investice do know-how, dovedností a zařízení v oblasti kybernetické bezpečnosti po celé Evropě a omezený přístup k nim.

Problém č. 3: Jen málo výsledků evropského výzkumu a inovací v oblasti kybernetické bezpečnosti vede k vytvoření řešení uplatnitelných na trhu a široce nasazených v celé ekonomice.

Tyto problémy mají řadu příčin, včetně nedostatečné úrovně důvěry mezi různými hráči na trhu kybernetické bezpečnosti, nedílných omezení stávající spolupráce a mechanismů pro sdružování prostředků, chybějícího rámce pro společné zadávání veřejných zakázek na nákladnou infrastrukturu a produkty/řešení v oblasti kybernetické bezpečnosti i nevyužitého potenciálu odrazujících a motivujících tržních mechanismů.

Čeho by měla tato iniciativa dosáhnout?

Cílem této iniciativy je zajistit, aby si EU udržela a vyvinula důležité (technické a průmyslové) kapacity, aby mohla sama zabezpečit svou digitální ekonomiku, společnost a demokracii, a aby členské státy mohly využívat nejpokročilejší řešení v oblasti kybernetické bezpečnosti a schopnosti v oblasti kybernetické obrany. Dále je cílem této iniciativy zvýšit celosvětovou konkurenceschopnost společností v EU působících v oblasti kybernetické bezpečnosti a zajistit, aby různé sektory evropského průmyslu měly přístup ke kapacitám a prostředkům, které jim umožní učinit z kybernetické bezpečnosti svou konkurenční výhodu. Těchto cílů by mělo být dosaženo vytvořením účinných mechanismů pro dlouhodobou strategickou spolupráci mezi všemi dotčenými hráči (orgány veřejné moci, podniky, civilní i obrannou vědeckou komunitou), sdružováním znalostí a prostředků v zájmu poskytování špičkových schopností a infrastruktur, podporou širokého nasazení evropských produktů a řešení v oblasti kybernetické bezpečnosti napříč celou ekonomikou a veřejným sektorem, podporou začínajících podniků a malých a středních podniků v oblasti kybernetické bezpečnosti, jakož i pomocí v souvislosti s řešením nedostatku dovedností v oblasti kybernetické bezpečnosti.

Jakou přidanou hodnotu budou mít tato opatření na úrovni EU?

Iniciativa by přidala hodnotu ke stávajícímu úsilí na vnitrostátní úrovni tím, že by přispěla k vytvoření propojeného celoevropského ekosystému kybernetické bezpečnosti zahrnujícího průmysl i výzkum. Měla by podnítit lepší spolupráci mezi relevantními zúčastněnými stranami (též mezi civilními a obrannými sektory v oblasti kybernetické bezpečnosti), aby se co nejlépe využily stávající prostředky a odborné znalosti v oblasti kybernetické bezpečnosti, které jsou rozesety po celé Evropě. Měla by pomoci EU a členským státům zaujmout proaktivní, dlouhodobý a strategický přístup k průmyslové politice v oblasti kybernetické bezpečnosti, který překročí hranice výzkumu a vývoje. Tento přístup by měl pomoci nejen najít průlomová řešení výzev v oblasti kybernetické bezpečnosti, kterým soukromý i veřejný sektor čelí, ale také podpořit účinné nasazení těchto řešení. Rovněž umožní příslušným výzkumným a průmyslovým komunitám i orgánům veřejné moci získat přístup ke klíčovým schopnostem, jako jsou testovací a experimentální zařízení, která jsou často kvůli nedostatečným finančním a lidským zdrojům mimo dosah jednotlivých členských států. Rovněž přispěje k řešení nedostatku v oblasti dovedností a předejde odlivu mozků, neboť rozsáhlým evropským projektům zajistí přístup k nejlepším talentům, čímž nabídne zajímavé profesní výzvy. Všechny výše uvedené faktory jsou také považovány za nutný předpoklad, aby se Evropa mohla stát celosvětově uznávaným předním hráčem v oblasti kybernetické bezpečnosti.

B. Řešení

Jaké legislativní a nelegislativní možnosti byly zvažovány? Je některá možnost upřednostňována? Proč?

Byla zvážena řada legislativních i nelegislativních možností politiky. V hloubkovém posouzení byly ponechány následující možnosti:

1. **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 programu Horizont Evropa.
2. **Možnost č. 1:** Síť kompetencí pro kybernetickou bezpečnost s Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost, které jsou zmocněny k provádění opatření na podporu průmyslových technologií i v oblasti výzkumu a vývoje.
3. **Možnost č. 2:** Síť kompetencí pro kybernetickou bezpečnost a Evropské výzkumné a odborné středisko pro kybernetickou bezpečnost zaměřené pouze na činnosti v oblasti výzkumu a inovací.

Mezi možnosti, které byly zamítnuty již v počáteční fázi, patřily: 1) žádná opatření, 2) pouze síť stávajících kompetenčních center a 3) využití stávající agentury (ENISA, REA nebo INEA).

Vzhledem k obecnému závazku, který již Komise ve vztahu k této iniciativě učinila, jakož i k významné roli, kterou mají hrát členské státy, je hlavním rozdílem mezi těmito dvěma podrobně analyzovanými možnostmi politiky jejich rozsah, jež se odráží v jejich právním základě: subjekt založený pouze na článku 187 SFEU (možnost č. 2) by omezil iniciativu na oblast výzkumu a inovací a zpravidla by předpokládal finanční příspěvek od soukromých subjektů. Naopak subjekt založený na dvojím právním základě – článku 187 SFEU a článku 173 SFEU (možnost č. 1) – by znamenal širší mandát, který by mimo jiné zahrnoval i nasazení, podporu průmyslu a vytváření silnějších synergií se sektorem kybernetické obrany. Také členské státy by hrály významnější roli – jak z hlediska řízení, tak i jako možní zadavatelé veřejných zakázek na technologie v oblasti kybernetické bezpečnosti.

Analýza ukázala, že k dosažení cílů iniciativy je nejvhodnější možnost č. 1, která zároveň bude mít nejpříznivější dopady na hospodářství, společnost a životní prostředí a zaručí zájmy Unie. Hlavní argumenty ve prospěch této možnosti zahrnovaly flexibilitu umožňující různé modely spolupráce s komunitou a sítí kompetenčních center, aby byly optimálně využity stávající znalosti a prostředky; možnost strukturovat spolupráci veřejných a soukromých zúčastněných stran ze všech relevantních odvětví včetně obrany; schopnost vytvořit skutečnou průmyslovou politiku v oblasti kybernetické bezpečnosti podporou činností spojených nejen s výzkumem a vývojem, ale i s uváděním na trh. Nakonec možnost č. 1 umožňuje také zvýšení soudržnosti tím, že iniciativa bude fungovat jako prováděcí mechanismus pro poskytování finančních prostředků v oblasti kybernetické bezpečnosti z programu Digitální Evropa a programu Horizont Evropa a podpoří synergie mezi civilním a obranným rozměrem kybernetické bezpečnosti v souvislosti s Evropským obranným fondem.

Kdo podporuje kterou možnost?

Na základě výsledků konzultací a shromážděných důkazů je zřejmé, že ze strany průmyslových i vědeckých komunit existuje poptávka po mechanismu, který by EU umožnil vytvořit soudržnou průmyslovou politiku kybernetické bezpečnosti, která bude přesahovat činnosti v oblasti výzkumu a vývoje, pokud má Evropa získat vedoucí postavení v oblasti kybernetické bezpečnosti v celosvětovém měřítku. Zároveň zúčastněné strany zdůraznily, že klíčem k úspěchu bude dobře definovaná úloha kompetenčního centra při podpoře a usnadňování úsilí sítě a příslušných komunit a inkluzivní přístup k síti založený na spolupráci, aby nevznikaly nové bariéry. Vzhledem k tomu, že kybernetická bezpečnost je rychle se rozvíjející obor, by struktura také měla být flexibilní, aby se mohla snadno přizpůsobit. Během celého procesu členské státy upozorňovaly na potřebu být inkluzivní vůči všem členským státům a jejich stávajícím centrům excelence a kompetencí a věnovat zvláštní pozornost doplňkovosti opatření. Zvláště s ohledem na kompetenční centrum členské státy zdůraznily význam jeho koordinační role při podpoře této sítě. Proto bude třeba v rámci jakékoli iniciativy Komise nalézt správnou rovnováhu mezi řídícími a prováděcími strukturami a zohlednit ji v těchto strukturách, aby byla zajištěna účinná koordinace na evropské úrovni a zároveň zohledněn vývoj na vnitrostátní úrovni.

C. Dopady upřednostňované možnosti

Jaké jsou výhody upřednostňované možnosti (je-li nějaká doporučena, jinak uveďte výhody

hlavních možností)?

Upřednostňovaná možnost umožní orgánům veřejné moci a průmyslu v členských státech efektivněji zabraňovat 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 (jako je doprava, zdravotnictví, bankovní a finanční služby). Dále by měla pozitivní dopad na konkurenceschopnost EU a malé a střední podniky, jelikož počítá s vytvořením mechanismu, který bude schopen vybudovat průmyslové kapacity členských států a Unie v oblasti kybernetické bezpečnosti a účinným způsobem ze špičkových vědeckých výsledků v Evropě tvořit řešení uplatnitelná na trhu, která by mohla být nasazena napříč celou ekonomikou. Tato možnost umožňuje sdružit prostředky k investicím do nezbytných kapacit na úrovni členských států, vytvořit sdílená evropská aktiva a zároveň dosáhnout úspor z rozsahu. Díky tomu by malé a střední podniky, průmyslová odvětví a výzkumní pracovníci měli získat lepší přístup k takovým zařízením, čímž se podnítí inovace a zkrátí proces vývoje. Dále se tak sníží náklady pro některé podniky na straně poptávky, což jim pomůže učinit z kybernetické bezpečnosti svou konkurenční výhodu. Tato možnost také podporuje využití tržních příležitostí, pokud jde o dvojí užití, protože umožňuje obranné a civilní komunitě spolupracovat na řešení společných problémů. Zároveň by měla znamenat přidanou hodnotu pro vnitrostátní úsilí o řešení nedostatku dovedností v oblasti kybernetické bezpečnosti. Na úrovni EU tato možnost rovněž umožní zvýšit soudržnost a podpořit synergie mezi různými mechanismy financování.

Také by mohla mít nepřímý pozitivní dopad na životní prostředí díky vývoji zvláštních řešení v oblasti kybernetické bezpečnosti pro odvětví, která mají potenciálně obrovský dopad na životní prostředí (např. jaderné elektrárny), čímž pomůže zabránit potenciálně zničujícím následkům kybernetických útoků na tento typ infrastruktury.

Jaké jsou náklady na upřednostňovanou možnost (je-li nějaká doporučena, jinak uveďte náklady na hlavní možnosti)?

Náklady na upřednostňovanou možnost souvisejí především s náklady na fungování kompetenčního centra a národních koordinačních center. Náklady související s prováděním různých programů financování (program Digitální Evropa a program Horizont Evropa) jsou předmětem samostatných posouzení dopadů.

Jaký bude dopad na podniky, včetně malých a středních podniků a mikropodniků?

Evropské společnosti na straně poptávky i nabídky v oblasti kybernetické bezpečnosti, včetně malých a středních podniků a mikropodniků působících v této oblasti, budou patřit mezi nejvýznamněji ovlivněné skupiny zúčastněných stran. Zřízením kompetenčního centra a sítě jim nevznikají regulační povinnosti, naopak získají nové příležitosti, pokud jde o snížení nákladů na navrhování nových produktů a pomoc se získáním snazšího přístupu ke komunitě investorů a přilákáním financování potřebného k nasazení řešení uplatnitelných na trhu. Pro malé a střední podniky a mikropodniky je ještě důležitější přístup k testovacím a experimentálním zařízením, protože nemají prostředky na nákup potřebné infrastruktury nebo na cestování mimo svůj trh (a mnohdy mimo EU), aby ji nalezly. Dále se předpokládá, že iniciativa by mohla evropským malým a středním podnikům a mikropodnikům aktivním v oblasti kybernetické bezpečnosti otevřít nové trhy. Zvolený mechanismus také zajistí koordinaci mezi výzkumem a průmyslem, a nasměruje tak výzkumné úsilí ke konkrétním průmyslovým potřebám. Poskytnutí špičkových odborných znalostí a nástrojů v oblasti kybernetické bezpečnosti nepřímo pomůže hospodářským subjektům dodržovat směrnici o bezpečnosti sítí a informací.

Očekávají se významné dopady na vnitrostátní rozpočty a správní orgány?

Iniciativa umožní členským státům koordinovat investice do nezbytné infrastruktury v oblasti kybernetické bezpečnosti na vnitrostátní a evropské úrovni. Mechanismus umožní sdružit prostředky na nástroje a infrastruktury, které by jinak pro jednotlivé členské státy byly nákladnější nebo finančně nedostupné. Takový přístup povede k úsporám z rozsahu a racionalizaci. Finanční příspěvek členských států na kompetenční centrum a příslušné akce by měl být souměřitelný s příspěvkem Unie.

Očekávají se jiné významné dopady?

Ano, iniciativa má jasně pozitivní dopad, neboť pravděpodobně výrazně zvýší schopnost členských států samostatně zabezpečit své ekonomiky, včetně ochrany kritických odvětví a zvýšení konkurenceschopnosti evropských podniků v oblasti kybernetické bezpečnosti i mnoha dalších odvětví, protože budou schopny vhodně zabezpečit svá současná aktiva a navrhovat inovativní výrobky, avšak zároveň snížit náklady na výzkum a vývoj související s bezpečností. To by nakonec mělo vést k tomu, že EU získá vedoucí postavení v oblasti digitálních technologií a technologií kybernetické bezpečnosti příští generace.

D. Návazná opatření

Kdy bude tato politika přezkoumána?

Právní nástroj bude obsahovat výslovné ustanovení o sledování klíčových ukazatelů výkonnosti i ustanovení o hodnocení a přezkumu, na základě kterých Evropská komise provede průběžné hodnocení s cílem posoudit dopad tohoto nástroje a jeho přidanou hodnotu. Evropská komise bude následně informovat Evropský parlament a Radu. Po uvedeném hodnocení může Komise navrhnout přezkum a prodloužení mandátu kompetenčního centra a sítě.