EURÓPSKA
KOMISIA

V Bruseli 12. 9. 2018
SWD(2018) 404 final

PRACOVNÝ DOKUMENT ÚTVAROV KOMISIE

ZHRNUTIE POSÚDENIA VPLYVU

Sprievodný dokument

NÁVRH NARIADENIA EURÓPSKEHO PARLAMENTU A RADY,

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

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

Súhrnný prehľad

Posúdenie vplyvu návrhu na zriadenie siete kompetenčných centier a Európskeho výskumného a kompetenčného centra v oblasti kybernetickej bezpečnosti

A. Potreba konať

Prečo? Aký problém sa rieši?

EÚ dnes stále nemá dostatočné technologické a odvetvové kapacity na to, aby nezávisle ochránila svoje hospodárstvo a kritické infraštruktúry a stala sa globálnym lídrom na poli kybernetickej bezpečnosti. Cieľom tejto iniciatívy je prispieť k riešeniu nasledujúcich problémov a súvisiacich aspektov, ktoré túto situáciu spôsobujú:

Problém č. 1: nedostatok strategickej a udržateľnej koordinácie a spolupráce medzi odvetviami, kyberneticko-bezpečnostnými výskumnými komunitami a verejnými správami s cieľom chrániť hospodárstvo, spoločnosť a demokraciu špičkovými európskymi kyberneticko-bezpečnostnými riešeniami;

Problém č. 2: poddimenzované investície a obmedzený prístup ku kyberneticko-bezpečnostným znalostiam, zručnostiam a kapacitám v celej Európe;

Problém č. 3: len málo európskych výskumných a inovačných výsledkov v oblasti kybernetickej bezpečnosti sa premení na trhové riešenia a plošne zavádza do hospodárstva.

Za týmito problémami stojí viacero faktorov vrátane nedostatku dôvery medzi jednotlivými hráčmi na trhu kybernetickej bezpečnosti, prirodzených obmedzení existujúcej spolupráce a mechanizmov združovania prostriedkov, chýbajúceho rámca spoločného obstarávania finančne náročnej kyberneticko-bezpečnostnej infraštruktúry, produktov a riešení, ako aj nevyužitého potenciálu tzv. push-pull trhových mechanizmov kombinujúcich dopyt a presadzovanie riešení.

Čo sa od tejto iniciatívy očakáva?

Cieľom iniciatívy je zabezpečiť, aby si EÚ zachovala a rozvíjala základné (technologické a odvetvové) kapacity na autonómne zabezpečenie svojho digitálneho hospodárstva, spoločnosti a demokracie, a aby členské štáty mohli využívať tie najmodernejšie kyberneticko-bezpečnostné riešenia a obranné spôsobilosti. Zároveň je jej cieľom posilniť globálnu konkurencieschopnosť kyberneticko-bezpečnostných firiem z EÚ a zabezpečiť, aby všetky odvetvia EÚ mali prístup ku kapacitám a zdrojom potrebným na to, aby pre ne bola kybernetická bezpečnosť konkurenčnou výhodou. Dosiahnuť by sa to malo zriadením účinných mechanizmov dlhodobej strategickej spolupráce všetkých relevantných aktérov (verejných orgánov, jednotlivých odvetví a výskumnej obce tak v civilnej, ako aj obrannej sfére), zlučovaním znalostí a zdrojov s cieľom poskytnúť špičkové spôsobilosti a infraštruktúry, stimuláciou plošného zavádzania európskych kyberneticko-bezpečnostných produktov a riešení v celom hospodárstve a vo verejnom sektore, podporou kyberneticko-bezpečnostných startupov a MSP, ako aj snahou o odstránenie medzier v kyberneticko-bezpečnostných zručnostiach.

Aká je pridaná hodnota opatrení na úrovni EÚ?

Iniciatíva by bola pridanou hodnotou k súčasnému úsiliu na vnútroštátnej úrovni, keďže by pomohla vytvoriť prepojený celoeurópsky odvetvový a výskumný ekosystém v oblasti kybernetickej bezpečnosti. Mala by podporiť lepšiu spoluprácu medzi relevantnými zainteresovanými stranami (vrátane civilného a obranného sektora kybernetickej bezpečnosti) s cieľom čo najlepšie využiť existujúce kyberneticko-bezpečnostné zdroje a znalosti z celej Európy. Zároveň by mala EÚ a členským štátom pomôcť zaujať proaktívny, dlhodobý a strategický postoj k odvetvovej politike kybernetickej bezpečnosti, ktorá presahuje rámec výskumu a vývoja. Tento prístup by mal pomôcť nielen pri objavovaní prelomových riešení kyberneticko-bezpečnostných výziev, s ktorými sa verejný a súkromný sektor stretáva, ale aj pri podpore ich zavádzania do praxe. Zároveň relevantným výskumným a odvetvovým komunitám a verejným orgánom sprístupní kľúčové kapacity, ako sú skúšobné a experimentačné zariadenia, ku ktorým sa samostatné členské štáty často nedostanú pre nedostatok finančných či ľudských zdrojov. Okrem toho prispeje k preklenutiu nedostatku zručností a zamedzeniu „úniku mozgov", keďže zabezpečí prístup tých najtalentovanejších odborníkov k rozsiahlym európskym projektom, čím im ponúkne zaujímavé profesionálne výzvy. Všetko z uvedeného sa zároveň považuje za potrebné na to, aby Európa dosiahla globálne uznanie za lídra na poli kybernetickej bezpečnosti.

B. Riešenia

Aké legislatívne a nelegislatívne možnosti politiky sa zvažovali? Je niektorá z možností uprednostňovaná? Prečo?

Bolo zvážených niekoľko politických možností, legislatívnych i nelegislatívnych. Na hlbšie preskúmanie sa zvolili tieto:

1. **východiskový scenár** – možnosť spolupráce: predpokladá sa pokračovanie v súčasnom prístupe k budovaniu kyberneticko-bezpečnostných odvetvových a technologických kapacít v EÚ podporou výskumu a inovácie, ako aj súvisiacich mechanizmov spolupráce v rámci programu Európsky horizont;
2. **možnosť 1:** kompetenčná sieť kybernetickej bezpečnosti a Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti s právomocami na vykonávanie opatrení na podporu odvetvových technológií, výskumu a inovácie;
3. **možnosť 2:** kompetenčná sieť kybernetickej bezpečnosti a Európske výskumné a kompetenčné centrum v oblasti kybernetickej bezpečnosti, ktoré by bolo obmedzené iba na výskumné a inovačné činnosti;

V prvej fáze boli celkom vylúčené tieto možnosti: 1) vôbec žiadne kroky; 2) iba sieť existujúcich kompetenčných centier a 3) použitie existujúcej agentúry (ENISA, REA alebo INEA).

Vzhľadom na všeobecný záväzok, ktorý Komisia v tejto oblasti už prijala, ako aj na význam roly členských štátov spočíva hlavný rozdiel medzi dvomi možnosťami politiky, ktoré sa analyzovali podrobnejšie, v ich rozsahu vzhľadom na právny základ: subjekt založený výlučne na článku 187 ZFEÚ (možnosť 2) by iniciatívu obmedzil iba na oblasť výskumu a inovácie, pričom by sa štandardne predpokladal finančný príspevok súkromných aktérov. Na druhej strane subjekt s dvojakým právnym základom – čl. 187 ZFEÚ a čl. 173 ZFEÚ (možnosť 1) by mal širší mandát, ktorý by okrem iného pokrýval aj zavádzanie, odvetvovú podporu a vytváranie silnejších synergií s kybernetickou obranou. Okrem toho by posilnil rolu členských štátov – tak z hľadiska riadenia, ako aj ich pozície potenciálnych obstarávateľov kyberneticko-bezpečnostných technológií.

Analýza ukázala, že na dosiahnutie cieľov iniciatívy pri maximalizácii hospodárskeho, spoločenského a environmentálneho účinku a ochrane záujmov Únie je najvhodnejšia možnosť 1. Medzi hlavné argumenty v jej prospech patrí flexibilita, ktorá umožňuje rôzne modely spolupráce s komunitou a sieťou kompetenčných centier, aby sa optimálne využili dostupné znalosti a zdroje; možnosť štruktúrovať spoluprácu verejných a súkromných aktérov zo všetkých relevantných sektorov vrátane obrany; možnosť vytvoriť skutočnú kyberneticko-bezpečnostnú odvetvovú politiku podporou činností, ktoré nesúvisia len s výskumom a vývojom, ale aj so zavádzaním riešení na trh. V neposlednom rade prinesie možnosť 1 aj zvýšenie koherentnosti, keďže je to implementačný mechanizmus kyberneticko-bezpečnostného financovania z programov Digitálna Európa a Európsky horizont, a posilní synergie medzi civilnou a obrannou zložkou kybernetickej bezpečnosti v kontexte Európskeho obranného fondu.

Kto podporuje ktorú možnosť?

Z výsledkov konzultácie a zhromažďovania informácií vyplýva, že ak sa má Európa stať globálnym lídrom na poli kybernetickej bezpečnosti, odvetvie i výskumná komunita volajú po mechanizme, ktorý by EÚ poskytol koherentnú odvetvovú politiku kybernetickej bezpečnosti nad rámec čisto výskumných a vývojových činností. Zároveň zainteresované strany zdôraznili, že kľúčom k úspechu bude správne vymedzenie roly centra pri podpore a uľahčovaní činnosti siete a príslušných komunít, ako aj inkluzívny a kolaboratívny prístup k sieti, aby sa znalosti neizolovali. Keďže sféra kybernetickej bezpečnosti sa rýchlo vyvíja, štruktúra by zároveň mala byť pružná a prispôsobivá. Členské štáty v celom procese zdôrazňovali potrebu začlenenia všetkých členských štátov a ich existujúcich centier excelentnosti a kompetencií s osobitným zameraním na doplnkovosť opatrení. Osobitne vo vzťahu k centru členské štáty zdôraznili význam jeho koordinačnej úlohy pri podpore siete. Iniciatíva Komisie preto musí nájsť a zohľadňovať rovnováhu v štruktúrach riadenia a implementácie, aby sa zaistila účinná celoeurópska koordinácia a zároveň sa zohľadnil vývoj na úrovni členských štátov.

C. Vplyvy uprednostňovanej možnosti

Aké sú výhody uprednostňovanej možnosti (prípadne hlavných možností, ak sa žiadna konkrétna možnosť neuprednostňuje)?

Uprednostňovaná možnosť umožní verejným orgánom a jednotlivým odvetviam v členských štátoch účinnejšiu prevenciu kybernetických hrozieb a reakciu na ne, keďže sa ponúknu a zavedú bezpečnejšie produkty a riešenia.

Osobitný význam to má z hľadiska zabezpečenia prístupu k základným službám (ako doprava, zdravotníctvo, bankovníctvo a finančné služby). Pozitívny bude aj vplyv na konkurencieschopnosť EÚ a MSP, keďže sa predpokladá vytvorenie mechanizmu, ktorý dokáže vybudovať kyberneticko-bezpečnostné odvetvové kapacity členských štátov aj Únie a účinne premietnuť európsku vedeckú excelentnosť do trhových riešení, ktoré možno zaviesť v celom hospodárstve. Vďaka tejto možnosti sa dajú zlučovať zdroje na investovanie do potrebných kapacít na úrovni členských štátov, rozvíjať spoločné európske aktíva a využiť úspory z rozsahu. Je pravdepodobné, že sa vďaka tomu zlepší prístup MSP, jednotlivých odvetví i výskumných pracovníkov k takýmto zariadeniam, čo podnieti inováciu a urýchli vývoj. Zároveň sa znížia náklady pre určité odberateľské odvetvia, ktoré budú môcť kybernetickú bezpečnosť využiť ako konkurenčnú výhodu. Vďaka tejto možnosti sa dajú využiť príležitosti na trhu dvojakého použitia, keďže obranný a civilný sektor budú môcť spolupracovať na spoločných problémoch. Zároveň bude pravdepodobne pridanou hodnotou pre snahy členských štátov o riešenie nedostatku kyberneticko-bezpečnostných zručností. Na úrovni EÚ táto možnosť umožňuje posilniť koherentnosť a synergie medzi rôznymi mechanizmami financovania.

Nepriamy pozitívny vplyv na životné prostredie by sa dal dosiahnuť vytvorením osobitných kyberneticko-bezpečnostných riešení pre sektory s potenciálne veľmi výrazným environmentálnym vplyvom (napr. jadrové elektrárne), aby dokázali zabrániť devastačným dôsledkom prípadných kybernetických útokov na tento typ infraštruktúry.

Aké sú náklady na uprednostňovanú možnosť (prípadne na hlavné možnosti, ak sa žiadna konkrétna možnosť neuprednostňuje)?

Náklady na uprednostňovanú možnosť sa viažu predovšetkým na prevádzku centra a národných koordinačných centier. Nákladom spojeným s implementáciou jednotlivých programov financovania (Digitálna Európa a Európsky horizont) sa venuje samostatné posúdenie vplyvu.

Aký bude vplyv na podniky, MSP a mikropodniky?

Medzi najväčšmi ovplyvnené skupiny aktérov patria európske spoločnosti, ktoré na poli kybernetickej bezpečnosti pôsobia tak na strane dopytu, ako aj ponuky vrátane MSP a mikropodnikov. Zriadenie kompetenčného centra a siete im neukladá žiadne regulačné povinnosti, ale ponúkne im nové príležitosti z pohľadu zníženia nákladov na vývoj nových produktov, uľahčí im prístup k investorským kruhom a pritiahne potrebné financovanie na zavedenie trhových riešení. V prípade MSP a mikropodnikov je prístup k verejne financovaným skúšobným a experimentačným zariadeniam o to významnejší, že nemajú prostriedky na nákup vlastnej infraštruktúry ani na využívanie infraštruktúry mimo svojho trhu (a často mimo EÚ). Ďalšou nádejou je, že táto iniciatíva otvorí európskym MSP a mikropodnikom pôsobiacim na poli kybernetickej bezpečnosti nové trhy. Okrem toho zvolený mechanizmus zabezpečí koordináciu výskumu s daným sektorom, takže výskumné úsilie bude smerované k napĺňaniu konkrétnych potrieb odvetvia. Poskytovanie špičkovej kyberneticko-bezpečnostnej expertízy a nástrojov nepriamo podporí súlad hospodárskych subjektov so smernicou NIS.

Očakáva sa významný vplyv na štátne rozpočty a verejnú správu?

Iniciatíva členským štátom umožní koordinovať investície do potrebnej kyberneticko-bezpečnostnej infraštruktúry na národnej i európskej úrovni. Tento mechanizmus umožní združenie zdrojov na zabezpečenie nástrojov a infraštruktúr, ktoré by inak boli pre jednotlivé členské štáty drahšie alebo cenovo celkom nedostupné. Takýto prístup by umožnil úspory z rozsahu a optimalizáciu. Finančný príspevok členských štátov na kompetenčné centrum a relevantné akcie by mal zodpovedať príspevku Únie.

Očakávajú sa iné významné vplyvy?

Áno, iniciatíva má jasný pozitívny vplyv, keďže sa predpokladá výrazné posilnenie schopnosti členských štátov samostatne zabezpečiť ich hospodárstva vrátane ochrany kľúčových odvetví, posilnenie konkurencieschopnosti európskych podnikov pôsobiacich v sektore kybernetickej bezpečnosti, ako aj ďalších odvetví, ktoré budú schopné primerane zabezpečiť svoje aktíva a vyvíjať zabezpečené inovačné produkty pri súčasnom znižovaní nákladov na bezpečnostný výskum a vývoj. V konečnom dôsledku by to malo EÚ pomôcť stať sa lídrom v oblasti digitálnych a kyberneticko-bezpečnostných technológií ďalšej generácie.

D. Nadväzné opatrenia

Kedy sa táto politika preskúma?

Právny nástroj bude explicitne zahŕňať ustanovenie o monitorovaní kľúčových ukazovateľov výkonnosti (KPI), ako

aj doložku o hodnotení a preskúmaní, podľa ktorej Európska komisia vykoná priebežné hodnotenie účinku nástroja a jeho pridanej hodnoty. Európska komisia následne podá správu Európskemu parlamentu a Rade. Na základe tohto hodnotenia môže Komisia navrhnúť preskúmanie a predĺženie mandátu kompetenčného centra a siete.