Az Európai Unió
Tanácsa

Brüsszel, 2018. szeptember 13.
(OR. en)

12104/18
ADD 5

Intézményközi referenciaszám:
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

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Jordi AYET PUIGARNAU igazgató
Az átvétel dátuma:	2018. szeptember 12.
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	SWD(2018) 404 final
Tárgy:	BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM A HATÁSVIZSGÁLAT VEZETŐI ÖSSZEFOGLALÓJA amely a következő dokumentumot kíséri Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról

Mellékelten továbbítjuk a delegációknak az SWD(2018) 404 final számú dokumentumot.

Melléklet: SWD(2018) 404 final

EURÓPAI
BIZOTTSÁG

Brüsszel, 2018.9.12.
SWD(2018) 404 final

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLAT VEZETŐI ÖSSZEFOGLALÓJA

amely a következő dokumentumot kíséri

Javaslat
AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról

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

Vezetői összefoglaló

Hatásvizsgálat a kompetenciaközpontok hálózata és az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont létrehozására irányuló javaslatról

A. A fellépés szükségessége

Miért? Milyen problémát kell megoldani?

Az EU jelenleg még mindig nem rendelkezik elegendő technológiai és ipari kapacitással ahhoz, hogy önállóan gondoskodjon gazdaságának és kritikus infrastruktúráinak biztonságáról, és világvezetővé váljon a kiberbiztonság területén. E kezdeményezés célja az alábbi problémák megoldásához és a fenti helyzetben közrejátszó tényezők alakításához való hozzájárulás:

1. probléma: Elégtelen szintű stratégiai és fenntartható koordináció, valamint együttműködés az iparágak, a kiberbiztonsági kutatói közösségek és a kormányzatok között a gazdaság, a társadalom és a demokrácia élvonalbeli európai kiberbiztonsági megoldásokkal történő védelméhez;

2. probléma: Európa-szerte kevés a beruházás, és korlátozott a kiberbiztonsági know-how, készségek és létesítmények elérhetősége;

3. probléma: Kevés európai kiberbiztonsági kutatási és innovációs eredményből születnek piacképes megoldások, amelyeket aztán széles körben bevezetnének a gazdaságban.

E problémák mögött több tényező húzódik meg: a kiberbiztonsági piac különböző szereplői közötti kellő mértékű bizalom hiánya, a meglévő együttműködési és forrásösszevonási mechanizmusok eredendő korlátai, a költséges kiberbiztonsági infrastruktúra és kiberbiztonsági termékek/megoldások közös beszerzésére szolgáló keret hiánya, valamint a kényszerítő és vonzó piaci mechanizmusokban rejlő lehetőségek kihasználatlansága.

Mi a kezdeményezés várható eredménye?

A kezdeményezés célja annak biztosítása, hogy az EU megőrizze és fejlessze az ahhoz szükséges alapvető (technológiai és ipari) kapacitásokat, hogy önállóan tudjon gondoskodni digitális gazdaságának, társadalmának és demokráciájának a biztonságáról, a tagállamok pedig élhessenek a legfejlettebb kiberbiztonsági megoldások és kibervédelmi képességek nyújtotta előnyökkel. A kezdeményezés célja egyszersmind az is, hogy növelje az uniós kiberbiztonsági vállalatok globális versenyképességét, és biztosítsa, hogy a különböző ágazatokban működő európai iparvállalatok hozzáférjenek az ahhoz szükséges kapacitásokhoz és erőforrásokhoz, hogy a kiberbiztonságot versenyelőnyükké tudják alakítani. Ezt az összes érintett szereplő (a hatóságok, az ipar, a civil és a honvédelmi területen működő kutatói közösség) közötti hosszú távú, stratégiai együttműködés eredményes mechanizmusainak kidolgozásával, élvonalbeli képességek és infrastruktúrák biztosítása érdekében a tudás és az erőforrások összevonásával, az európai kiberbiztonsági termékek és megoldások egész gazdaságban és a közszektorban való széles körű elterjesztésének ösztönzésével, az induló kiberbiztonsági vállalkozások és kkv-k támogatásával, valamint a kiberbiztonsági készséghiány felszámolásának segítésével kell megvalósítani.

Milyen többletértéket képvisel az uniós szintű fellépés?

A kezdeményezés hozzáadott értéket jelent a nemzeti szinten jelenleg folyó erőfeszítésekhez azáltal, hogy elősegíti egy egész Európára kiterjedő, hálózatban működő kiberbiztonsági ipari és kutatási ökoszisztéma megteremtését. Várhatóan ösztönzőleg hat majd az érintett érdekelt felek (ezen belül a polgári és a katonai kiberbiztonsági ágazat) közötti együttműködésre, ezáltal optimálisan ki lehet használni az Európa-szerte elérhető kiberbiztonsági erőforrásokat és szaktudást. Segít az EU-nak és a tagállamoknak abban, hogy olyan proaktív és hosszabb távú stratégiai szemléletet kövessenek a kiberbiztonsági ágazati politika tekintetében, amely túlmutat a kutatáson és a fejlesztésen. Ez a megközelítés nemcsak hogy elősegíti a magán- és az állami szektor előtt álló kiberbiztonsági kihívások áttörő megoldásainak kifejlesztését, de támogatja ezen megoldások eredményes gyakorlati alkalmazását is. Lehetővé teszi továbbá az érintett kutatási és ipari közösségek, valamint a hatóságok számára, hogy hozzáférjenek olyan kulcsfontosságú kapacitásokhoz – például tesztelési és kísérleti létesítményekhez –, amelyek a pénzügyi és emberi erőforrások elégtelensége miatt gyakran nem elérhetők az egyes tagállamok számára. A kezdeményezés továbbá azáltal, hogy a legkiválóbb tehetségek számára hozzáférést biztosít a nagy léptékű európai projektekhez, és ezáltal érdekes szakmai kihívásokat teremt, hozzájárul a készséghiány megszüntetéséhez és az elitelvándorlás elkerüléséhez. A fentiek mindegyike szükségesnek tűnik

ahhoz is, hogy Európa a kiberbiztonság területén vezető térségként globálisan elismertté váljon.

B. Megoldások

Milyen jogalkotási és nem jogalkotási szakpolitikai alternatívák merültek fel? Van-e előnyben részesített megoldás? Miért?

Számos jogalkotási és nem jogalkotási szakpolitikai alternatíva mérlegelése történt meg. A következő alternatívák maradtak fenn mélyreható értékelésre:

1. **Alapforgatókönyv**: az együttműködésen alapuló alternatíva, amely azon a feltevésen alapul, hogy folytatódik a jelenlegi megközelítés alkalmazása az uniós kiberbiztonsági ipari és technológiai kapacitások építése terén, azaz a kutatás és az innováció, valamint a kapcsolódó együttműködési mechanizmusok a Horizont Európa program keretében kapnak támogatást;
2. **1. alternatíva:** Kiberbiztonsági kompetenciahálózat, egy Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont szervezettel, amely felhatalmazást kap ipari technológiákat és a kutatás és innováció területére tartozó tevékenységeket támogató intézkedések végrehajtására;
3. **2. alternatíva:** Kiberbiztonsági kompetenciahálózat egy Európai Kiberbiztonsági Kutatási és Kompetenciaközponttal, amely kizárólag kutatási és innovációs tevékenységekre szorítkozik;

A korai szakaszban elvetett alternatívák között a következők szerepeltek: 1. a fellépés teljes mellőzése; 2. hálózat kizárólag a meglévő kompetenciaközpontokból; és 3. egy meglévő ügynökség (ENISA, REA vagy INEA) igénybevétele.

Figyelemmel a Bizottság által e kezdeményezés iránt eddig is felvállalt általános elkötelezettségre, valamint tekintettel a tagállamok által betöltendő fontos szerepre, a két részletesen elemzett szakpolitikai alternatíva közötti fő különbség azok hatályában rejlik, amelyet a jogalapjuk is tükröz: a csak az EUMSZ 187. cikkén alapuló jogalany (2. alternatíva) a kutatás és az innováció területére korlátozná a kezdeményezést, és jellemzően magánszereplőktől származó pénzügyi hozzájárulást feltételezne. Másrészt egy kettős jogalapon – az EUMSZ 187. és 173. cikkén nyugvó szervezet (1. alternatíva) tágabb körű megbízatást jelentene, amely többek között a bevezetést és az ipari támogatást is felölelné, és a kibervédelemmel erősebb szinergiákat teremtene. Egyszersmind hangsúlyosabb szerephez juttatná a tagállamokat, az irányításban betöltött szerepüket illetően és a kiberbiztonsági technológia potenciális beszerzőiként egyaránt.

Az elemzés tanúsága szerint az 1. alternatíva a legalkalmasabb a kezdeményezés céljainak eléréséhez, és ugyanekkor ez az alternatíva biztosítja a legjelentősebb gazdasági, társadalmi és környezeti hatást, és védi az Unió érdekeit is. Az ezen alternatíva mellett felsorakoztatott legfontosabb érvek többek között: a rugalmasság, amely a közösséggel és a kompetenciaközpontok hálózatával való együttműködés különböző modelljeit teszi lehetővé a meglévő ismeretek és erőforrások felhasználásának optimalizálása érdekében; a köz- és a magánszféra valamennyi érintett ágazatában – többek között a védelmi szektorban – működő érdekelt felek közötti együttműködés strukturálásának lehetősége; egy valódi kiberbiztonsági ipari politika létrehozásának lehetősége azáltal, hogy nemcsak a kutatáshoz és fejlesztéshez, hanem a piaci bevezetéshez kapcsolódó tevékenységek is támogatásban részesülnek. Végül, de nem utolsósorban az 1. alternatíva lehetővé teszi a koherencia növelését is azáltal, hogy a Digitális Európa programból és a Horizont Európa programból származó, kiberbiztonsággal kapcsolatos finanszírozás végrehajtási mechanizmusaként működik, és az Európai Védelmi Alap vonatkozásában erősíti a kiberbiztonság civil és védelmi vetületei közötti szinergiákat.

Ki melyik alternatívát támogatja?

A konzultációs és bizonyítékgyűjtési folyamatok eredménye szerint az ipari és a kutatói közösség részéről egyaránt egyértelmű igény mutatkozik egy olyan mechanizmus iránt, amely lehetővé teszi az EU számára, hogy a kutatási és fejlesztési tevékenységeken túlmutató, koherens kiberbiztonsági ipari politikával rendelkezzen, és Európa ezzel világvezetővé válhasson a kiberbiztonság területén. Az érdekelt felek ugyanakkor hangsúlyozták, hogy a siker kulcsa az lesz, hogy a központ hálózat és az érintett közösségek erőfeszítéseinek támogatásában és megkönnyítésében játszott szerepe megfelelő meghatározást nyerjen, valamint hogy inkluzív, együttműködésen alapuló megközelítést alkalmazzanak a hálózat tekintetében, újabb vertikális hierarchiájú rendszerek létrehozását megelőzendő. A struktúrának emellett rugalmasnak kell lennie, hogy könnyen adaptálható legyen, tekintve, hogy a kiberbiztonság gyors ütemben változó környezet. A tagállamok az egész folyamat során hangsúlyozták, hogy az összes tagállam, valamint meglévő kiválósági és kompetenciaközpontjaik irányába nyitottnak kell lenni, és külön

figyelmet kell fordítani az intézkedések egymást kiegészítő jellegére. A tagállamok kifejezetten a központtal kapcsolatban annak a hálózat támogatásában betöltött koordinációs szerepét hangsúlyozták. Ezért minden bizottsági kezdeményezésnek meg kell találnia a megfelelő egyensúlyt az irányítási és végrehajtási struktúrákban, és figyelembe kell vennie az irányítási és végrehajtási struktúrák ezen egyensúlyát, biztosítva ezzel az eredményes európai koordinációt, a nemzeti szintű fejlemények figyelembevétele mellett.

C. Az előnyben részesített alternatíva hatásai

Melyek az előnyben részesített alternatíva (ha nincs ilyen, akkor a főbb lehetőségek) előnyei?

Az előnyben részesített alternatíva valamennyi tagállamban lehetővé fogja tenni a hatóságok és az iparvállalatok számára, hogy eredményesebben megelőzzék a kiberfenyegetéseket, illetve reagáljanak azokra, mégpedig azáltal, hogy biztonságosabb termékeket és megoldásokat kínálnak, illetve biztonságosabb termékekkel és megoldásokkal vértezik fel magukat. Ez különösen fontos az alapvető szolgáltatásokhoz (pl. közlekedés, egészségügy, banki és pénzügyi szolgáltatások) való hozzáférés védelme terén. Kedvező hatást gyakorolna az EU versenyképességére és a kkv-kra is, mivel egy olyan mechanizmus létrehozását feltételezi, amely képes fejleszteni a tagállamok és az Unió kiberbiztonsági kapacitásait, valamint az európai tudományos kiválóságot ténylegesen olyan piacképes megoldásokra váltani, amelyek az egész gazdaságban bevezethetők. Ez az alternatíva lehetővé teszi az erőforrások összevonását, hogy a tagállamok szintjén megvalósulhassanak a szükséges kapacitásokba történő beruházások, és közös európai eszközöket lehessen kifejleszteni, méretgazdaságosság elérése mellett. Ez várhatóan növeli majd az ilyen létesítmények hozzáférhetőségét a kkv-k, az iparvállalatok és a kutatók számára, ami pedig ösztönözni fogja az innovációt és le fogja rövidíteni a fejlesztési folyamatokat. Ez egyúttal csökkenteni fogja egyes keresleti oldali vállalkozások költségeit, és segíteni fogja azokat a kiberbiztonság versenyelőnyükké alakításában. Az alternatíva révén kihasználhatóvá válnak a kettős felhasználásban rejlő piaci lehetőségek azáltal, hogy lehetővé teszi a védelmi és a civil közösségek számára a közös problémákon történő együttes munkát. Valószínűleg értéktöbbletet hoz a kiberbiztonsági készséghiány kezelésével kapcsolatos nemzeti erőfeszítések szempontjából is. Ez az alternatíva egyszersmind uniós szinten lehetővé teszi a különböző finanszírozási mechanizmusok közötti koherencia és szinergiák javítását.

Közvetett kedvező környezeti hatás érhető el a potenciálisan jelentős környezeti hatást kifejtő ágazatoknak (pl. atomerőművek) szóló, speciális kiberbiztonsági megoldások kidolgozásával, amelyek segítik ezen ágazatokat abban, hogy elkerüljék az ilyen típusú infrastruktúrák elleni kiberbiztonsági támadások potenciális pusztító következményeit.

Milyen költségekkel jár az előnyben részesített alternatíva (ha nincs ilyen, akkor milyen költségekkel járnak a főbb lehetőségek)?

Az előnyben részesített alternatíva költségei főként a központ és a nemzeti koordinációs központok működési költségeivel függenek össze. A különböző finanszírozási programok (Digitális Európa program és Horizont Európa program) végrehajtásával összefüggő költségek külön hatásvizsgálatok tárgyát képezik.

Hogyan érinti a fellépés a vállalkozásokat, köztük a kis- és középvállalkozásokat és a mikrovállalkozásokat?

A javaslat által leginkább érintett érdekelti csoportok közé többek között azok az európai vállalatok tartoznak majd, amelyek kiberbiztonsági területen – akár keresleti, akár kínálati oldalon – működnek, a kkv-kat és mikrovállalkozásokat is beleértve. A kompetenciaközpont és a hálózat létrehozása nem jár számukra szabályozási kötelezettségekkel, ugyanakkor lehetőséget teremt majd az új termékek tervezésével összefüggő költségek csökkentésére, és segíteni fogja a vállalatokat abban, hogy könnyebben hozzáférjenek a befektetői közösséghez, és megszerezzék a szükséges finanszírozást a piacképes megoldások bevezetéséhez. A kkv-k és a mikrovállalkozások esetében még fontosabb a közfinanszírozású vizsgálati és kísérleti létesítményekhez való hozzáférés, mivel nem rendelkeznek az ahhoz szükséges forrásokkal, hogy megvásárolják a szükséges infrastruktúrát, vagy annak elérése érdekében saját piacukon (és gyakran az EU-n) kívülre utazzanak. Reményeink szerint e kezdeményezés új piacokat is megnyitna a kiberbiztonság területén működő európai kkv-k és mikrovállalkozások számára. Ezen túlmenően a választott mechanizmus biztosítani fogja a kutatás és az ipar közötti koordinációt, és a kutatási erőfeszítéseket ily módon a konkrét ipari szükségletek felé fogja terelni. A kiberbiztonság területén az élvonalbeli szaktudás és eszközök biztosítása közvetetten támogatni fogja a gazdasági szereplőket a hálózat- és információbiztonsági irányelvnek való megfelelésben.

Lesz-e jelentős hatása az intézkedésnek a tagállamok költségvetésére és közigazgatására?

A kezdeményezés lehetővé fogja tenni a tagállamok számára, hogy nemzeti és európai szinten koordinálják a szükséges kiberbiztonsági infrastrukturára irányuló beruházásokat. A mechanizmus lehetővé fogja tenni a források olyan eszközök és infrastruktúrák érdekében való összevonását, amelyek másként az egyes tagállamok számára költségesebbek vagy megfizethetetlenek lennének. E megközelítés méretgazdaságosságot és észszerűsítést tenne lehetővé. A tagállamok által a kompetenciaközpont számára, valamint az érintett intézkedésekhez nyújtott pénzügyi hozzájárulásnak arányban kell állnia az uniós hozzájárulással.

Lesznek-e egyéb jelentős hatások?

Igen, a kezdeményezésnek egyértelmű pozitív hatása lesz, mivel várhatóan jelentősen növeli majd a tagállamok ahhoz szükséges kapacitásait, hogy önállóan gondoskodhassanak gazdaságaik biztonságáról, ideértve a kritikus ágazatok védelmét, valamint az európai kiberbiztonsági vállalkozások és a különböző más ágazatokba tartozó vállalatok versenyképességének növelését, amelyek képesek lesznek arra, amelyek képesek lesznek megfelelően gondoskodni meglévő eszközeik biztonságáról és biztonságos innovatív termékeket tervezni, miközben a biztonsággal kapcsolatos K+F-költségeik csökkennek. Ennek pedig végső soron lehetővé kell tennie az EU számára, hogy az élre kerüljön a következő generációs digitális és kiberbiztonsági technológiák területén.

D. További lépések

Mikor kerül sor a szakpolitikai fellépés felülvizsgálatára?

A jogi eszköznek része lesz egy kifejezetten a fő teljesítménymutatók nyomon követésére vonatkozó rendelkezés, valamint egy értékelésre és felülvizsgálatra vonatkozó rendelkezés, amely szerint az Európai Bizottság az eszköz hatásának és hozzáadott értékének mérésére időközi értékelést fog végezni. Az Európai Bizottság ezt követően beszámol az Európai Parlamentnek és a Tanácsnak. Az értékelést követően a Bizottság javasolhatja a kompetenciaközpont és a hálózat megbízatásának felülvizsgálatát és bővítését.