EURÓPAI BIZOTTSÁG

Brüsszel, 2010.9.30.
SEC(2010) 1127

BIZOTTSÁGI SZOLGÁLATI MUNKADOKUMENTUM

A HATÁSVIZSGÁLAT ÖSSZEFOGLALÁSA

amely a következő dokumentumot kíséri:

Javaslat:

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA)

{COM(2010) 521 végleges}
{SEC(2010) 1126}

A HATÁSVIZSGÁLAT ÖSSZEFOGLALÁSA

1. TÁRGY ÉS HÁTTÉR

1.1. Tárgy

A hatásvizsgálat arra összpontosít, hogy hogyan alakítható ki a legelőnyösebb módon egy olyan, korszerűsített, a hálózat- és információbiztonság területén jelentkező kihívások kezelésének széles körben elismerten megfelelő és szükséges szakpolitikai eszközeként funkcionáló hálózat- és információbiztonsági ügynökség, amely – attól az időponttól fogva, amikor a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) megbízatása 2012 márciusában véget ér – támogatást nyújt a tagállami szerveknek és a Bizottságnak a hálózat- és információbiztonság területén kitűzött szakpolitikai célok teljesítésében.

1.2. Háttér

Mai világunkban a társadalom és a gazdaság rendkívüli mértékben támaszkodik az információs és kommunikációs technológia (IKT) zavartalan működésére. Ezért létfontosságú biztosítani egyfelől a rendszerek stabilitását, másfelől a felhasználók beléjük vetett bizalmát. A rendszerek működését fenyegető egyre több veszélyforrás, támadás és rosszindulatú szoftver kockázatot jelenthet az alapvető hálózatos és informatikai infrastruktúra zavartalan működése szempontjából. Mivel ezek a rendszerek transznacionális jellegűek, a hálózat- és információbiztonság területén jelentkező kihívások európai szinten igényelnek választ.

E kérdések kezelésére a 460/2004/EK rendelettel[1] 2004-ben ötéves kezdeti időtartamra létrejött az Európai Hálózat- és Információbiztonsági Ügynökség (a továbbiakban: ENISA), melynek elsődleges céljául a jogalkotó a következőket tűzte ki: „*a Közösségen belüli magas szintű és hatékony hálózat- és információbiztonság biztosítása, valamint az Európai Unió polgárai, fogyasztói, vállalkozásai és a közszektor szervezetei érdekében a hálózat- és információbiztonság kultúrájának kifejlesztése [...], ezáltal elősegítve a belső piac zavartalan működését.*”

Azóta a hálózat- és az információbiztonsággal kapcsolatos kihívások a technológia fejlődését és a piaci körülmények alakulását követve komoly változásokon mentek át. Ezért a Bizottság már jóval az ENISA-rendelet hatályának 2009. márciusi lejárta előtt a legfontosabb érdekeltek bevonásával kezdeményezte annak meghatározását, hogy mely szakpolitikai eszközökkel biztosítható legelőnyösebben 2009-től a hálózat- és információbiztonság területén az Európai Unió által kitűzött célok teljesülése. Az ENISA működésének 2007. évi időközi értékelését[2] és egy nyilvános konzultációt[3] követően a Tanács és az Európai Parlament 2008. szeptember 24-én rendeletet[4] fogadott el az ENISA akkori megbízatásának három évvel, vagyis 2012.

---

1 Az Európai Parlament és a Tanács 460/2004/EK rendelete (2004. március 10.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról.

2 A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) értékeléséről, COM(2007) 285, 2007. június 1., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:HU:NOT

3 A nyilvános konzultáció 2007. június 13-tól 2007. szeptember 7-ig tartott.

4 Az Európai Parlament és a Tanács 1007/2008/EK rendelete (2008. szeptember 24.) az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az Ügynökség megbízatási ideje tekintetében történő módosításáról, HL L 293., 2008.10.31.

március 13-ig történő meghosszabbításáról. A rendelet preambulumában a Tanács és az Európai Parlament sürgette „***az Ügynökségre vonatkozó további megbeszéléseket***”, illetőleg „***a hálózat- és az információbiztonság fokozása irányában tett európai erőfeszítések általános irányának további átgondolását***”.

A Bizottság azzal segítette ezeket az egyeztetéseket, hogy 2008 novemberében nyilvános konzultációt indított útjára a hálózat- és az információbiztonságra vonatkozó megerősített uniós szakpolitikai törekvések lehetséges célkitűzéseinek meghatározásáról, valamint a megvalósításukhoz szükséges eszközrendszerről.[5] A Bizottság 2008 decemberében műhelytalálkozót is tartott a tagállamok illetékes hatóságainál dolgozó hálózat- és információbiztonsági szakértők részvételével, mely áttekintette a hálózat- és információbiztonságra vonatkozó megerősített uniós szakpolitika lehetséges eszközeit és mechanizmusait. A Bizottság 2009 márciusában közleményt fogadott el a kritikus informatikai infrastruktúrák védelméről,[6] melyben kulcsfontosságú szereplőként jelölte meg az ENISA-t a biztonság, az ellenálló képesség és a felkészültség megerősítésére irányuló európai uniós erőfeszítések támogatásában. A Bizottság által alkalmazott megközelítésmódot támogatásáról biztosította a Tallinnban 2009. április 27–28-án a kritikus informatikai infrastruktúrák védelme tárgyában tartott miniszteri konferencia, melynek következtetései között a következő olvasható: „***az előttünk álló újfajta, hosszabb időre szóló kihívások miatt szükségessé vált az Ügynökség megbízatásának alapos újragondolása és újrafogalmazása, és ennek révén az Európai Unió prioritásainak és igényeinek hangsúlyosabb figyelembevétele****, a válaszadási képesség rugalmasabbá tétele, a készségek és a képességek fejlesztése és az Ügynökség operatív hatékonyságának és tevékenysége átfogó hatásainak megerősítése. Ezáltal gondoskodni lehet arról, hogy az ENISA működése az egyes tagállamoknak és az Európai Uniónak mint egésznek egyaránt állandó jelleggel a javára váljék.*”

A Tanács 2009. december 18-án állásfoglalást fogadott el „*a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről*”,[7] amely hangsúlyozza, hogy „***a módosított megbízatással működő ENISA-nak az EU szakértői központjaként kell működnie az EU-val kapcsolatos hálózat- és információbiztonsági kérdésekben***”.

A Bizottság által „Európa 2020: Az intelligens, fenntartható és inkluzív növekedés stratégiája” címmel közzétett dokumentum[8] az Európa elé 2020-ra kitűzött célok teljesítése érdekében megteendő egyik kiemelt kezdeményezésként az európai digitális menetrendet jelölte meg, amelyben központi helyet foglal el a hálózat- és információbiztonság kérdése. Az **európai digitális menetrenddel kapcsolatos bizalmat és biztonságot megcélzó kezdeményezés célja annak biztosítása, hogy az EU, a tagállamok és az érdekeltek magas szinten felkészülhessenek a hálózat- és az információbiztonsággal kapcsolatos problémák megelőzésére, észlelésére és hatékonyabb kezelésére, és továbbfejleszthessék ilyen irányú képességeiket**. Ez hozzá fog járulni az európai egységes digitális piacon a

---

5 A nyilvános konzultáció 2008. november 7-től 2009. január 9-ig tartott. A nyilvános konzultációról összeállított jelentés a http://ec.europa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm internetcímen olvasható.

6 A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a kritikus informatikai infrastruktúrák védelméről, COM(2009) 149, 2009. március 30.

7 A Tanács állásfoglalása (2009. december 18.) a hálózat- és információbiztonság együttműködésre építő európai megközelítéséről (2009/C 321/01).

8 COM(2010) 2020.

bizalom és a biztonság megerősödéséhez, és javítani fogja az európai vállalkozások versenyképességét.

2. PROBLÉMAMEGHATÁROZÁS

2.1. Mi a probléma lényege?

Az érdekelteket az alábbi részproblémák teszik kiszolgáltatottá a hálózat- és információbiztonsági természetű veszélyforrásoknak és váratlan eseményeknek. Mindegyik azt mutatja, hogy a probléma kezeléséhez egy olyan megbízható EU-szintű struktúrára van szükség, amely szerte Európában képes lépést tartani a hálózat- és információbiztonságot övező technológiai és piaci feltételek folyamatos változásával.

- **A nemzeti szintű erőfeszítések sokfélesége és szétaprózódottsága.** A hálózat- és az információbiztonság területén jelentkező problémák nem igazodnak az országhatárokhoz, ezért eredményesen nem lehet ellenük kizárólag nemzeti szintű eszközökkel küzdeni. Az egyes tagállamok közszervei eltérő módszerekkel próbálják meg kezelni a problémát. A különböző tagállamokban érvényben lévő biztonsági előírások sokfélesége az európai uniós léptékben működő vállalkozásokra is többletterhet ró, ami az erőfeszítések elaprózódását és a versenyképesség gyengülését eredményezi az európai belső piacon.

- **Európa gyenge korai figyelmeztető és válaszadási képessége.** A jelenlegi nemzeti szintű korai figyelmeztető és eseménykezelő rendszerek jelentős eltéréseket mutatnak, miközben EU-szinten nem működik ilyen rendszer. Szükség van olyan szakpolitikai eszközökre, amelyek azonosítják a hálózat- és az információbiztonság területén jelentkező kockázatokat és rendszereink gyenge pontjait, létrehozzák a válaszadás mechanizmusait, és gondoskodnak arról, hogy ezeket a válaszadási mechanizmusokat az érdekeltek ismerjék és alkalmazzák.

- **A folyamatosan változó problémákra vonatkozó megbízható európai adatok hiánya és az ezzel összefüggő ismeretek elégtelen volta.** Nagyon kevés kvantitatív adat áll rendelkezésünkre a hálózat- és információbiztonságot érintő váratlan események hatásairól vagy akár csak a számáról, ami igencsak megnehezíti mind a megfelelő intézkedések kidolgozásán munkálkodó szakpolitikai döntés-előkészítők és döntéshozók, mind pedig a biztonsági célú beruházásaikat tervező vállalkozások dolgát.

- **A hálózat- és információbiztonság területén jelentkező kockázatok és kihívások nem kellő ismerete.** A hálózat- és információbiztonság biztosításával kapcsolatos felelősség az egyes érintett személyek és szervezetek vállán nyugszik, a felelősségi viszonyok azonban nincsenek minden esetben egyértelműen meghatározva, és az ezzel kapcsolatos kommunikáció is hiányos. A fogyasztók gyakran alábecslik a hálózat- és információbiztonsági kockázatokat, és nincsenek kellőképpen tisztában a saját IKT-rendszereik biztonságával kapcsolatos felelősségükkel, a vállalkozások pedig elsősorban a hálózat- és információbiztonság költségeit érzékelik, a potenciális megtakarásokat kevésbé.

- **A hálózat- és információbiztonság területén felmerülő problémák nemzetközi vetületei.** A hálózat- és információbiztonság területét érintő veszélyforrások és az ezekből származó biztonsági események természetüknél fogva nemzetköziek, ezért fennáll annak a veszélye, hogy nemzetközi szintű erőfeszítések hiányában az EU fellépése nem lesz elegendően eredményes. Ahhoz, hogy az EU nemzetközi pozíciói javulhassanak, európai

uniós stratégiát kell kialakítani, és az EU-t referenciaponttá kell tenni a hálózat- és információbiztonság területén.

- **Az együttműködési modellek szükségessége a politikai célok megfelelő szintű valóra váltásához.** A hálózat- és információbiztonságra irányuló szakpolitika megfelelő színvonalú végrehajtásához EU-szintű együttműködési modellek kellenek. Az érdekelteknek a hálózat- és információbiztonságra vonatkozó stratégiájuk végrehajtása keretében útmutatásra van szükségük a hálózat- és információbiztonságot érintő veszélyforrások azonosításához és a helyes gyakorlat kialakításához.

- **A számítógépes bűnözés elleni hatékonyabb fellépés szükségessége.** A hálózat- és információbiztonsággal kapcsolatos erőfeszítéseknek eddig elsősorban a volt első pillér, azaz az intézmények közötti egyeztetések adtak keretet. A Lisszaboni Szerződés hatálybalépésével most érdemes szélesebb feladatkörrel felruházni a hálózat- és információbiztonsággal foglalkozó ügynökséget, vagyis tevékenységét olyan „második és harmadik pilléres" területekre is kiterjeszteni, amelyeken korábban a Tanács egyedül hozott döntéseket.

2.2. Kit érint a legsúlyosabban a probléma?

A hálózat- és információbiztonság területén jelentkező váratlan események számos érdekeltre lehetnek nagy hatással: nagy és kisebb vállalkozásokra, állami szervekre, hatóságokra és az egyes polgárokra egyaránt. Más szóval a hálózat- és információbiztonság mindenkit érint, és mindenki felelősséggel tartozik érte.

A hálózat- és információbiztonság területén bekövetkező váratlan eseményeknek sem a pontos számáról, sem a gazdasági hatásairól nincsenek vagy csak alig vannak objektív kvantitatív adataink. Jelzésértékű ugyanakkor, hogy az IDC EMEA piacfelmérése[9] szerint az EU-27 háztartásainak 28%-át érték az előző 12 hónap folyamán problémák kéretlen elektronikus levelek vagy számítógépes vírusok miatt, míg az előző évben az üzleti szektor felhasználóinak átlagosan 7%-a élt át biztonsági eseményt.

3. AZ EU-SZINTŰ FELLÉPÉS INDOKOLTSÁGA ÉS HOZZÁADOTT ÉRTÉKE, SZUBSZIDIARITÁS

A hálózatok és az informatikai rendszerek egymástól való kölcsönös függése rendkívül nehézzé, majdhogynem lehetetlenné teszi az egyes ember számára, hogy egyedül helyesen felmérje, milyen globális gazdasági és társadalmi hatásokkal járnak a hálózat- és információbiztonság területén jelentkező váratlan események kivédésére meghozott intézkedései. Az eltérő nemzeti szintű politikák és gyakorlati megoldások megtörik a belső piac működését – egyrészről a hálózat- és információbiztonság területén bekövetkező váratlan események negatív externáliái miatt (az elégtelen politika a többi tagállam piacaira is kihat), másrészről pedig a helyes politika pozitív externáliái következtében (az egyik tagállamban követett helyes gyakorlat szélesebb körben is javítja a hálózat- és információbiztonság helyzetét, így társadalmi szempontból egyértelműen jótétemény). Az EU-politika

[9] IDC EMEA, The European Network and Information Security Market, Scenario, Trends and Challenges („Az európai hálózat- és információbiztonsági piac, forgatókönyvek, tendenciák és kihívások"), 2009. április. A dokumentum az Eurobarometer 2007. áprilisi „E-Communications" felmérésére hivatkozik.

beavatkozása tehát indokolt, hiszen valós hozzáadott értéket képes biztosítani a belső piac működéséhez. Ezt a hozzáadott értéket már az ENISA-t létrehozó 460/2004/EK rendelet is felismerte, amikor az ENISA egyik céljaként a belső piac zavartalan működésének elősegítését jelölte meg.

Ezen túlmenően a hálózat- és információbiztonság területén való európai uniós fellépést a *szubszidiaritás elve* is indokolja. Mint a kritikus informatikai infrastruktúra védelméről szóló közlemény is rámutat, a hálózat- és információbiztonságra irányuló tagállami politikákba való teljes be nem avatkozást zászlajára tűző EU-stratégia nem volna más, mint arra kérni a tagállamokat, hogy ki-ki csak a saját háza táját őrizze, és ne foglalkozzék az informatikai rendszerek egymástól való kölcsönös függésével. Megfelel tehát a szubszidiaritás elvének az a törekvés, mely a hálózat- és információbiztonságot fenyegető veszélyforrások határokon átívelő vonatkozásainak helyes kezelése érdekében kellő mértékű koordinációt igyekszik biztosítani a tagállamok között. Az EU-szintű fellépés emellett a meglévő nemzeti szintű politikák eredményességét is növeli.

Az EU polgárai egyre nagyobb mértékben bízzák adataikat komplex informatikai rendszerekre (vö. például a „számítási felhő" jelenségével). A hálózat- és információbiztonságra vonatkozó kellően összpontosított, együttműködésre építő szakpolitikai fellépés ennek megfelelően komoly mértékben segítheti az *alapjogok*, különösen pedig *a személyes adatok és a magánélet védelméhez fűződő jog hatékony érvényesülését*. Az EU fellépése már csak ezért is bőven indokoltnak tűnik.

4. SZAKPOLITIKAI CÉLKITŰZÉSEK

A hatásvizsgálat áttekinti, hogy egy korszerűsített hálózat- és információbiztonsági ügynökség, melyet széles körben a legalkalmasabb szervezeti struktúrának tartanak, milyen mértékben alakítható ki a legkedvezőbben úgy, hogy más uniós eszközökkel együtt hozzájárulhasson a szakpolitikai célkitűzések teljesítéséhez.

Az általános célkitűzés annak biztosítása, hogy az EU, a tagállamok és az érdekeltek magas szinten felkészülhessenek a hálózat- és az információbiztonsággal kapcsolatos problémák megelőzésére, észlelésére és hatékonyabb kezelésére, és továbbfejleszthessék ilyen irányú képességeiket. Ez hozzá fog járulni az európai egységes digitális piacon a bizalom és a biztonság megerősödéséhez, és javítani fogja az európai vállalkozások versenyképességét.

Ezt a célkitűzést a hatásvizsgálat hét **konkrét célterületre** vetíti ki:

(1) **Koherensebb szabályozás** – iránymutatás és tanácsadás a Bizottság és a tagállamok részére a hálózat- és információbiztonság holisztikus normatív keretének kialakításában, illetőleg naprakésszé tételében

(2) **Megelőzés, észlelés és reagálóképesség** – a készültség javítása, ennek érdekében hozzájárulás egy európai korai figyelmeztető és eseményreagáló képességhez; páneurópai készenléti tervek és gyakorlatok

(3) **A szakpolitikai döntéshozatal támogatása** – segítségnyújtás és tanácsadás a Bizottság és a tagállamok részére

(4) **Az érdekeltek felkészítése a kihívásokra** – a biztonság és a kockázatkezelés kultúrájának kialakítása a köz- és a magánszektor szereplői közötti információcsere és széles körű együttműködés ösztönzésével, a lakosság és a kis- és középvállalkozások

közvetlen előnyére is; a hálózat- és információbiztonsággal kapcsolatos tudatosság kultúrájának kialakítása

(5) **Európa életképessé tétele nemzetközi viszonylatban** – magas szintű együttműködés kialakítása harmadik országokkal és nemzetközi szervezetekkel a hálózat- és információbiztonság területén alkalmazandó globális stratégia kialakítása, valamint az európai hatókörű magas szintű nemzetközi kezdeményezések megtételének elősegítése érdekében

(6) **Együttműködésen alapuló végrehajtás** – az együttműködés elősegítése a hálózat- és információbiztonságra vonatkozó szakpolitikák végrehajtásában

(7) **Küzdelem a számítástechnikai bűnözés ellen** – eredményes válaszlépések kialakítása a számítógépes bűnözés hálózat- és információbiztonsági vetületeivel szemben, együttműködésben a (volt) második és harmadik pilléres hatóságokkal, köztük az Europollal.

5. LEHETSÉGES SZERVEZETI FORMÁK, SZAKPOLITIKAI VÁLASZTÁSI LEHETŐSÉGEK

A fent felsorolt szakpolitikai választási lehetőségekhez rendelhető különböző lehetséges szervezeti formákat a hatásvizsgálat (4. fejezet és 4. melléklet) tekinti át részletesen. Ezek a szervezeti formák a következők: (i) ügynökség; (ii) köz-magán partnerség (ppp), kisebb vagy nagyobb mértékben formális keretek között; (iii) informális kapcsolattartási hálózat; (iv) az illetékes szervek állandó hálózata; és (v) a feladatok ellátása közvetlenül a Bizottság valamely szervezeti egysége által.

E különböző szervezeti formák összehasonlítása alapján a következő szempontok miatt az ügynökségi forma tűnik a rendelkezésre álló szakpolitikai eszközök közül a legkedvezőbbnek: (1) jogbiztonság a szervezeti struktúrát és az érdemi kérdéseket illetően; (2) alkalmasság egy olyan érzékeny ágazat sajátos problémáinak megoldására, mint a hálózat- és információbiztonsági (külső szakértő szerv, az érintettek közötti kapcsolatok koordinálása, a tagállamok részvétele/elkötelezettsége); és (3) az ENISA elfogadottsága és jó híre a hálózat- és információbiztonsággal foglalkozók körében.

Ennek megfelelően a következőkben bemutatandó szakpolitikai választási lehetőségeket az ügynökségi formára vonatkozóan dolgoztuk ki és értékeltük részletesen.

1. lehetőség: A beavatkozás mellőzése

A beavatkozás teljes mellőzése esetében azt feltételeztük, hogy az ENISA 2012 márciusától megszűnik létezni, és egyetlen európai uniós intézmény sem veszi át sem teljes egészében, sem részben annak jelenlegi feladatait.

Az ENISA megszüntetése azt jelentené, hogy minden eddigi befektetés (például egy, a nagymértékben szakosodott szakemberek számára is vonzó szervezet felállítása, a tapasztalatgyűjtés, vagy az érdekeltekkel, az érdekeltek számára, illetőleg a nemzetközi intézményekkel való hálózatépítés terén) kárba veszne éppen akkor, amikor a már felállt ügynökség kezdi felvenni az utazósebességet.

Az európai hálózat- és információbiztonsági problémakör összetett volta egy korszerűsített és megerősített ügynökséget tesz szükségessé, nem pedig a már meglévő bezárását. Erre utal,

hogy például az elektronikus hírközlés átalakított keretszabályozása[10] kifejezetten új feladatokat jelöl ki az ENISA számára, mint ahogy az is, hogy az érdekeltek széles körben támogatásukról biztosították a hálózat- és információbiztonság területén működő európai ügynökség súlyának növelését.

2. lehetőség: A jelenlegi politika folytatása változatlan formában

A 2. lehetőség a „minden marad a régiben" elvet jelenti, vagyis azt, hogy a jelenleg is meglévő szakpolitikai eszköz a jelenlegi formában és a jelenlegi források mellett marad fenn a továbbiakban is. Az érdekeltek nagy általánosságban egyetértenek abban, hogy az ENISA mára a hálózat- és információbiztonságot érintő kérdések hiteles referenciapontjává, a szakterület kiválósági központjává fejlődött.

A létszám és a költségvetés jelenlegi korlátai mellett az ügynökség csak a hálózat- és információbiztonsággal kapcsolatos kérdések egy igen szűk körére lenne képes hatást kifejteni. Ez azonban ellentétes volna azzal, amit az érdekeltek általában látni szeretnének. Ha az ügynökség nem kapja meg a lehetőséget a továbbfejlődésre és a megnövekedett elvárásoknak való megfelelésre, akkor végső soron hitele is veszélybe kerülhet.

3. lehetőség: Az ENISA jelenlegi funkcióinak kiterjesztése a bűnüldöző és a magánélet védelmével foglalkozó szervek teljes bevonásával

Ez a lehetőség a hálózat- és információbiztonsági ügynökség szerepének kiterjesztését jelenti oly módon, hogy a szerv a jövőben a következő kérdésekre összpontosítana:

- kapcsolattartási hálózat létrehozása és fenntartása az érdekeltek között, valamint egy tudáshálózat létrehozása és fenntartása,
- támogató központként való működés a hálózat- és információbiztonság területén a szakpolitikai előkészítő és végrehajtó munka támogatására (különösen az elektronikus hírközlés adatvédelmi aspektusaival, az elektronikus aláírással és személyazonosság-megállapítással, valamint a hálózat- és információbiztonságra vonatkozó beszerzési standardokkal kapcsolatban),
- a kritikus informatikai infrastruktúrák védelmére és a számítógépes rendszerek ellenálló képességére vonatkozó európai uniós politika támogatása (gyakorlatok, EP3R,[11] európai információmegosztási és figyelmeztető rendszer stb.),
- európai uniós keret létrehozása a hálózat- és információbiztonságra vonatkozó adatok gyűjtése érdekében, ennek részeként az adatközlés és az információmegosztás jogi keretei módszertanának és gyakorlati megvalósításának kidolgozása,
- a hálózat- és információbiztonság gazdaságtanának tanulmányozása és ennek dokumentálása,
- az együttműködés serkentése harmadik országokkal és nemzetközi szervezetekkel a hálózat- és információbiztonság területén alkalmazandó globális stratégia kialakítása, valamint az európai hatókörű magas szintű nemzetközi kezdeményezések megtételének elősegítése érdekében,

---

10 Lásd http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:HU:HTML

11 Az ellenálló képesség javításáért felelős köz-magán partnerség (EP3R), lásd COM(2009) 149.

- nem operatív feladatok ellátása a bűnüldöző hatóságok és az igazságszolgáltató szervek által folytatott együttműködés keretében, a hálózat- és információbiztonság területén.

Az Ügynökség rendelkezne mindazokkal az erőforrásokkal, amelyek szükségesek ahhoz, hogy tevékenységét kielégítő és mélyreható módon, azaz valós hatást kifejtve végezze. Több forrással az ENISA sokkal proaktívabb szerepet lenne képes vállalni, és több kezdeményezést tudna tenni az érdekeltek aktív részvételének ösztönzésére. Ez az új helyzet emellett nagyobb rugalmasságot is biztosítana, így a szerv gyorsabban lenne képes idomulni a hálózat- és információbiztonság területén tapasztalható folyamatos változásokhoz.

4. lehetőség: Operatív funkciók biztosítása a számítógépes támadások és a biztonsági események elleni küzdelemben való részvétel céljából

Ez esetben a 3. lehetőség kapcsán felsorolt feladatok mellett az ügynökség operatív funkciókat is ellátna, így például aktívabb szerepet kapna a kritikus informatikai infrastruktúra védelmére vonatkozó uniós törekvésekben, ezen belül különösen a biztonsági események megelőzésében és kezelésében, konkrétan például azáltal, hogy az EU számítástechnikai katasztrófaelhárító csoportjaként (Computer Emergency Response Team – CERT) működne a hálózat- és információbiztonság területén, illetőleg azáltal, hogy európai uniós hálózat- és információbiztonsági válságközpontként koordinálná a nemzeti CERT-ek munkáját, ideértve mind a napi szintű rutinfeladatokat, mind pedig a vészhelyzeti szolgáltatásokat.

Ez a lehetőség az ügynökség rendelkezésére álló költségvetés és humánerőforrások jelentős megnövelését igényelné, ami felveti azt a kérdést, hogy vajon az Ügynökség képes lenne-e az új feladatokat és az új forrásokat hatékonyan befogadni, és a várt előnyök tükrében fel tudná-e eredményesen használni megnövekedett költségvetését.

5. lehetőség: Operatív funkciók biztosítása a bűnüldöző hatóságok és az igazságszolgáltatás munkájának a számítástechnikai bűnözés területén való segítése céljából

A 4. lehetőség esetében megjelölt feladatokon túlmenően ez esetben az ügynökség:

- eljárásjogi támogatást nyújtana (vö. egyezmény a számítástechnikai bűnözésről), például forgalmi adatokat gyűjtene, adattartalmat figyelne meg, szolgáltatásbénító („denial-of-service”) támadások esetén adatforgalmat figyelne;
- a hálózat- és információbiztonsági vonatkozású bűncselekmények kivizsgálásában való részvétel céljából szakértő központként szolgálna.

A 4. lehetőséghez hasonlóan ez esetben is jelentős mértékben növelni kellene az ügynökség erőforrásait, és ez esetben is ugyanazok az aggályok merülnek fel a befogadóképesség, illetve a költségvetés hatékony felhasználása tekintetében.

6. A SZAKPOLITIKAI VÁLASZTÁSI LEHETŐSÉGEK ÖSSZEHASONLÍTÁSA ÉS A HATÁSOK ELEMZÉSE

A lehetséges gazdasági, társadalmi és környezeti hatások elemzése alapján kimondható, hogy ***az 1. lehetőség*** minden szempontból kedvezőtlen lenne, és a helyzet rosszabbodását eredményezné.

A 2. lehetőség elmarad az optimálistól, mert az ügynökség nem rendelkezne a hálózat- és információbiztonság területén tapasztalható folyamatos változásokból fakadó kihívások

megfelelő kezeléséhez szükséges erőforrásokkal, ami kockáztatná a szerv jó hírét, végső soron pedig hitelességét is.

A 3. lehetőség esetében a korszerűsített hálózat- és információbiztonsági ügynökség hozzájárulna:

a nemzeti szintű politikák szétaprózódottságának csökkentéséhez (első részprobléma), a tényadatokon alapuló, kellően tájékozott és megalapozott szakpolitikai döntés-előkészítői és döntéshozói munkához (harmadik részprobléma), valamint a hálózat- és információbiztonság területén jelentkező kockázatok és kihívások általános ismeretének növeléséhez (negyedik részprobléma) azzal, hogy:

- hatékonyabb tagállami szintű adatgyűjtést tenne lehetővé a kockázatokra, a veszélyforrásokra és a sérülékeny elemekre vonatkozóan,
- több hozzáférhető információt biztosítana a már meglévő és a jövőben felmerülő kihívásokról és kockázatokról,
- jobb minőségű tagállami hálózat- és információbiztonsági politikákat eredményezne,

Európa korai figyelmeztető és válaszadási képességének javításához (második részprobléma) azzal, hogy:

- segítené a Bizottságot és a tagállamokat a páneurópai gyakorlatok megszervezésében, miáltal méretgazdaságosságot tenne lehetővé az európai uniós szintű biztonsági események kezelésében,
- elősegítené az EP3R működését, miáltal – a biztonság és az ellenálló képesség területén meghatározandó közös politikai céloknak és EU-szintű standardoknak köszönhetően – végső soron hozzájárulna a beruházási kedv növeléséhez,

egy közös globális stratégia kialakításának elősegítéséhez a hálózat- és információbiztonság területén (ötödik részprobléma) azzal, hogy:

- fokozná az EU-n kívüli országokkal folytatott információ- és tudáscserét,

a számítástechnikai bűnözéssel szembeni küzdelem hatékonyságának és eredményességének javításához (hetedik részprobléma) azzal, hogy:

- nem operatív jellegű feladatok ellátásával részt venne a bűnüldöző és az igazságszolgáltató szervek együttműködésében például kétirányú információcsere és továbbképzések szervezése útján (együttműködve például az Európai Rendőrakadémiával).

A 4. lehetőség a 3. lehetőség esetében elértnél nagyobb operatív szintű hatást fejtene ki. Az Európai Unió hálózat- és információbiztonsági CERT-jeként és a nemzeti szintű CERT-ek munkájának koordinálásával az ügynökség egyebek mellett nagyobb méretgazdaságosság elérését tenné lehetővé az egész EU-t érintő biztonsági események kezelésében, és a biztonság és az ellenálló képesség fokozásával csökkentené a vállalkozások működési kockázatait.

Az 5. lehetőség a 3. és a 4. lehetőséghez képest nagyobb eredményességet biztosítana a számítástechnikai bűnözés elleni küzdelemben azzal, hogy a bűnüldöző és az igazságszolgáltató szervek támogatása érdekében további operatív feladatokat rendelne az ügynökséghez.

Miközben hatásait illetően mind a 4., mind az 5. lehetőség kedvezőbb lenne, mint a 3., mindkét esetben tartani kell attól, hogy a kritikus informatikai infrastruktúra védelmével kapcsolatos új feladatkörök érzékenyen érintenék a tagállamokat (a tagállamok egy része nem támogatná az operatív funkciók centralizálását). A feladatok ilyen irányú kibővítése az ügynökség helyzetét is nehezebben megfoghatóvá tenné. Ha az ügynökség tevékenységi területe ilyen új, az eddigiektől merőben eltérő operatív feladatokkal egészülne ki, az rövid távon olyan szempontból is igencsak kockázatos volna, hogy az ügynökség esetleg nem lenne képes ezt a fajta feladatkörét egy bizonyos ideig ésszerűen ellátni. Végül, de nem utolsósorban, a 4. és az 5. lehetőség esetében a költségek is túlságosan magasak: az új feladatok az ENISA jelenlegi költségvetésének négy-ötszörösére való növelését tennék szükségessé.

A korszerűsített hálózat- és információbiztonsági ügynökség szervezeti formájára adódó ***öt lehetőség hatásainak összehasonlítása*** alapján az 1. és a 2. lehetőséget érdemes elvetni, mert egyik sem tenné lehetővé a hálózat- és információbiztonság komplex problematikájának megfelelő EU-szintű megoldását. Ezzel szemben a 3., a 4. és az 5. lehetőség esetében az EU képes lenne megfelelő szinten kezelni a jövőben a hálózat- és információbiztonság területén jelentkező szakpolitikai jellegű kihívásokat. Jelen pillanatban ugyanakkor a 4. és az 5. lehetőség mind a tagállamok többségének politikai érzékenységét, mind a költségvetési vonzatot tekintve túlságosan ambiciózusnak tűnik. Ezért ***a hálózat- és információbiztonság területén azonosított problémákat minden bizonnyal a 3. megoldással lehet a leghatékonyabban kezelni.***

7. NYOMON KÖVETÉS ÉS ÉRTÉKELÉS: HOGYAN MÉRHETŐK A TÉNYLEGES KÖLTSÉGEK ÉS HASZNOK, HOGYAN MÉRHETŐ A KIFEJTENI KÍVÁNT HATÁS?

A jogalkotási javaslat értelmében rendszeres időközönként értékelést kell végezni, melynek eredményeit a Bizottság köteles továbbítani az Európai Parlamentnek és a Tanácsnak, illetőleg nyilvánosságra hozni. Ebben az értékelésben az ügynökség igazgatóságával közösen megállapított feladatmeghatározás alapján figyelembe kell venni valamennyi releváns érdekelt észrevételeit, és elemezni kell, hogy az ügynökség mennyire hatékonyan teljesíti céljait, hogy az ügynökségi forma továbbra is a legmegfelelőbb eszköz-e az adott célra, valamint hogy az ügynökség megbízatása és/vagy az azt létrehozó rendelet más rendelkezései módosításra szorulnak-e. Az értékelés elvégzését követően az igazgatóság ajánlásokat fogalmaz meg a Bizottság részére a rendelet szükségesnek ítélt módosításairól. Az ügynökség igazgatósága és ügyvezető igazgatója az értékelés eredményeit köteles figyelembe venni a szerv tevékenységének többéves tervezésekor.

Az Ügynökség működése felett az ombudsman a Szerződés 228. cikkének megfelelően felügyeleti jogkört gyakorol.