EURÓPAI BIZOTTSÁG

AZ EURÓPAI UNIÓ KÜLÜGYI ÉS BIZTONSÁGPOLITIKAI FŐKÉPVISELŐJE

Brüsszel, 2013.2.7.
JOIN(2013) 1 final

KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

Az Európai Unió kiberbiztonsági stratégiája:

Nyílt, megbízható és biztonságos kibertér

KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

Az Európai Unió kiberbiztonsági stratégiája:

Nyílt, megbízható és biztonságos kibertér

1. BEVEZETÉS

1.1. Előzmények

Az elmúlt húsz évben az internet és tágabb értelemben a kibertér jelentős hatást gyakorolt a társadalom valamennyi szegmensére. Mindennapjaink, alapvető jogaink, társas életünk és gazdaságaink az információs és kommunikációs technológiák zökkenőmentes működésétől függnek. A nyitott és szabad kibertér világszerte előmozdította a politikai és társadalmi integrációt; ledöntötte a határokat az országok, a közösségek és a polgárok között, valamint lehetővé tette a globális interakciót és az információk és elképzelések megosztását; fórumot biztosított a szólásszabadság és az alapvető jogok gyakorlására, és támogatta az embereket abban, hogy megpróbálják demokratikussá és igazságosabbá tenni társadalmaikat – legfőképp az arab tavasz során.

A kibertér csak akkor maradhat nyitott és szabad, ha a kibertérben is ugyanazok a normák, alapelvek és értékek érvényesülnek, mint amelyeket az Európai Unió a való életben képvisel. Az alapvető jogokat, a demokráciát és a jogi normákat ebben a közegben is meg kell védeni. Szabadságunk és jólétünk egyre nagyobb mértékben függ a stabil és innovatív internettől, amely tovább fog fejlődni, ha a magánszektor innovációja és a civil társadalom hozzájárul a növekedéséhez. Internetes szabadság nem létezik azonban megbízhatóság és biztonság nélkül. A virtuális teret meg kell védeni a biztonsági eseményektől, a rosszhiszemű tevékenységektől és a visszaélésektől; a kormányok fontos szerepet játszanak a szabad és biztonságos kibertér biztosításában. A kormányokra számos feladat vár: a hozzáférés és a nyitottság védelme, az internetes alapvető jogok tiszteletben tartása és védelme, valamint az internet megbízhatóságának és átjárhatóságának fenntartása. A kibertér jelentős részének tulajdonosai és üzemeltetői azonban a magánszektorból kerülnek ki, így bármilyen sikeres kezdeményezést csak a magánszektor vezető szerepének elismerésével lehet megalkotni.

Az információs és kommunikációs technológia (ikt) vált gazdasági növekedésünk gerincévé, és az összes gazdasági ágazat számára fontos erőforrást jelent. Az ikt napjainkban a gazdaságaink működését biztosító összetett rendszerek alapjául szolgál a pénzügyi, egészségügyi, energiaügyi, közlekedési és egyéb alapvető fontosságú ágazatokban; számos üzleti modell épül az internet folyamatos rendelkezésre állására és az információs rendszerek zavartalan működésére.

Az egységes digitális piac létrehozásával Európa évente mintegy 500 milliárd EUR-val növelhetné GDP-jét[1], ami 1000 EUR/fő növekedési átlagot jelent. Az új internetalapú technológiák elterjedéséhez – ideértve az elektronikus fizetést, a számítási felhőt vagy a gépek közötti kommunikációt[2] – bizalomra van szükség az emberek részéről. Az Eurobarométer

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Például olyan, érzékelőkkel felszerelt növények, amelyek kommunikálnak az öntözőrendszerrel, amikor meg kell locsolni őket.

2012-es felméréséből[3] azonban kiderült, hogy az európaiak közel egyharmada sajnos nem tudja az internetet kellő bizalommal használni banki műveletekre vagy vásárlásra. A válaszadók túlnyomó többsége ezenkívül biztonsági megfontolásokból nem oszt meg személyes információkat interneten keresztül. Az Unió internet felhasználóinak több mint tíz százaléka volt már internetes csalás áldozata.

Az utóbbi évek tapasztalatai alapján a digitális világ óriási előnyöket tartogat, ugyanakkor támadható is. Riasztó mértékben nő a szándékos és véletlen kiberbiztonsági[4] események előfordulása, amelyek olyan, természetesnek vett alapvető szolgáltatások biztosításában okozhatnak fennakadást, mint a vízellátás, az egészségügyi ellátás, a villamosenergia- vagy a mobilszolgáltatás. Ezek a fenyegetések különböző forrásokból származhatnak, ideértve a bűncselekményeket, a politikai célú, terror- vagy államilag támogatott támadásokat, valamint a természeti katasztrófákat és a nem szándékosan elkövetett hibákat is.

A magánszektor és az egyének ellen irányuló számítástechnikai bűncselekmények[5] az EU gazdaságára már most hatással vannak. A számítástechnikai bűnelkövetők egyre kifinomultabb módszerekkel hatolnak be az információs rendszerekbe, lopnak el fontos adatokat vagy követelnek váltságdíjat vállalatoktól. A gazdasági kémkedés és az államilag támogatott tevékenységek növekedése a kibertérben új típusú fenyegetést jelent az Európai Unió kormányai és vállalatai számára.

Az Unión kívüli országok kormányai megfigyelés és saját polgáraik ellenőrzése céljából is visszaélhetnek a kibertérrel. Az Unió ez ellen annyit tehet, hogy előmozdítja az internetes szabadságot, és biztosítja az alapvető jogok tiszteletben tartását az internethasználattal kapcsolatban.

Ezek a tényezők megmagyarázzák, hogy a különböző országok kormányai miért fogtak világszerte kiberbiztonsági stratégiák kidolgozásába, és miért tekintik a virtuális teret egyre fontosabb nemzetközi kérdésnek. Itt az ideje annak, hogy az Unió határozottabban lépjen fel ezen a területen. Ez, a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: főképviselő) által előterjesztett, az Európai Unió kiberbiztonsági stratégiájára vonatkozó javaslat felvázolja az Unió jövőképét, tisztázza a szerepköröket és felelősségi köröket, valamint meghatározza a szükséges intézkedéseket a polgárok jogainak határozott és hatékony védelme és támogatása alapján annak érdekében, hogy az Unió internetes környezete a legbiztonságosabb legyen a világon.

1.2. Kiberbiztonsági alapelvek

A határokat nem ismerő, sokrétű internet a globális fejlődés egyik legerősebb eszközévé vált, amely nem tartozik állami felügyelet vagy szabályozás hatálya alá. Habár fontos, hogy a

---

[3] 390. sz. Eurobarométer különfelmérés a kiberbiztonságról, 2012.

[4] A kiberbiztonság azokat a biztosítékokat és intézkedéseket jelenti, amelyek segítségével mind a polgári, mind a katonai területeken egyaránt megvédhető a virtuális tér azoktól a fenyegetésektől, amelyek azok összefüggő hálózataival és információs infrastruktúráival kapcsolatosak, vagy amelyek károsíthatják ezeket. A kiberbiztonság célja a hálózatok és az infrastruktúra rendelkezésre állásának és integritásának, valamint a benne lévő információk titkosságának megőrzése.

[5] A számítástechnikai bűnözés számos különböző bűncselekményt jelenthet, amelyek során a számítógépek és az információs rendszerek az elsődleges eszközök, illetve ezek az elsődleges célok. A számítástechnikai bűnözés hagyományos szabálysértéseket (például csalás, hamisítás és személyazonosság-lopás), tartalmakhoz kapcsolódó szabálysértéseket (például gyermekpornográfia internetes terjesztése vagy fajgyűlöletre uszítás) és csak számítógépekre és információs rendszerekre korlátozódó szabálysértéseket (például információs rendszerek elleni támadások, hozzáférés megtagadása vagy rosszindulatú szoftverek) is magában foglal.

magánszektor továbbra is vezető szerepet töltsön be az internet kiépítésében és mindennapos kezelésében, egyre erősebbé válik az átláthatóságra, az elszámoltathatóságra és a biztonságra vonatkozó igény. Ez a stratégia tisztázza azokat az alapelveket, amelyeknek uniós és nemzetközi szinten egyaránt vezérelniük kell a kiberbiztonsági politikát.

Az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikai világra

Ugyanazok a törvények és normák vonatkoznak a kibertérre, mint amelyek mindennapjaink más területein is érvényesek.

Az alapvető jogok, a szólásszabadság, a személyes adatok és a magánélet védelme

A kiberbiztonság csak akkor lehet hatékony és eredményes, ha az Európai Unió Alapjogi Chartájában meghatározott alapjogokra és alapvető szabadságjogokra, valamint az Európai Unió alapértékeire épül. Ugyanez fordítva is igaz: az egyének jogai nem biztosíthatóak biztonságos hálózatok és rendszerek nélkül. A kiberbiztonság céljából végzett információmegosztást – amennyiben személyes adatok forognak kockán – az uniós adatvédelmi jogszabályoknak megfelelően kell végezni, és az egyének jogait ezen a területen teljes mértékben figyelembe kell venni.

Mindenki számára biztosított hozzáférés

A polgárok számára az internethez való hozzáférés korlátozottsága vagy hiánya, valamint a digitális írástudatlanság hátrányt jelent, tekintve, hogy a társadalmi tevékenységeket a digitális világ nagymértékben áthatja. Mindenki számára lehetővé kell tenni az internethez és az akadálytalan információáramláshoz való hozzáférést. Biztosítani kell az internet integritását és biztonságát annak érdekében, hogy biztonságosan elérhető legyen mindenki számára.

Demokratikus és hatékony, számos érdekelt fél bevonásával történő irányítás

A digitális világot nem egyetlen jogalany irányítja. Jelenleg számos érdekelt fél – akik nagyrészt kereskedelmi és nem kormányzati jogalanyok – vesz részt az internetes erőforrások, protokollok és szabványok mindennapos kezelésében és az internet fejlesztésében. Az Európai Unió elismeri az összes érdekelt fél fontosságát az internet jelenlegi szabályozási modelljében, és támogatja ezt a több érdekelt fél részvételén alapuló szabályozási megközelítést[6].

Közös felelősségünk: a biztonság

Amiatt, hogy életünk minden területén egyre jobban függünk az információs és kommunikációs technológiáktól, olyan sebezhető pontok alakultak ki, amelyeket pontosan meg kell határozni, alaposan elemezni kell, meg kell oldani vagy mérsékelni kell. Minden érintett szereplőnek, köztük az állami szerveknek, a magánszektornak és az egyes polgároknak is el kell ismerniük ezt a közös felelősséget, fel kell lépniük a saját védelmükben, és szükség esetén összehangolt válaszlépéseket kell tenniük a kiberbiztonság erősítése érdekében.

[6] Lásd még: A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: „Az internet szabályozása: a következő lépések”, COM(2009) 277.

2. STRATÉGIAI PRIORITÁSOK ÉS INTÉZKEDÉSEK

Az Európai Uniónak olyan internetes környezetet kell biztosítania, amely mindenki számára lehetővé teszi a lehető legnagyobb mérvű szabadságot és biztonságot. Habár alapvetően a tagállamok feladata, hogy megbirkózzanak a kibertérben felmerülő biztonsági problémákkal, ez a stratégia konkrét intézkedéseket javasol, amelyek javíthatják az Unió átfogó teljesítményét. A rövid és hosszú távú intézkedések különböző szakpolitikai eszközöket[7] tartalmaznak, és különböző típusú szereplőkre vonatkoznak, ideértve az Unió intézményeit, a tagállamokat, vagy magát az ágazatot.

A stratégiában ismertetett uniós jövőképet öt stratégiai prioritásban foglaltuk össze, amelyek a fent kiemelt kihívásokra adnak választ:

- kibertámadásokkal szembeni ellenálló képesség elérése;
- a számítástechnikai bűnözés drasztikus csökkentése;
- kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP) tekintetében;
- kiberbiztonsági ipari és technológiai erőforrások kifejlesztése;
- összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása.

2.1. A kibertámadásokkal szembeni ellenálló képesség elérése

A kibertámadásokkal szembeni ellenálló képesség Unió-szerte történő előmozdítása érdekében az állami hatóságoknak és a magánszektornak egyaránt ki kell fejleszteniük a szükséges képességeket és hatékonyan együtt kell működniük. Az eddig elvégzett tevékenységek révén elért pozitív eredmények alapján[8] további uniós fellépések segítségével elháríthatóak a főleg nemzetközi jellegű kiberkockázatok és -fenyegetések, és veszélyhelyzetekben összehangolt válaszlépésekre nyílik lehetőség. Ez jelentős mértékben elősegíti a belső piac megfelelő működését, és megerősíti az Unió belső biztonságát.

Ha a kiberbiztonsági események megelőzése, feltárása és kezelése érdekében nem teszünk jelentős erőfeszítéseket az állami és privát kapacitások, erőforrások és eljárások javítására, Európa továbbra is sebezhető marad. Ezért a Bizottság hálózat- és információbiztonsággal (NIS) kapcsolatos szakpolitikát hozott létre[9]. Az **Európai Hálózat- és Információbiztonsági Ügynökséget** (ENISA) 2004-ben hozták létre[10]. A Tanács és a Parlament jelenleg egyeztet az

---

7 Az információmegosztással kapcsolatos intézkedéseknek – amennyiben személyes adatok forognak kockán – meg kell felelniük az uniós adatvédelmi jogszabályoknak.

8 Lásd e közleményben, valamint a hálózat- és információbiztonságról szóló irányelvre vonatkozó bizottsági javaslatot kísérő bizottsági szolgálati munkadokumentum hatásvizsgálatában található hivatkozásokat, különösen a 4.1.4., az 5.2. szakaszt, a 2. mellékletet, a 6. mellékletet és a 8. mellékletet.

9 A Bizottság 2001-ben elfogadta a „Network and Information Security: Proposal for A European Policy Approach" (Hálózat- és információbiztonság: európai politikai megközelítésre irányuló javaslat) (COM(2001) 298) című közleményt; 2006-ban pedig a biztonságos információs társadalomra irányuló stratégiát (COM(2006) 251). A Bizottság 2009 óta cselekvési tervet és közleményt fogadott el a kritikus informatikai infrastruktúrák védelméről (CIIP) (a COM(2009) 149 dokumentumot a 2009/C 321/01. sz. tanácsi állásfoglalásban; a COM(2011) 163 dokumentumot pedig a 10299/11. sz. tanácsi következtetésekben hagyták jóvá).

10 A 460/2004/EK rendelet.

ENISA megerősítésére és megbízatása korszerűsítésére irányuló új rendeletről[11]. Az elektronikus hírközlési keretirányelv[12] előírja az elektronikus hírközlési szolgáltatóknak, hogy megfelelően kezeljék a hálózataikat érintő kockázatokat, és hogy jelentsék a jelentős biztonsági eseményeket. Az uniós adatvédelmi jogszabályok[13] ezenkívül előírják az adatkezelők számára, hogy biztosítsák az adatvédelmi követelmények és biztosítékok betartását, ideértve a biztonsággal kapcsolatos intézkedéseket, valamint a nyilvánosan hozzáférhető elektronikus hírközlési szolgáltatások területén be kell jelenteniük az illetékes nemzeti hatóságoknak többek között a személyes adatok megsértésével járó eseményeket.

Az önkéntes kötelezettségvállalásoknak köszönhetően bekövetkezett előrelépések ellenére Unió-szerte még mindig vannak hiányosságok, főleg a nemzeti képességek, a határokon átnyúló események esetében végzett koordináció, illetve a magánszektor részvétele és felkészültsége tekintetében. A stratégiát a következő célok érdekében **jogalkotási** javaslat kíséri:

- Közös nemzeti szintű minimumkövetelmények megállapítása a NIS tekintetében, amelyek az alábbiakra kötelezik a tagállamokat: a NIS-ben illetékes nemzeti hatóságok kijelölése; jól működő, hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT) létrehozása; és a NIS-re vonatkozó nemzeti stratégia és nemzeti együttműködési terv elfogadása. A kapacitásépítés és -koordináció az Unió intézményeit is érinti: 2012-ben állandó, hálózatbiztonsági vészhelyzeteket elhárító csoportot („CERT-EU”) hoztak létre, amely az uniós intézmények, ügynökségek és szervek informatikai rendszereinek biztonságáért felel.

- A NIS tekintetében illetékes nemzeti hatóságok közötti információmegosztás és kölcsönös segítségnyújtás lehetővé tétele érdekében összehangolt megelőzési, feltárási, mérséklési és reagálási mechanizmusok létrehozása. A NIS tekintetében illetékes nemzeti hatóságokat felkérik arra, hogy megfelelő uniós együttműködést biztosítsanak, különösen az uniós NIS együttműködési terv alapján, amelynek célja a több tagállamra kiterjedő kiberbiztonsági eseményekre való reagálás. Ez az együttműködés a tagállamok európai fóruma (EFMS)[14] összefüggésében elért előrelépésekre fog épülni. A fórumon, amely integrálható lesz a leendő együttműködési mechanizmusba, eredményes vitákra és megbeszélésekre került sor a NIS-szakpolitikáról.

- A magánszektor felkészültségének és részvételének javítása. Mivel a hálózati és információs rendszerek nagy része magántulajdonban van és a magánszektor szereplői üzemeltetik őket, a magánszektor bevonása létfontosságú a kiberbiztonság javítása szempontjából. A magánszektornak technikai szinten ki kell fejlesztenie saját ellenálló képességét a kibertámadásokkal szemben, és meg kell osztania a bevált gyakorlatokat a többi ágazattal is. A biztonsági eseményekre való reagálás, az okok azonosítása és az igazságügyi szakértői vizsgálatok elvégzése céljából kifejlesztett ágazati eszközöket a közszférának is hasznosítania kell.

---

11 COM(2010) 521. Az ebben a stratégiában előterjesztett intézkedések nem tartalmazzák az ENISA meglévő vagy jövőbeli megbízatásának módosítását.

12 A 2002/21/EK irányelv 13. cikke (1) bekezdésének a. és b. pontja.

13 A 95/46/EK irányelv 17. cikke; a 2002/58/EK irányelv 4. cikke.

14 A tagállamok európai fórumát a COM(2009) 149 közlemény hozta létre a tagállamok hatóságai közötti, a kritikus informatikai infrastruktúrák biztonságával és ellenálló képességével kapcsolatos bevált gyakorlatokról szóló vitákat ösztönző platformként.

A magánszektor szereplői esetében azonban még mindig nincsenek hatékony ösztönzők a NIS események vagy azok hatására vonatkozó megbízható adatok benyújtására, a kockázatkezelési kultúra elfogadására vagy a biztonsági megoldásokba való beruházásokra. A jogalkotási javaslat célja ezért annak biztosítása, hogy számos fontos terület (például az energia-, a közlekedési, a bank-, a tőzsdeszektor, a fő internetes szolgáltatások szolgáltatói, valamint a közigazgatások) szereplői értékeljék a felmerülő kiberbiztonsági kockázatokat, megfelelő kockázatkezeléssel biztosítsák, hogy a hálózati és információs rendszerek megbízhatóak és ellenállóképesek legyenek, és megosszák a megszerzett információkat a NIS tekintetében illetékes nemzeti hatóságokkal. A kiberbiztonsági kultúra elterjedése javíthatja a magánszektor üzleti lehetőségeit és versenyképességét, ami versenyelőnnyé kovácsolhatja a kiberbiztonságot.

Azokat a biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az alapvető szolgáltatások folytonosságára és a hálózati és információs rendszereken alapuló termékek biztosítására, az egyes szereplőknek be kell jelenteniük a NIS tekintetében illetékes nemzeti hatóságnak.

A NIS tekintetében illetékes nemzeti hatóságoknak más szabályozó szervekkel – különösen az adatvédelmi hatóságokkal – együtt kell működniük és információkat kell cserélniük. A NIS tekintetében illetékes hatóságoknak cserébe be kell jelenteniük a gyaníthatóan súlyos bűncselekményeket a bűnüldöző hatóságoknak. A nemzeti illetékes hatóságoknak ezenkívül egy arra kijelölt weboldalon rendszeresen nem bizalmas információkat kell közzétenniük a biztonsági eseményekre, kockázatokra és összehangolt válaszlépésekre vonatkozó folyamatos korai előrejelzésekről. A jogi kötelezettségek nem helyettesíthetik és nem akadályozhatják meg például a köz- és magánszektor közötti, a biztonsági szintek javítását, valamint az információk és bevált gyakorlat cseréjét szolgáló informális és önkéntes együttműködés kiépítését. Az európai köz-magán reziliencia-partnerség (EP3R[15]) különösen stabil és hatékony uniós szintű platform, amelyet tovább kell fejleszteni.

Az Európai Hálózatfinanszírozási Eszköz[16] pénzügyi támogatást nyújt a legfontosabb infrastruktúrák számára, melyek összekapcsolják a tagállamok NIS képességeit, megkönnyítve ezáltal az együttműködést Unió-szerte.

Végül pedig az uniós szintű kiberbiztonsági eseményekkel kapcsolatos gyakorlatok nagyon fontosak a tagállamok és a magánszektor közötti együttműködés ösztönzése szempontjából. Az első gyakorlatra 2010-ben került sor a tagállamok részvételével („Cyber Europe 2010”), a második gyakorlatot pedig a magánszektor bevonásával 2012 októberében hajtották végre („Cyber Europe 2012”). Az Unió és az USA közös szimulációs gyakorlatára 2011 novemberében került sor („Cyber Atlantic 2011”). A következő évek programján további gyakorlatok szerepelnek nemzetközi partnerek részvételével.

---

15 Az ellenálló képesség javításáért felelős köz-magán partnerséget a COM(2009) 149 közlemény hozta létre. Ez a platform az elektronikus kommunikáció széles körű zavaraira való reagálás érdekében előrelépéseket kezdeményezett, és ösztönözte az állami és magánszektor közötti együttműködést az ellenálló képességgel kapcsolatos legfontosabb eszközök, erőforrások, funkciók és közös alapkövetelmények terén, valamint az együttműködési szükségletek és mechanizmusok terén.

16 https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. 09.03.02. számú CEF költségvetési tétel – Távközlő hálózatok (az internetes nemzeti közszolgálati hálózatok összekapcsolódásának és átjárhatóságának, valamint e hálózatok elérhetőségének előmozdítása érdekében).

A Bizottság:

- az európai kritikus infrastruktúrák hálózat- és információbiztonsági sebezhetőségeinek azonosítása és ellenálló rendszerek kifejlesztésének ösztönzése érdekében folytatja tevékenységeit, amelyeket a Közös Kutatóközpont a tagállamok hatóságaival és a kritikus infrastruktúrák tulajdonosaival és üzemeltetőivel szoros együttműködésben lát el.
- 2013 elején **a botnetek és rosszindulatú programok elleni küzdelemmel** kapcsolatos uniós finanszírozású kísérleti projektet[17] indít el a tagállamok, a magánszektorbeli szervezetek, például az internetszolgáltatók és a nemzetközi partnerek közötti koordináció és együttműködés keretének megteremtése érdekében.

A Bizottság az alábbiakra kéri az ENISA-t:

- A tagállamok támogatása az erős **nemzeti képességek** kialakításában **a kibertámadásokkal szembeni ellenálló képesség területén**, főleg az ipari vezérlőrendszerek, a szállítás és az energiaipari infrastruktúra biztonságával és ellenálló képességével kapcsolatos ismeretek összegyűjtése révén.
- Az ipari vezérlőrendszerekre szakosodott uniós hálózatbiztonsági incidenskezelő csoportok (SCIRT) megvalósíthatóságának vizsgálata 2013-ban.
- A tagállamok és az uniós intézmények további támogatása rendszeres **páneurópai kiberbiztonsági gyakorlatok** megrendezésével, amelyek az Unió nemzetközi kiberbiztonsági gyakorlatokban való részvételének működési alapjául is fognak szolgálni.

A Bizottság az alábbiakra kéri az Európai Parlamentet és a Tanácsot:

- Az uniós **közös, magas szintű hálózat- és információbiztonságra (NIS)** vonatkozó irányelvjavaslat minél hamarabbi **elfogadása**, amely a nemzeti képességekkel és felkészültséggel, az uniós szintű együttműködéssel, a kockázatkezelési gyakorlatok elterjedésével és a NIS-sel kapcsolatos információk megosztásával foglalkozik.

A Bizottság az alábbiakra kéri az ágazatot:

- Vezető szerep vállalása a magas szintű kiberbiztonságba való **beruházásban** és bevált gyakorlatok, valamint ágazati szintű és a hatóságokkal való információmegosztás kidolgozása abból a célból, hogy biztosítsa az eszközök és egyének hatékony és megbízható védelmét, főleg az állami és a magánszektor partnerségei, például az EP3R és a Digitális élet iránti bizalom (Trust in Digital Life, TDL) révén[18].

A tudatosság javítása

A kiberbiztonságról való gondoskodás közös feladat. A végfelhasználók fontos szerepet játszanak a hálózati és információs rendszerek biztonságának lehetővé tételében: fel kell

[17] CIP-ICT PSP-2012-6, 325188. Teljes költségvetése 15 millió EUR, ebből az uniós finanszírozás 7,7 millió EUR-t tesz ki.

[18] http://www.trustindigitallife.eu/

világosítani őket a rájuk leselkedő internetes veszélyekről, és egyszerű védelmi lépésekre kell őket megtanítani.

Az elmúlt években számos kezdeményezés született, amelyeket érdemes folytatni. A tudatosság növelésében különösen az ENISA vett részt, amikor jelentéseket tett közzé, szakértői műhelytalálkozókat szervezett, valamint az állami és a magánszektor között partnerségeket alakított ki. Az Europol, az Eurojust és a nemzeti adatvédelmi hatóságok szintén aktív szerepet játszanak a tudatosság növelésében. Az ENISA 2012 októberében néhány tagállammal közösen megszervezte az európai kiberbiztonsági hónapot. A kiberbiztonsággal és a számítástechnikai bűnözéssel foglalkozó EU–USA munkacsoportnak[19] egyik kiemelt feladata a tudatosság növelése, és fontos szerepet játszik a (gyermekek internetes védelmére összpontosító) „Biztonságosabb Internet" programban[20] is.

[19] A 2010. novemberi EU–USA csúcstalálkozón létrehozott (MEMO/10/597) munkacsoport feladata együttműködési megközelítések kialakítása számos különböző kiberbiztonsági és számítástechnikai bűnözéssel kapcsolatos kérdésben.

[20] A „Biztonságosabb Internet" program finanszírozza a gyermekek internetes jólétével foglalkozó nem kormányzati szervezetek és a bűnüldöző hatóságok hálózatát, amelyek információkat és bevált gyakorlatokat osztanak meg egymással az internet jogsértő, gyermekek szexuális kizsákmányolásával kapcsolatos anyagok terjesztésére való használatával kapcsolatban, valamint a kutatók hálózatát, akik információkat gyűjtenek az internetes technológiák felhasználásáról, valamint a gyermekekkel kapcsolatos kockázatairól és következményeiről.

A Bizottság az alábbiakra kéri az ENISA-t:

- 2013-ban javasoljon menetrendet a „hálózat- és információbiztonsági jogosítvány” vonatkozásában, amely informatikai szakemberek (például weboldalakért felelős adminisztrátorok) készségeinek és szakértelmének javítására irányuló önkéntes minősítési rendszer.

A Bizottság:

- az ENISA támogatásával 2014-ben kiberbiztonsági **bajnokságot szervez**, amelyen egyetemi hallgatók fognak versenyezni NIS-megoldások megalkotásában.

A Bizottság az alábbiakra kéri a tagállamokat[21]:

- a végfelhasználók tudatosságának növelése érdekében 2013-tól kezdve évente egyszer **kiberbiztonsági hónap** szervezése az ENISA támogatásával és a magánszektor részvételével. 2014-től kezdve EU–USA szinkronizált kiberbiztonsági hónapot kell szervezni.
- **A NIS-sel kapcsolatos oktatásra és képzésre vonatkozó nemzeti erőfeszítések fokozása** az alábbiak bevezetésével: NIS-sel kapcsolatos képzés az iskolákban 2014-től; NIS-sel és biztonságos szoftverfejlesztéssel, valamint személyes adatok védelmével kapcsolatos képzés a számítástechnika szakos diákoknak; és NIS-alapképzés a közigazgatásban dolgozó személyzet számára.

A Bizottság az alábbiakra kéri az ágazatot:

- A kiberbiztonsággal kapcsolatos **tudatosság** ösztönzése **minden területen**, az üzleti gyakorlatban és az ügyfelekkel való kapcsolattartásban egyaránt. Az ágazatnak különösen azt kell átgondolnia, hogy a vezérigazgatókat és az igazgatótanácsokat hogyan tehetik elszámoltathatóvá a kiberbiztonság biztosítása tekintetében.

2.2. A számítástechnikai bűnözés drasztikus csökkentése

Minél digitálisabbá válik a világ, annál több lehetőség nyílik számítástechnikai bűncselekmények elkövetésére. A számítástechnikai bűnözés a leggyorsabban terjedő bűncselekmények közé tartozik, amelynek naponta több mint egymillió ember esik áldozatául. A számítástechnikai bűnelkövetők és hálózataik egyre kifinomultabbá válnak, ezért megfelelő eszközökkel és képességekkel kell felvérteződnünk ellenük. A számítástechnikai bűncselekmények magas profittal és alacsony kockázatokkal járnak, a bűnelkövetők pedig gyakran kihasználják a webhelytartományok anonimitását. A számítástechnikai bűnözés nem ismer határokat – az internet globális elérhetősége miatt a bűnüldöző hatóságoknak összehangolt és együttműködésen alapuló nemzetközi megközelítést kell alkalmazniuk a növekvő fenyegetés ellen.

Szigorú és hatékony jogszabályok

[21] Az érintett nemzeti hatóságok részvételével, ideértve a NIS tekintetében illetékes hatóságokat és az adatvédelmi hatóságokat is.

Az Uniónak és a tagállamoknak szigorú és hatékony jogszabályokra van szükségük a számítástechnikai bűnözés elleni küzdelemhez. Az Európa Tanács számítástechnikai bűnözésről szóló egyezménye, más néven a Budapesti Egyezmény kötelező erejű nemzetközi szerződés, amely hatékony keretet biztosít a nemzeti jogszabályok elfogadásához.

Az Unió már elfogadott néhány jogszabályt a számítástechnikai bűnözéssel kapcsolatban, például a gyermekek online szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló irányelvet[22]. Ezenkívül hamarosan információs rendszerek elleni támadásokkal kapcsolatos irányelvet is elfogad, amely előtérbe helyezi a botnetek alkalmazásának szankcionálását.

A Bizottság:

- biztosítja a számítástechnikai bűnözéssel kapcsolatos irányelvek gyors átültetését és végrehajtását;
- ösztönzi azokat a tagállamokat, amelyek még nem írták alá az **Európa Tanács számítástechnikai bűnözésről szóló Budapesti Egyezményét**, hogy minél hamarabb hagyják jóvá és hajtsák végre rendelkezéseit.

A számítástechnikai bűnözés elleni küzdelmet ösztönző továbbfejlesztett működési képesség

A számítástechnikai bűnelkövetők által alkalmazott módszerek gyorsan fejlődnek: a bűnüldöző hatóságok elavult eszközökkel nem szoríthatják vissza a számítástechnikai bűnözést. Jelenleg nem minden tagállam rendelkezik a számítástechnikai bűnözés elleni hatékony küzdelemhez szükséges eszközökkel. Minden tagállamnak hatékony számítástechnikai bűnözés elleni egységekre van szüksége.

A Bizottság:

- Finanszírozási programjai[23] segítségével támogatja a tagállamokat a **hiányosságaik feltárásában** és a számítástechnikai bűnözés kivizsgálására és leküzdésére irányuló **képességeik megerősítésében**. A Bizottság ezenkívül tovább fogja támogatni azokat a szerveket, amelyek összekapcsolják a kutatás és a tudományos élet képviselőit, a bűnüldöző hatóságokat és a magánszektort, a Bizottság által finanszírozott, néhány tagállamban már létrehozott, számítástechnikai bűnözéssel foglalkozó kiválósági központok által végzett munkához hasonlóan.
- A tagállamokkal együttműködve meghatározza a bevált gyakorlatokat és a legjobb rendelkezésre álló technikákat, ideértve a Közös Kutatóközpont támogatását a számítástechnikai bűnözés elleni küzdelemben (például igazságügyi szakértői eszközök kifejlesztése és használata vagy a kockázatelemzés tekintetében).
- A szakpolitikai megközelítések és a bevált gyakorlatok összehangolása érdekében szorosan együttműködik a nemrég **az Europol keretein belül létrehozott**

[22] A 2004/68/IB tanácsi kerethatározat felváltásáról szóló 2011/93/EU irányelv.

[23] 2013-ban a „Bűnmegelőzés és a bűnözés elleni küzdelem” program (ISEC) alapján. 2013 után pedig a „Belső Biztonsági Alap” alapján (új eszköz a többéves pénzügyi keretben).

Számítástechnikai Bűnözés Elleni Európai Központtal (EC3) és az Eurojusttal.

Hatékonyabb uniós szintű koordináció

Az Unió kiegészítheti a tagállamok munkáját azáltal, hogy összehangolt és együttműködésen alapuló megközelítést mozdít elő, elősegítve a bűnüldöző és az igazságügyi hatóságok, valamint az uniós és az Unión kívüli állami és magánszektorbeli érdekelt felek együttműködését.

A Bizottság:

- Támogatja a közelmúltban létrehozott, **Számítástechnikai Bűnözés Elleni Európai Központot** (EC3), amely a számítástechnikai bűnözés elleni küzdelem európai központja lesz. Az EC3 elemzéseket és hírszerzési tevékenységeket biztosít, támogatja a vizsgálatokat, magas szintű igazságügyi szakértői vizsgálatokat nyújt, elősegíti az együttműködést, információmegosztási csatornákat hoz létre a tagállamok illetékes hatóságai, a magánszektor és más érdekelt felek között, és fokozatosan a bűnüldöző közösség képviselőjévé fogja kinőni magát[24].
- Támogatja a tartományregisztrálók elszámoltathatóságának növelésére és a weboldalak tulajdonosaival kapcsolatos információk pontosságának biztosítására irányuló erőfeszítéseket, főként a Bejegyzett Nevek és Számok Internetszervezete (ICANN) számára megfogalmazott bűnüldözési javaslatok alapján, az uniós jogszabályokkal összhangban, az adatvédelmi szabályokat is ideértve.
- A legújabb jogszabályok alapján lépéseket tesz a gyermekek online szexuális zaklatása ellen tett uniós erőfeszítések további megerősítése céljából. A Bizottság elfogadta a gyermekbarát internet európai stratégiáját[25] és az Unióval és harmadik országokkal együtt létrehozta **a gyermekek online szexuális bántalmazása elleni globális szövetséget**[26]. A szövetség a Bizottság és az EC3 által támogatott további tagállami intézkedések közvetítője.

A Bizottság az alábbiakra kéri az Europolt (EC3):

- Kezdetben a tagállamok számítástechnikai bűnözéssel kapcsolatos nyomozásainak elemzési és operatív támogatására összpontosítson, ezáltal segítve a számítástechnikai bűnözői hálózatok felszámolását és megakadályozását elsősorban a gyermekek szexuális zaklatása, a fizetési csalások, a botnetek és a behatolás területén.
- Rendszeresen készítsen stratégiai és működési jelentéseket a különböző tendenciákról és erősödő fenyegetésekről a prioritások meghatározása és a

[24] Az Európai Bizottság 2012. március 28-án „Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása” címmel közleményt fogadott el.

[25] COM(2012) 196 final.

[26] 2012. június 7-i és 8-i tanácsi következtetések a gyermekek online szexuális bántalmazása elleni globális szövetség létrehozásáról (EU–USA együttes nyilatkozata) és nyilatkozat a gyermekek online szexuális bántalmazása elleni globális szövetség létrehozásáról (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

tagállamok számítástechnikai bűnözéssel foglalkozó csoportjai nyomozati tevékenységének kezelése érdekében.

A Bizottság arra kéri az Európai Rendőrakadémiát (CEPOL), hogy az Europollal együttműködésben:

- koordinálja a tanfolyamok kidolgozását és megtervezését annak érdekében, hogy a bűnüldöző hatóságokat ellássák a számítástechnikai bűnözés elleni hatékony küzdelemhez szükséges tudással és szakértelemmel.

A Bizottság az alábbiakra kéri az Eurojustot:

- A számítástechnikai bűnözéssel kapcsolatos nyomozások során az igazságügyi együttműködés, valamint a tagállamok közötti és harmadik országokkal való együttműködés útjában álló fő akadályok meghatározása, és a számítástechnikai bűnözéssel kapcsolatos nyomozás és büntetőeljárások műveleti és stratégiai szintű támogatása, valamint a kapcsolódó képzések támogatása.

A Bizottság az alábbiakra kéri az Eurojustot és az Europolt (EC3):

- Szoros együttműködés többek között információcsere révén annak érdekében, hogy megbízatásuknak és illetékességüknek megfelelően növeljék a számítástechnikai bűnözés elleni küzdelem terén mutatott hatékonyságukat.

2.3. Kibervédelmi politika és képességek fejlesztése a közös biztonság- és védelempolitika (KBVP) keretében

Az uniós kiberbiztonsági erőfeszítések a kibervédelem dimenzióját is tartalmazzák. A tagállamok védelmi és nemzetbiztonsági érdekeit támogató kommunikációs és információs rendszerek ellenálló képességének növelése érdekében a kibervédelmi képesség fejlesztését a kifinomult számítástechnikai fenyegetések felismerésére, a reagálásra és a javításra kell irányítani.

Mivel ezek a fenyegetések sokfélék lehetnek, fejleszteni kell a kritikus számítástechnikai eszközök védelmére irányuló civil és a katonai módszerek közötti szinergiákat. Ezeket az erőfeszítéseket a kutatás és fejlesztés segítségével, valamint a kormányok, a magánszektor és a tudományos élet képviselői közötti szorosabb együttműködés révén kell támogatni. A felesleges erőfeszítések elkerülése érdekében az Unió megvizsgálja, hogyan tudnák a NATO-val kiegészíteni egymás munkáját azon kritikus kormányzati, védelmi és más információs infrastruktúrák ellenálló képességének növelése érdekében, amelyektől mind a tagállamok, mind a NATO tagjai függnek.

A főképviselő az alábbi alapvető tevékenységekre fog összpontosítani, és felkéri a tagállamokat és az Európai Védelmi Ügynökséget az együttműködésre:

- Az uniós kibervédelmi követelmények értékelése, valamint az Unió kibervédelmi képességei és technológiái fejlesztésének ösztönzése a képességfejlesztés összes szempontjának átfogó kezelése érdekében – ideértve az elméletet, az irányítást, a szervezetet, a személyzetet, a képzést, a technológiát, az infrastruktúrát, a logisztikát és az átjárhatóságot.

- Uniós kibervédelmi szakpolitikai keret kialakítása a KBVP feladatai és műveletei körébe tartozó hálózatok védelme érdekében, ideértve a dinamikus kockázatkezelést, a továbbfejlesztett kockázatelemzést és az információmegosztást. Kibervédelmi képzési és gyakorlati lehetőségek javítása a katonaság számára európai és multinacionális összefüggésben, ideértve a kibervédelmi elemek integrációját a meglévő gyakorlati kínálatba.

- A uniós civil és katonai szereplők közötti párbeszéd és együttműködés ösztönzése – különös hangsúlyt fektetve a bevált gyakorlatok és az információk cseréjére, valamint a korai előrejelzésre, az eseményekre való reagálásra, a kockázatértékelésre, a tudatosság növelésére és a kibervédelem prioritásként való kezelésére.

- Hatékony védelmi képességek biztosítása, együttműködési területek meghatározása és a felesleges erőfeszítések elkerülése érdekében párbeszéd biztosítása nemzetközi partnerekkel, ideértve a NATO-t, más nemzetközi szervezeteket és a multinacionális kiválósági központokat.

2.4. Kiberbiztonsági ipari és technológiai erőforrások kifejlesztése

Európa kiváló kutatási és fejlesztési kapacitásokkal rendelkezik, de az innovatív ikt-termékek és -szolgáltatások terén piacvezető nemzetközi vállalatok az Unión kívül helyezkednek el. Fennáll a veszélye annak, hogy Európa túlságosan függeni fog a máshol előállított információs és kommunikációs technológiáktól, valamint a határain kívül kifejlesztett biztonsági megoldásoktól. Fontos, hogy az Unióban és harmadik országokban előállított, kritikus szolgáltatások és infrastruktúrák esetében és egyre nagyobb mértékben mobil eszközök esetében használt hardver- és szoftverösszetevők megbízhatóak és biztonságosak legyenek, és garantálják a személyes adatok védelmét.

A kibervédelmi termékek egységes piacának előmozdítása

A biztonság szintjének növelése csak akkor lehetséges, ha az értéklánc minden tagja (például a berendezések gyártói, a szoftverfejlesztők, az információs társadalommal kapcsolatos szolgáltatók) prioritásként kezeli a biztonságot. A jelek szerint[27] azonban számos szereplő még mindig tehernek tartja a biztonságot, és alacsony a biztonsági megoldások iránti kereslet. A kiberbiztonsági teljesítményre vonatkozó megfelelő követelményeket kell bevezetni az Európában használt ikt-termékek teljes értéklánca tekintetében. A magánszektornak ösztönzőkre van szüksége a magas szintű kiberbiztonság megvalósítása érdekében; például megfelelő kiberbiztonsági teljesítményt jelző címkék segítségével, hogy a jó kiberbiztonsági teljesítményű és ilyen múlttal rendelkező vállalatok ezt előnyös tulajdonságként tüntethessék fel, és így versenyelőnyre tegyenek szert. A javasolt NIS-irányelvben meghatározott kötelezettségek ezenkívül jelentősen hozzájárulnak az üzleti verseny fokozásához az érintett ágazatokban.

A rendkívül biztonságos termékek iránti európai piaci keresletet is serkenteni kell. A stratégia célja egyrészről az ikt-termékek biztonságával kapcsolatos együttműködés és átláthatóság növelése. Olyan platform létrehozását tűzi ki célul, amely elősegíti az érintett európai állami és magánszektorbeli érdekelt felek együttműködését, annak érdekében, hogy az értéklánc egészében megfelelő kibervédelmi gyakorlatok alakuljanak ki, és létrejöjjenek a biztonságos ikt-termékek kifejlesztéséhez és elfogadásához szükséges kedvező piaci körülmények. Az egyik legfontosabb lépés a megfelelő kockázatkezelés elvégzésének, biztonsági szabványok és megoldások elfogadásának, valamint olyan, lehetőleg önkéntes alapú uniós minősítési rendszerek létrehozásának ösztönzése, amelyek az Unióban és nemzetközi szinten már meglévő rendszerekre épülnek. A Bizottság ösztönözni fogja, hogy a tagállamok koherens megközelítéseket fogadjanak el a földrajzi elhelyezkedés miatti egyenlőtlenségek elkerülése érdekében.

A Bizottság másrészről támogatni fogja a biztonsági szabványok kifejlesztését és közreműködik a számítási felhő területén létrehozott önkéntes minősítési rendszerek fenntartásában, figyelembe véve az adatvédelem biztosításának szükségességét. A feladatok elvégzésének az ellátási lánc biztonságára kell összpontosítania, különösen a kritikus gazdasági ágazatokban (ipari vezérlőrendszerek, energia- és szállítási infrastruktúra). Ennek a munkának az Európai Szabványügyi Szervezetek (Európai Szabványügyi Bizottság, CENELEC, ETSI)[28] és a kiberbiztonsági koordinációs csoport (Cybersecurity Coordination Group, CSCG) tevékenységére, valamint az ENISA, a Bizottság és más érintett szereplők szakértelmére kell épülnie.

A Bizottság:

- a biztonságos ikt-megoldások elfogadására és az Európában használt ikt-termékekre vonatkozó jó kiberbiztonsági teljesítmény elterjedésére irányuló ösztönzők kifejlesztése érdekében 2013-ban **platformot** fog létrehozni a magán- és az állami szektor számára **a NIS-megoldásokról**;
- 2014-ben a platform tevékenysége alapján ajánlásokat fogalmaz meg a kiberbiztonság biztosítására az ikt-értéklánc teljes terjedelmében;

[27] Lásd a hálózat- és információbiztonságról szóló irányelvre vonatkozó bizottsági javaslatot kísérő bizottsági szolgálati munkadokumentum hatásvizsgálatának 4.1.5.2. pontját.

[28] Különösen az intelligens hálózatokra vonatkozó M/490 szabvány értelmében az intelligens hálózatra és referenciaszerkezetre vonatkozó első szabványok.

- megvizsgálja, hogy az ikt-hardverek és -szoftverek fő beszállítói hogyan tájékoztathatnák a nemzeti illetékes hatóságokat a feltárt sebezhetőségekről, amelyek fontos biztonsági kérdéseket vetnek fel.

A Bizottság az alábbiakra kéri az ENISA-t:

- Az érintett nemzeti illetékes hatóságokkal, az érintett érdekelt felekkel, a nemzetközi és európai szabványügyi hatóságokkal és az Európai Bizottság Közös Kutatóközpontjával együttműködve **műszaki iránymutatások és ajánlások** megfogalmazása **a NIS-re vonatkozó szabványok és bevált gyakorlatok elfogadásával kapcsolatban** az állami és magánszektorban.

A Bizottság az alábbiakra kéri az állami és magánszektor érdekelt feleit:

- Az ágazat által kifejlesztett **biztonsági szabványok**, műszaki normák, valamint a beépített biztonsági és a beépített adatvédelmi alapelvek az ikt-termékek gyártói és szolgáltatásnyújtói általi fejlesztésének és elfogadásának ösztönzése; a szoftverek és a hardverek új generációinak ellátása **erősebb, beépített és felhasználóbarát biztonsági funkciókkal**.
- Ágazati szabványok kidolgozása a vállalatok kiberbiztonsági teljesítménye vonatkozásában és a nyilvánosság számára elérhető információk javítása **biztonsági címkék** vagy ún. „sárkányjelek” kialakításával, amelyek segítségével a fogyasztók könnyebben eligazodhatnak a piacon.

A kutatás-fejlesztési célú beruházások és az innováció ösztönzése

A K+F segíthet erős ágazati szakpolitika kialakításában, megbízható európai ikt-ágazat előmozdításában, a belső piac fellendítésében és Európa külföldi technológiáktól való függésének csökkentésében. A K+F segítségével megszüntethetők az ikt biztonsági hiányosságai, fel lehet készülni a biztonsági kihívások következő generációjára, figyelembe lehet venni a felhasználók igényeinek folyamatos fejlődését, és a javunkra lehet fordítani a kettős felhasználású technológiák előnyeit. Továbbra is támogatnia kell ezenkívül a kriptográfia fejlődését. A szükséges ösztönzők biztosítása és a megfelelő szakpolitikai feltételek megteremtése révén elő kell segíteni a K+F eredmények kereskedelmi megoldásokba való átültetését.

Az Uniónak a lehető legtöbbet kell kihoznia a „Horizont 2020”[29] kutatási és innovációs keretprogramból, amely 2014-ben fog elindulni. A bizottsági javaslat a megbízható ikt-vel és a számítástechnikai bűnözés leküzdésével kapcsolatos konkrét célkitűzéseket tartalmaz, amelyek összhangban vannak e stratégiával. A Horizont 2020 támogatni fogja az új ikt technológiákkal kapcsolatos biztonsági kutatásokat; megoldásokat nyújt a „végponttól végpontig” biztonságos ikt-rendszerek, szolgáltatások és alkalmazások számára, ösztönzőket nyújt a meglévő megoldások végrehajtásához és elfogadásához, továbbá választ keres a hálózati és információs rendszerek közötti átjárhatóságra. A különböző finanszírozási programok optimalizálása és megfelelőbb koordinálása uniós szinten különös figyelmet fog

[29] A Horizont 2020 az Innovatív Unió és az Európa 2020 kiemelt kezdeményezés végrehajtására irányuló pénzügyi eszköz, amelynek célja Európa globális versenyképességének biztosítása. Az Unió 2014-től 2020-ig tartó új kutatási és innovációs keretprogramjának célja az Európai növekedés beindítása és új munkahelyek teremtése.

kapni (Horizont 2020, Belső Biztonsági Alap, EVÜ-kutatás, ideértve az európai együttműködési keretet is).

A Bizottság:

- Felhasználja a Horizont 2020-at arra, hogy az ikt adatvédelmi és biztonsági területeivel foglalkozzon, a K+F-től az innovációig és az új technológiák bevezetéséig. A Horizont 2020 keretében ezenkívül különböző eszközök kifejlesztésére is sor fog kerülni a virtuális teret támadó bűnözői és terrorista tevékenységek elleni küzdelemhez.
- Az uniós intézmények és a tagállamok kutatási menetrendjeinek jobb koordinációját elősegítő mechanizmusokat hoz létre és arra ösztönzi a tagállamokat, hogy többet fektessenek be a K+F-be.

A Bizottság az alábbiakra kéri a tagállamokat:

- Az ikt-termékek és -szolgáltatások biztonsági funkciói fejlesztésének és bevezetésének szorgalmazása érdekében 2013 végéig a **közigazgatások vásárlóerejére épülő** legjobb gyakorlatok kifejlesztése (például közbeszerzés révén).
- Az ágazat és a tudományos élet képviselői korai részvételének ösztönzése a megoldások kifejlesztésében és összehangolásában. Erre akkor kerülhet sor, ha Európa ipari bázisából és a kapcsolódó K+F technológiai innovációkból a lehető legtöbbet hozzuk ki, és biztosítjuk a polgári és katonai szervezetek kutatási menetrendje közötti összhangot.

A Bizottság az alábbiakra kéri az Europolt és az ENISA-t:

- Megfelelő digitális igazságügyi szakértői eszközök és technológiák kifejlesztése érdekében új tendenciák és szükségletek azonosítása a számítástechnikai bűnözés és a kiberbiztonsági minták alakulása tekintetében.

A Bizottság az alábbiakra kéri az állami és magánszektor érdekelt feleit:

- A biztosítási ágazattal együttműködve **harmonizált mérőszámok kialakítása a kockázati felárak kiszámításához**, ami a biztonságba befektető vállalatok számára alacsonyabb kockázati felárakat biztosítana.

2.5. Összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása

A nyitott, szabad és biztonságos kibertér fenntartása globális kihívás, amellyel az Uniónak az érintett nemzetközi partnerekkel és szervezetekkel, a magánszektorral és a civil társadalommal együtt kell megbirkóznia.

Az Unió az internet nyitottságát és szabadságát fogja támogatni, viselkedési normák kialakítását fogja ösztönözni, és a meglévő nemzetközi jogszabályokat fogja alkalmazni a kibertérrel kapcsolatos nemzetközi politikájában. Igyekezni fog ezenkívül felszámolni a digitális szakadékot, és aktív szerepet fog vállalni a kiberbiztonsági kapacitás kiépítésére irányuló nemzetközi erőfeszítésekben. Az Unió nemzetközi kötelezettségvállalását a kibertérrel kapcsolatos kérdésekben az Unió alapvető értékei, vagyis az emberi méltóság, a

szabadság, a demokrácia, az egyenlőség, a jogszerűség és az alapvető jogok tiszteletben tartása fogja vezérelni.

A kibertérrel kapcsolatos kérdések beemelése az Unió külkapcsolataiba és a közös kül- és biztonságpolitikába

A Bizottságnak, a főképviselőnek és a tagállamoknak koherens uniós nemzetközi kiberpolitikát kell megfogalmazniuk, amelynek célja a nagyobb kötelezettségvállalás és a legfontosabb nemzetközi partnerekkel és szervezetekkel, valamint a civil társadalommal és a magánszektorral fenntartott kapcsolatok megerősítése. A kiberkérdésekben végzett uniós konzultációkat a nemzetközi partnerekkel úgy kell megtervezni, koordinálni és végrehajtani, hogy fejlesszék a tagállamok és a harmadik országok között folyamatban lévő kétoldalú párbeszédeket. Az Unió nagyobb hangsúlyt fog fektetni a harmadik országokkal folytatott párbeszédre, különös tekintettel a saját értékeit osztó, hasonló gondolkodású partnerekre. Magas szintű adatvédelem elérését fogja ösztönözni, ideértve a személyes adatok harmadik országba való átadását is. A kibertérben tapasztalt globális kihívások elleni küzdelem érdekében az Unió szorosabb együttműködésre fog törekedni az ezen a területen tevékenykedő szervezetekkel, ideértve az Európa Tanácsot, az OECD-t, az ENSZ-t, az EBESZ-t, a NATO-t, az AU-t, az ASEAN-t és az OAS-t. Különösen fontos az Egyesült Államokkal való kétoldalú együttműködés, amelyet főként a kiberbiztonsággal és a számítástechnikai bűnözéssel foglalkozó EU–USA munkacsoporttal összefüggésben továbbra is ápolni fognak.

Az Unió nemzetközi kiberpolitikájának egyik legfontosabb eleme, hogy a virtuális teret a szabadság és az alapvető jogok érvényesülésének helyszínévé igyekszik formálni. Az internethez való hozzáférés folyamatos bővülésének világszerte elő kell segítenie a demokratikus reformot és annak ösztönzését. A fokozottabb globális összeköttetéshez nem szabad cenzúrának vagy tömeges megfigyelésnek társulnia. Az Uniónak ösztönöznie kell a vállalati szociális felelősségvállalást[30], és nemzetközi kezdeményezéseket kell indítania a terület globális összehangolásának javítása érdekében.

A biztonságosabb kibertér elérése a polgároktól a kormányokig a globális információs társadalom minden szereplőjének a felelőssége. Az Unió támogatja a kibertérben tanúsított magatartásra vonatkozó és az összes érdekelt fél által betartandó normák meghatározására irányuló erőfeszítéseket. A polgárokhoz hasonlóan, akiktől az Unió elvárja, hogy az interneten is teljesítsék polgári kötelességeiket, társadalmi felelősségvállalásaikat és betartsák a jogszabályokat, a különböző kormányoknak is követniük kell a normákat és a jogszabályokat. Az átláthatóság növelése és az állam magatartásával kapcsolatos tévhitek kockázatának csökkentése érdekében az Unió a nemzetközi biztonság tekintetében ösztönzi a bizalomépítő intézkedések kifejlesztését a kiberbiztonság területén.

Az Unió nem várja el nemzetközi jogi eszközök létrehozását a kibertérrel kapcsolatos kérdésekben.

A Polgári és Politikai Jogok Nemzetközi Egyezségokmányában, az emberi jogok európai egyezményében és az Európai Unió Alapjogi Chartájában meghatározott jogi kötelezettségeket az internet világában is be kell tartani. Az Unió foglalkozni fog azzal a kérdéssel, hogyan biztosítható ezen intézkedések betartása a kibertérben is.

[30] A vállalati társadalmi felelősségvállalásra vonatkozó megújult uniós stratégia (2011–2014); COM(2011) 681 végleges.

A számítástechnikai bűnözés ellen irányuló Budapesti Egyezményt bármely harmadik ország elfogadhatja. Az egyezmény minta a számítástechnikai bűnözés elleni nemzeti jogszabályok megfogalmazásához, és a területtel kapcsolatos nemzetközi együttműködés alapjául szolgál.

Amennyiben a fegyveres konfliktusok a kibertérre is kiterjednek, az adott helyzetre a nemzetközi humanitárius jog és – megfelelő esetben – az emberi jogok alkalmazandók.

A kiberbiztonsággal kapcsolatos kapacitásépítés és ellenállóképes információs infrastruktúrák fejlesztése harmadik országokban

A fokozottabb nemzetközi együttműködés segíteni fogja a kommunikációs szolgáltatásokat biztosító és előmozdító alapvető infrastruktúrák zökkenőmentes működését. Idetartozik a bevált gyakorlatok megosztása, az információcsere, a korai előrejelzés és a közös incidenskezelési gyakorlatok stb. Az Unió e cél elérése érdekében fokozni fogja a kritikus informatikai infrastruktúrák védelmére (CIIP) létrehozott együttműködési hálózatok megerősítésére irányuló nemzetközi erőfeszítéseket, amelyekben a különböző kormányok és a magánszektor is részt vesz.

A világ nem minden része élvezi az internet előnyeit a nyitott, biztonságos, interoperábilis és megbízható hozzáférés hiánya miatt. Az Európai Unió ezért az internet integritásának és biztonságának biztosítása és a számítástechnikai bűnözés elleni hatékony küzdelem céljából továbbra is támogatni fogja az országokat abban, hogy állampolgáraik számára hozzáférést biztosítsanak az internethez.

A Bizottság és a főképviselő a tagállamokkal együttműködésben az alábbiakat tervezi:

- Összefüggő nemzetközi, a kibertérrel kapcsolatos szakpolitika kidolgozása a fő nemzetközi partnerek és szervezetek bevonása, a számítástechnikai kérdések KKBP-ben való beemelése és a globális kiberbiztonsági kérdések összehangolásának javítása érdekében.
- Viselkedési normák és bizalomépítő intézkedések kialakításának támogatása a kiberbiztonság terén. Párbeszédek ösztönzése azzal kapcsolatban, hogy a meglévő nemzetközi jogszabályokat hogyan lehet a kibertérben alkalmazni, valamint a Budapesti Egyezmény számítástechnikai bűnözés elleni felhasználásának ösztönzése.
- Az alapvető jogok előmozdításának és védelmének támogatása, ideértve az információhoz való hozzáférést és a szólásszabadságot is, különös tekintettel az alábbiakra: a) új, nyilvános iránymutatások kidolgozása az internetes és az interneten kívüli szólásszabadságról; b) az internetes cenzúrához és tömeges megfigyeléshez használható termékek vagy szolgáltatások exportjának nyomon követése; c) az internet-hozzáférés, a nyitottság és az ellenálló képesség növelésére irányuló intézkedések és eszközök kifejlesztése a kommunikációs technológiákkal végzett cenzúra vagy tömeges megfigyelés ellen; d) az érdekelt felek felruházása olyan képességekkel, amelyek segítségével a kommunikációs technológiákat az alapvető jogok előmozdítására használhatják.
- Kötelezettséget vállal a nemzetközi partnerekkel és szervezetekkel, valamint a magánszektorral és a civil társadalommal együtt arra, hogy támogatni fogja a globális kapacitásépítést harmadik országokban az információhoz és a nyitott

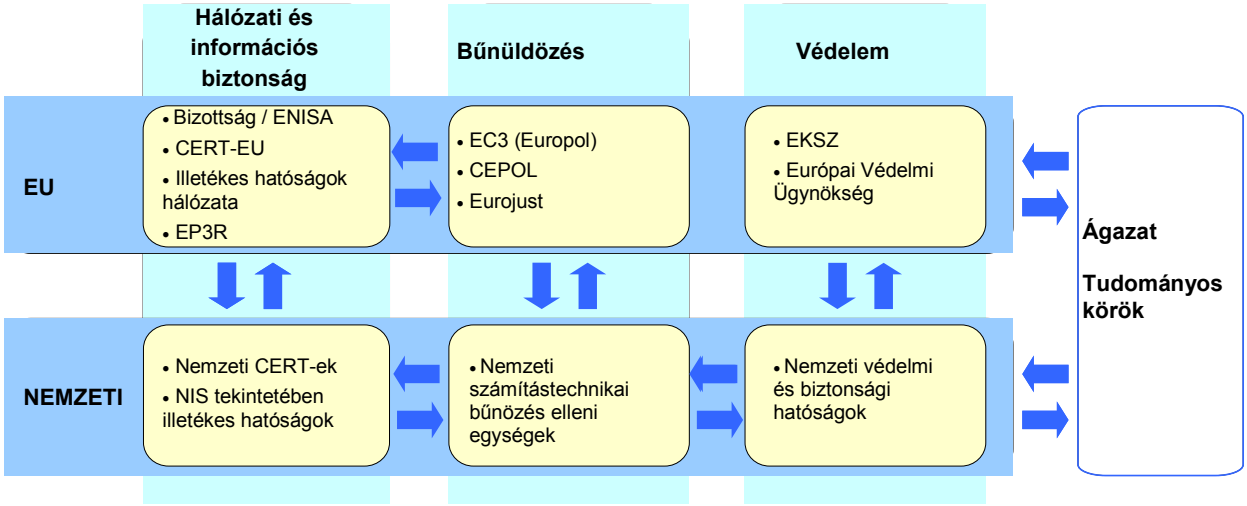
internethez való hozzáférés javítása, valamint a kiberfenyegetések megelőzése és az azok elleni küzdelem érdekében, ideértve a véletlen eseményeket, a számítástechnikai bűnözést és a kiberterrorizmust is, és az adományozók fokozottabb koordinációja érdekében figyelmet fordít a kapacitásépítési törekvések irányítására.

- Különböző európai uniós támogatási eszközök felhasználása a kiberbiztonsági kapacitásépítésre, ideértve a bűnüldöző, igazságügyi és műszaki személyzet képzését a kiberfenyegetések ellen; valamint idevágó nemzeti szakpolitikák, stratégiák és intézmények létrehozása harmadik országokban.
- A szakpolitikai koordináció és az információmegosztás javítása a kritikus informatikai infrastruktúrák nemzetközi védelmi hálózatai, például a Meridian hálózat segítségével, valamint a NIS tekintetében illetékes hatóságok és mások közötti együttműködés segítségével.

3. SZEREPKÖRÖK ÉS FELELŐSSÉGI KÖRÖK

A kiberbiztonsági események nem ismernek országhatárokat az összefonódó digitális gazdaságban és társadalomban. Az összes érintettnek, a NIS tekintetében illetékes hatóságoktól kezdve a hálózatbiztonsági vészhelyzeteket elhárító csoportokon és a bűnüldöző hatóságokon át az ágazatokig, felelősséget kell vállalniuk nemzeti és uniós szinten, és együtt kell működniük a kiberbiztonság megerősítésében. Mivel különböző jogi keretek és joghatóságok kerülhetnek szóba, az egyik legnagyobb kihívás az Unió számára a számos érintett fél szerepköreinek és felelősségi köreinek tisztázása.

A kérdés összetettsége és az érintett felek sokfélesége miatt nincs lehetőség központi európai felügyelet kialakítására. A legjobban a nemzeti kormányok szervezhetik meg a kiberbiztonsági események és kibertámadások megelőzését és az azokra való reagálást, és hozhatnak létre a magánszektorral és a nyilvánossággal közös kapcsolatokat és hálózatokat a különböző szakpolitikai irányzatoknak és jogi kereteknek megfelelően. Ugyanakkor a kockázatok potenciálisan vagy ténylegesen határokat nem ismerő jellege miatt a hatékony nemzeti fellépéshez gyakran az Európai Unió beavatkozására is szükséges lehet. A kiberbiztonság átfogó módon történő kezeléséhez a tevékenységeket három, különböző jogi keretekben működő fő pillérre, a NIS-re, a bűnüldözésre és a védelemre kell építeni:



3.1. A NIS tekintetében illetékes hatóságok / a hálózatbiztonsági vészhelyzeteket elhárító csoportok, a bűnüldöző hatóságok és a védelmi szervek közötti koordináció

Nemzeti szint

A tagállamoknak jelenleg is, vagy akár a stratégia eredményeképpen rendelkezniük kell a számítástechnikai ellenálló képesség, a számítástechnikai bűnözés és a védelem kezelésére alkalmas rendszerekkel; és el kell érniük a kiberbiztonsági események kezeléséhez szükséges képességek megfelelő szintjét. Mivel azonban a különböző érintett szerveknek a kiberbiztonság különböző területein vannak műveleti kötelezettségei, és mert fontos a magánszektor bevonása, a nemzeti szintű koordinációt valamennyi minisztérium vonatkozásában optimalizálni kell. A tagállamoknak nemzeti kiberbiztonsági stratégiájukban meg kell határozniuk a különböző nemzeti hatóságok szerepköreit és felelősségi köreit.

Annak érdekében, hogy a tagállamok és a magánszektor átfogó képet kapjon a különböző fenyegetésekről, és mind a számítástechnikai támadások elkövetésénél, mind az ezekre való gyors reagálás esetében alkalmazott új tendenciákat és technikákat jobban megismerje, ösztönözni kell a nemzeti hatóságok közötti és a magánszektorral folytatott információcserét. Kiberbiztonsági események esetén aktiválandó nemzeti NIS együttműködési tervek létrehozásával a tagállamok egyértelműen kioszthatják a szerepköröket és a felelősségi köröket, és optimalizálhatják az eseményekre való reagálást.

Uniós szint

A nemzeti szinthez hasonlóan uniós szinten is több szereplő foglalkozik a kiberbiztonsággal: az ENISA a NIS tekintetében, az Europol/EC3 a bűnüldözés tekintetében, az EVÜ pedig a védelem tekintetében. A tagállamok képviseltetik magukat ezen ügynökségek és hatóságok igazgatótanácsában, és uniós szintű koordinációs platformokkal rendelkeznek.

Számos olyan területen is ösztönözni kell a koordinációt és az együttműködést az ENISA, az Europol/EC3 és az EVÜ között, amelyben mindhárman érintettek, főleg a tendenciák elemzése, a kockázatelemzés, a képzés és a bevált gyakorlatok megosztása terén. Együttműködésük során azonban meg kell őrizniük sajátosságaikat. Ezen ügynökségeknek és hatóságoknak a CERT-EU-val, a Bizottsággal és a tagállamokkal együtt támogatniuk kell a területen elismert, műszaki és szakpolitikai szakértők közösségének kialakítását.

A koordináció és az együttműködés informális csatornáit strukturáltabb kapcsolatok fogják kiegészíteni. Az Európai Unió Katonai Törzse és az EVÜ kibervédelmi munkacsoportja szolgálhat a védelmi koordináció közvetítőjeként. Az Europol/EC3 programtestülete elő fogja segíteni többek között az Eurojust, a CEPOL, a tagállamok[31], az ENISA és a Bizottság közötti együttműködést, valamint lehetőséget fog biztosítani a különböző „know-how”-k megosztására és arra, hogy az EC3 intézkedéseit az összes érdekelt fél szakértelmének és megbízatásának elismerésével, partnerség keretében hajtsák végre. Az ENISA új megbízatása segítségével várhatóan megerősíti az Europollal és az ágazatbeli érdekelt felekkel ápolt kapcsolatait. A legfontosabb azonban az, hogy a Bizottság jogalkotási javaslata a NIS-ről együttműködési keretet hozzon létre a NIS tekintetében illetékes nemzeti hatóságok hálózata révén, és tegye lehetővé az információcserét a NIS és a bűnüldöző hatóságok között.

[31] Az Európai Unió számítástechnikai bűnözéssel foglalkozó munkacsoportjában képviselve, amely a tagállamok számítástechnikai bűnözés elleni egységeinek vezetőiből áll.

Nemzetközi szint

A Bizottság és a főképviselő a tagállamokkal együtt koordinált nemzetközi fellépést tesz lehetővé a kiberbiztonság területén. A Bizottság és a főképviselő ezáltal az Unió alapértékei szerint jár el, és ösztönzi a kibertechnológiák békés, nyitott és átlátható használatát. A Bizottság, a főképviselő és a tagállamok szakpolitikai párbeszédet folytatnak a nemzetközi partnerekkel és a nemzetközi szervezetekkel, például az Európa Tanáccsal, az OECD-vel, az EBESZ-szel, a NATO-val és az ENSZ-szel.

3.2. Uniós támogatás jelentős számítástechnikai biztonsági esemény vagy támadás esetén

A jelentős számítástechnikai biztonsági események vagy támadások nagy valószínűséggel hatást gyakorolnak az uniós kormányokra, vállalkozásokra és egyénekre. E stratégia, és különösen a NIS-re vonatkozó irányelvjavaslat eredményeképpen a számítástechnikai biztonsági események megelőzése, feltárása és az azokra való reagálás várhatóan javulni fog, és a tagállamoknak és a Bizottságnak alaposabban kell tájékoztatniuk egymást a számítástechnikai biztonsági eseményekről vagy támadásokról. A válaszadási mechanizmusok el fognak térni azonban a biztonsági esemény természete, súlyossága és nemzetközi vonatkozásai függvényében.

Ha az esemény komoly hatást gyakorol az üzleti tevékenységek folyamatosságára, a NIS-irányelv szerint nemzeti vagy uniós együttműködési terveket kell létrehozni az esemény nemzetközi jellegétől függően. A NIS tekintetében illetékes hatóságok hálózatát ebben az esetben információcserére és támogatásra használnák. Ez lehetővé tenné az érintett hálózatok és szolgáltatások megóvását és/vagy helyreállítását.

Ha az esemény a jelek szerint bűncselekményhez kapcsolódik, értesíteni kell az Europol-t / EC3-at, hogy az érintett országok bűnüldöző hatóságaival együtt nyomozást indíthasson, bizonyítékokat gyűjthessen, azonosíthassa a behatolókat, majd gondoskodjon a büntetőjogi felelősségre vonásról.

Ha az esemény vélhetően informatikai kémkedéshez vagy egy másik ország által finanszírozott támadáshoz kapcsolódik, illetve nemzetbiztonsági vonatkozásai vannak, a nemzetbiztonsági és védelmi hatóságok riasztják a megfelelő partnerhatóságokat, hogy azok értesüljenek a támadásról, és megtehessék a megfelelő védelmi intézkedéseket. Ilyen esetben aktiválják a korai figyelmeztető mechanizmusokat, valamint szükség esetén a válságkezelési és egyéb eljárásokat is. Különösen súlyos számítástechnikai biztonsági esemény vagy támadás elegendő alapot adhat a tagállamnak az uniós szolidaritási klauzula alkalmazására (az Európai Unió működéséről szóló szerződés 222. cikke).

Ha az esemény során megsérül a személyes adatok titkossága, a 2002/58/EK irányelv értelmében be kell vonni a nemzeti adatvédelmi hatóságokat vagy a nemzeti szabályozó hatóságot.

Végül pedig a számítástechnikai biztonsági események és támadások könnyebben kezelhetővé válnak a kapcsolati hálózatok és a nemzetközi partnerek támogatása révén. Idetartozhat majd a műszaki enyhítés, a bűnügyi nyomozás vagy a válságkezelési és reagálásra szolgáló mechanizmusok aktiválása.

4. KÖVETKEZTETÉSEK ÉS TOVÁBBI INTÉZKEDÉSEK

Ez a javasolt uniós kiberbiztonsági stratégia, amelyet a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője (főképviselő) terjesztett elő, a polgárok jogainak határozott védelme és előmozdítása alapján felvázolja az Unió jövőképét ezen a területen, és meghatározza a szükséges intézkedéseket annak érdekében, hogy az Unió internetes környezete a világon a legbiztonságosabbá váljon[32].

Ez a jövőkép csak akkor lehet reális, ha nagy számú szereplő valós partnerséget köt, felelősséget vállal és szembenéz a jövő kihívásaival.

A Bizottság és a főképviselő ezért felkéri a Tanácsot és az Európai Parlamentet, hogy támogassák a stratégiát, és segítsenek az előirányzott intézkedések végrehajtásában. A magánszektor és a civil társadalom kötelezettségvállalására is szükség van, mivel fontos szerepet játszanak a biztonság szintjének növelésében és a polgárok jogainak védelmében.

Eljött a cselekvés ideje. A Bizottság és a főképviselő határozott szándéka, hogy a szükséges biztonság megvalósításában együtt fognak működni valamennyi szereplővel. A stratégia mielőbbi végrehajtásának biztosítására és a lehetséges fejlemények tükrében történő értékelése érdekében magas szintű konferenciát kívánnak rendezni az összes érdekelt részvételével, és egy év elteltével értékelni fogják az előrehaladást.

[32] A stratégia finanszírozását a 2014–2020-as többéves pénzügyi keretre (amelyet a költségvetési hatóságnak jóvá kell hagynia, és amely a 2014–2020-as többéves pénzügyi keret jóváhagyott végleges összegeitől függ) vonatkozó bizottsági javaslatban az érintett szakpolitikai területek (Európai Hálózatfinanszírozási Eszköz, Horizont 2020, Belső Biztonsági Alap, KKBP, nemzetközi együttműködés, főképp a Stabilitási Eszköz) esetében előirányzott összegek fogják fedezni. Mivel szükséges az általános kompatibilitás biztosítása a decentralizált ügynökségek számára rendelkezésre álló álláshelyek és a decentralizált ügynökségek tekintetében a következő többéves pénzügyi keretben meghatározott részleges felső határ között, erre ösztönzik majd azokat az ügynökségeket (CEPOL, EVÜ, ENISA, EUROJUST és EUROPOL/EC3), amelyeket e közleményben új feladatokkal bíztak meg, amennyiben meghatározásra került az ügynökség tényleges kapacitása a növekvő erőforrások befogadására, és azonosították az átcsoportosítás minden lehetőségét.