Az Európai Gazdasági és Szociális Bizottság véleménye – Közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája

(saját kezdeményezésű vélemény)

(2023/C 293/04)

Előadó: **Anastasis YIAPANIS**

Társelőadó: **Alberto MAZZOLA**

Közgyűlési határozat:	2022.9.20.
Jogalap:	eljárási szabályzat 52. cikk (2) bekezdés
	saját kezdeményezésű vélemény
Illetékes szekció:	Ipari Szerkezetváltás Konzultatív Bizottsága (CCMI)
Elfogadás a szekcióülésen:	2023.3.27.
Elfogadás a plenáris ülésen:	2023.6.14.
Plenáris ülésszak száma:	579.
A szavazás eredménye:	
(mellette/ellene/tartózkodott)	208/1/2

1. **Következtetések és ajánlások**

1.1. Az Európai Gazdasági és Szociális Bizottság (EGSZB) támogatja a javasolt uniós kibervédelmi politikát, de azt várta volna, hogy a szervezett civil társadalom jelentősebb szerepet kapjon e javaslatok kidolgozásában. Az EGSZB jelenleg nehéznek tartja annak értékelését, hogy a közös közleményben felvázolt jövőbeli kezdeményezések megvalósulnak-e, és elérik-e a kívánt eredményeket, és sürgeti az uniós intézményeket és a tagállamokat, hogy kezeljék prioritásként és mielőbb mozdítsák elő a bejelentett kezdeményezéseket.

1.2. Az EGSZB hangsúlyozza, hogy további intézkedésekre van szükség az EU kiberfenyegetések felderítésére való képességének javítása érdekében, és kéri, hogy a K+F-finanszírozást irányítsák az élvonalbeli uniós képességek fejlesztésére. A magán- és a közszféra közötti együttműködés alapvető fontosságú, és nem lehet egyirányú. Az EGSZB úgy véli, hogy uniós koordinációra van szükség a széttagoltság kezelése, valamint a tagállamok közötti együttműködés és közös beruházások biztosítása érdekében.

1.3. Az EGSZB támogatja az EU Kibervédelmi Koordinációs Központjának létrehozását, és azt ajánlja, hogy a tagállamok kötelezzék el magukat a hét minden napján, napi 24 órában megvalósuló, gyors reagálás mellett, értékeljék az uniós kiberválság-reagálási mechanizmusok kiberkészültségét és teljesítményét, az (EU) 2022/2555 európai parlamenti és tanácsi irányelvben ([1]) (NIS2 irányelv) meghatározott katonai képességekre és kritikus ágazatokra egyaránt összpontosítva. Az EGSZB támogatja az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) megbízatásának kiterjesztését az uniós Kibervédelmi Koordinációs Központ munkájának támogatására.

1.4. Az EGSZB úgy véli, hogy az Unió kiberbiztonsági stratégiai autonómiájának és szuverenitásának fokozása érdekében dinamikus, valós idejű tesztelési és információmegosztási platformot kell kifejleszteni vagy átvenni a magánszektorból a meglévő képességek jelenlegi hiányosságainak azonosítására. Ezt a platformot fel lehetne használni a bevált gyakorlatok megosztására, a kiberbiztonsági események bejelentésére, valamint a kiberbűnözők uniós jegyzékének összeállítására is.

([1]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)(HL L 333., 2022.12.27., 80. o.).

1.5. Az EGSZB hangsúlyozza, hogy jobban fel kell készülni a főleg a kritikus infrastruktúrákat célzó kibertámadásokra (amelyeket például Oroszország követ el Ukrajna ellen). A polgári és katonai ökoszisztémák közötti együttműködés elengedhetetlen a hatékony válságkezeléshez, az interoperabilitáshoz, valamint a párhuzamos erőfeszítések és beruházások elkerüléséhez, többek között szimulált számítógépes támadások révén.

1.6. Az EGSZB úgy véli, hogy a kibervédelembe történő beruházásoknak az uniós polgárok és a kritikus infrastruktúrák védelmét kell előtérbe helyezniük, amihez hozzátartozik a megbízható hardver- és szoftverbeszállítók használata is. A prioritásokat és a beruházásokat a tagállamokkal és az EU-val egyetértésben, megfelelő időközönként frissíteni kell, a magánszféra érdekelt feleinek bevonásával.

1.7. Az EU-nak meg kell őriznie és fejlesztenie kell azokat a kapacitásokat, amelyek digitális gazdaságának, társadalmának, demokráciájának és kritikus technológiáinak biztosításához, valamint a kulcsfontosságú kiberbiztonsági szolgáltatások nyújtásához szükségesek. Az EU stratégiai autonómiájának biztosításához elengedhetetlen a harmadik országoktól való függőség csökkentése. Az EGSZB elengedhetetlennek tartja, hogy az EU elfogadjon valamilyen középtávú megközelítést a kulcsfontosságú technológiák autonómiája tekintetében, és határozottan kiáll amellett, hogy uniós székhelyű vállalatok hozzanak létre kutatási és termelési létesítményeket, és hogy legyen egy autonóm kiber-ökoszisztémára összpontosító, megfelelő európai iparpolitika.

1.8. A kkv-knak célzott támogatást kell kapniuk, és hozzáférést kell biztosítani számukra olyan finanszírozási programokhoz, amelyek növelik ellenálló képességüket a kibertámadásokkal szemben, valamint segítséget, képzést és oktatási lehetőségeket kell nyújtani nekik a kiberkockázatokkal és az azok ellen való védekezéssel kapcsolatban. Az EU-nak olyan ösztönző mechanizmust kell biztosítania, amely elősegíti, hogy a kkv-k fokozatosan megismerkedjenek az előbb említettekkel, és amely elősegíti az innovatív kkv-k fejlesztését.

1.9. Az EGSZB támogatja a Kiberkészségek Akadémiája létrehozásának tervét, és arra kéri az Európai Bizottságot, hogy koordináljon és finanszírozzon nagyszabású képzési és szakképzési programokat minden tagállam bevonásával, hogy a kibervédelemben érintett valamennyi ügynökség és szervezet, valamint a civil magánhálózatok számára képzett munkaerő álljon rendelkezésre.

1.10. Az EGSZB szerint a polgárok kiberbiztonsággal kapcsolatos tudatosságának növelése alapvető fontosságú a kibertámadásoknak való kitettség csökkentéséhez, és olyan kiberbiztonsági oktatási tanterveket és egész életen át tartó képzési programokat szorgalmaz, amelyek a kiberkészségek és -ismeretek fejlesztésére összpontosítanak. Az EGSZB támogatja, hogy a kiberbiztonságot valamennyi jövőbeli uniós közpolitikában általánosan érvényesítsék, és hogy tájékoztassák a nagyközönséget a kiberfenyegetésekről.

1.11. Az EGSZB úgy véli, hogy a NATO szövetségeseivel a katonai területeken folytatott szoros együttműködésnek teljeskörű koordinációra és viszonosságra, közös K+F+I projektekre, a bevált gyakorlatok megosztására, nagyszabású képzési programokra és a kibertámadások szimulációjára kell összpontosítania, azzal a fő céllal, hogy bővítsék a közös reagálási képességet.

1.12. Az EGSZB arra kéri a főképviselőt, hogy vizsgálja meg a jelenlegi kétoldalú kiberpárbeszédeket, és kezdjen további megbeszéléseket más országokkal és az érintett nemzetközi szervezetekkel annak érdekében, hogy létre lehessen hozni egy globális keretet a nemzetközi jognak a kibertérben való betartásához, különös hangsúlyt fektetve a viszonosságra. Az EGSZB úgy véli, hogy az EU alkalmas arra, hogy vezető szerepet vállaljon a kiberbiztonság jövőjéről szóló nemzetközi vitákban, különösen az ENSZ-en belül, mivel az EU-ban szilárd alapjai vannak az alapvető demokratikus szabadságoknak.

1.13. Az EU-nak határozott álláspontot kell képviselnie a polgárokkal szembeni bármilyen szociális pontozási rendszerrel szemben. Az EGSZB szeretné világossá tenni, hogy valódi demokrácia nem létezhet a személyes adatok hatékony védelme nélkül, és úgy véli, hogy a felelősségteljes és hatékony adatkezelés elengedhetetlen ahhoz, hogy a hiperkonnektivitás versenyelőnnyé váljon.

2. **Bevezetés és általános megjegyzések**

2.1. A társadalmak digitális bővülése számos kiberbiztonsági fenyegetéssel jár, amelyeket a technológiai fejlesztések idéznek elő. Az elmúlt néhány évben jelentősen nőtt a kibertámadások száma és kifinomultsága, aláásva mind az állami, mind a magánszervezetek biztonságát. Függetlenül attól, hogy zsarolóvírusokról, rosszindulatú szoftverekről, e-mail-támadásokról, adatsértésekről, dezinformációról, elosztott szolgáltatásmegtagadási támadásokról vagy más típusú támadásokról beszélünk, ezek mind következetes és folyamatos fenyegetést jelentenek az EU egészének biztonságára nézve.

2.2. Az EGSZB üdvözli *az uniós kibervédelmi politikáról szóló közös közleményt* ([2]), és úgy véli, hogy most kell cselekedni, a lehető leghamarabb és uniós szinten összehangoltan, bevonva mind a polgári, mind a katonai kibertér-ökoszisztémákat, és megfelelő beruházási keretet biztosítva a kibervédelmi képességek számára. Az EGSZB azonban megjegyzi, hogy a közlemény csupán a cselekvés iránti elkötelezettséget és a megvalósítandó jövőbeli uniós kezdeményezések listáját tartalmazza, és lehetetlennek tartja annak értékelését, hogy a jövőbeli kötelezettségvállalások ténylegesen megvalósulnak-e, mivel a társjogalkotók közötti jövőbeli tárgyalások természetesen befolyásolják majd az uniós kiberbiztonsági cselekvési terv végeredményét.

2.3. A KA-SAT műholdas hálózat elleni orosz támadás, amely megzavarta az ukrán katonai erők közötti kommunikációt, valamint a közelmúltbeli botrány, amelynek során egyes védelmi vállalatok Éric Léandrit a nevükben kiberkémkedésre szerződtették, jól mutatják, hogy a kiberbiztonság első helyen szerepel a biztonsági fenyegetések között az EU-ban. Bár az általános adatvédelmi rendelet szilárd uniós jogszabály, és már több éve hatályban van, egyértelmű, hogy a rendelkezésre álló adatok növekvő mennyisége sérülékeny, és napról napra nő annak a kockázata, hogy harmadik felek átlépik a jogszerűség határát.

2.4. Tekintettel a kibertámadások határokon átnyúló jellegére, uniós koordinációra van szükség a jelenlegi széttagoltság csökkentése és annak biztosítása érdekében, hogy a tagállamok készen álljanak a közös együttműködésre és beruházásokra. Ez különösen fontos olyan jövőbeli esetekben, amikor egyetlen tagállamot ér támadás, az összes többinek pedig lehetőséget kell kapnia, hogy azonnali támogatást nyújtson.

3. **Együttes fellépés az erősebb kibervédelem érdekében**

3.1. Az EGSZB tudomásul veszi a bejelentett ambiciózus kezdeményezéseket, amelyek létrehozzák az EU Kibervédelmi Koordinációs Központját, kidolgozzák a CyDEf-X projektet, életre hívják a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportokat, kidolgozzák az uniós kiberbiztonsági szolidaritási kezdeményezést, valamint felmérik az IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó kiberbiztonsági tanúsítási rendszerek kidolgozását. Az EGSZB azt ajánlja, hogy valamennyi tagállam álljon készen a gyors reagálásra a hét minden napján, napi 24 órában, az uniós koordinációs központ pedig vegyen részt a tagállamok kiberbiztonsági felkészültségéről és az európai kiberválság-reagálási mechanizmus hatékonyságáról szóló rendszeres jelentések értékelésében és kidolgozásában, mind a katonai képességekre, mind pedig a NIS 2 irányelvben meghatározott kritikus ágazatokra összpontosítva. Minden tagállamnak rendelkeznie kell a kiberbiztonsági események esetén történő beavatkozásra kiképzett szakemberekkel, és rendszeresen tesztelnie kell a más tagállamokban való beavatkozási képességüket.

3.2. Bár a közlemény a fokozatos javítások hosszú listáját tartalmazza, az EGSZB szerint jó lett volna konkrét ütemtervet kidolgozni e kezdeményezések végrehajtására, a hatáskörök egyértelmű elkülönítésével, valamint benyújtási és elfogadási határidők megjelölésével. Az EGSZB szerint a szervezett civil társadalomnak jelentősebb szerepet kellett volna kapnia e javaslatok kidolgozásában.

3.3. Az EGSZB szerint a tagállamoknak meg kell erősíteniük belső képességeiket a kiberfenyegetésekkel szembeni fellépéshez, ugyanakkor együttműködési projekteket kell folytatniuk, és meg kell osztaniuk az információkat és a bevált gyakorlatokat a többi tagállambeli partnereikkel. Valamennyi tagállamban a technológia gyorsított bevezetésére ([3]) és mielőbbi beruházásokra van szükség a kibervédelmi képességekbe, valamint a kibertámadások észlelésére, az ellenük való védekezésre és az okozott károk helyreállítására irányuló közös felkészültségbe. Az EGSZB úgy véli, hogy az Unió kiberbiztonsági autonómiájának támogatása érdekében dinamikus, valós idejű tesztelési és információmegosztási platformot kell kifejleszteni vagy a magánszektorból átvenni, amely a jelenleg hiányzó képességek azonosítására összpontosít.

3.4. Az EGSZB osztja azt a nézetet, hogy ebben a szakaszban a katonai kibertéri műveleteknek szigorúan a tagállamok hatáskörében kell maradniuk; az EGSZB támogatja az uniós katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok (milCERT), a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) és az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja (CERT-EU) között bejelentett együttműködést.

3.5. A közelmúltban elfogadott NIS 2 irányelv és a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv ([4]) már konkrét nemzeti és ágazati kötelezettségeket vezetett be az uniós kibervédelmi keretre vonatkozóan. További intézkedésekre van szükség az EU kollektív észlelési kapacitásának javítása érdekében, és az EGSZB kutatási és fejlesztési beruházásokat szorgalmaz az élvonalbeli uniós képességek fejlesztése érdekében.

([2]) A Bizottság közleménye az EU kibervédelmi politikájáról.
([3]) Például a NATO-nak az Atlanti-óceán északi részére vonatkozó védelmi innovációs akcelerátora (DIANA).
([4]) CER-irányelv.

4. **Az uniós védelmi ökoszisztéma biztonságának garantálása**

4.1. Az EGSZB úgy véli, hogy a vele együtt járó bonyolultság és a gyorsan változó technológiai kihívások átalakították a védelmi ökoszisztémát, és hogy a kiberbiztonság a katonai és a polgári szektor, valamint az uniós polgárok közös ügyévé vált. A polgári és katonai ökoszisztémák közötti együttműködés ma minden eddiginél fontosabb, és előnyökkel jár a hatékonyabb válságkezelés, valamint a folyamatos előrehaladás és az interoperabilitás tekintetében, elkerülve az átfedéseket vagy ugyanazon erőfeszítések és beruházások megsokszorozódását. A tagállamoknak készen kell állniuk arra, hogy a nemzeti kritikus infrastruktúrákat stressztesztnek vessék alá a jövőbeli kibertámadásokkal szembeni ellenálló képesség értékelésére és növelésére.

4.2. Az EGSZB úgy véli, hogy a kibervédelmi beruházásoknak elsősorban az uniós polgárok és a kritikus infrastruktúrák védelmére kell irányulniuk. Tekintettel a digitális átalakulás gyors ütemére és a fenyegetettségi környezet gyors fejlődésére, az EGSZB határozottan sürgeti, hogy az EU és a tagállamok rendszeresen aktualizálják a prioritásokat és a beruházásokat, az érintett magánszereplőkkel történő alapos konzultáció mellett. A tárgyak internetének (IoT) eszközei gyakran nem részesülnek olyan jó védelemben, mint a hagyományos eszközök, ezért az EGSZB az IDAM-platformokon keresztül egy minimális biztonsági szint biztosítását kéri. Mivel a tanúsítás kulcsfontosságú módszer a magasabb szintű biztonság biztosításához, az EGSZB kéri, hogy az új uniós tanúsítási megközelítés helyezzen nagyobb hangsúlyt a tárgyak internetének biztonságára.

4.3. Az EU-nak ellenállóvá kell válnia a kibertámadásokkal szemben, és hatékony kiberelrettentést kell létrehoznia. A kritikus infrastruktúrát védeni kell mindenfajta kibertámadással szemben, és ebben az uniós védelmi rendszereknek is részt kell vállalniuk. Az EGSZB szerint az EU stratégiai érdeke biztosítani, hogy az Unió megőrizze és fejlessze képességeit digitális gazdaságának, társadalmának és demokráciájának biztonságossá tételéhez, és hogy elérje a teljes digitális szuverenitást, mivel ez az egyetlen módja annak, hogy megvédjük a kritikus technológiákat és hatékony kiberbiztonsági szolgáltatásokat nyújtsunk. A harmadik országoktól való függőség csökkentése az EU stratégiai autonómiája szempontjából is létfontosságú. Az EGSZB úgy véli, hogy az ágazati uniós ügynökségeknek (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA, stb.) részt kell venniük a folyamatban, és iránymutatást kell nyújtaniuk a kiberbiztonsági rendszerek kidolgozásában.

4.4. A Covid19-világjárvány felgyorsította a digitális átállást, és a hagyományos munkavégzést hibriddé és/vagy távolivá alakította át, ami új munkakapcsolatokat és elvárásokat teremtett, valamint a digitális nomádok új, egyre bővülő osztályát eredményezte. Az EGSZB tudomásul veszi a munkaerőpiac gyors változásait, amelyek folyományaként a vállalatok „zéró bizalmi" architektúrára tértek át az olyan megoldások révén, mint a személyazonosság-kezelő és hozzáférés-kezelő rendszer (IAM) és az emelt szintű hozzáférés kezelés (PAM). Az EGSZB szerint a vállalatok ilyen típusú erőforrás-gazdálkodása új megoldásokat nyújt a kiberfenyegetésekkel kapcsolatban, és a magánszektort támogatni kell innovatív digitális megoldásaik biztonsági szintjének megerősítésében.

4.5. Az EGSZB kissé csalódott az Európai Bizottság azon kijelentésével kapcsolatban, miszerint „a tagállamokkal együttműködve végrehajtási tervet lehetne kidolgozni", és úgy véli, hogy egy ilyen végrehajtási tervnek inkább kötelezőnek kellene lennie. Ezt a tagállamokkal közösen kellene kidolgozni, és a lehető leghamarabb végrehajtani. Az EGSZB aggódik az Európai Bizottság e könnyed hozzáállása miatt, és sürgeti az uniós intézményeket és a tagállamokat, hogy segítsék elő a bejelentett kezdeményezések gyors előrehaladását.

5. **Beruházás a kibervédelmi képességekbe**

5.1. A technológiai fejlődés gyors előrehaladtával a kibertér a hadviselés legújabb harcterévé vált a szárazföld, a tenger, a levegő és a világűr után. Emellett hatalmas bűnügyi lehetőségeket teremtett a rosszindulatú kiberszereplők számára, a független hackerektől a hivatásos bűnözőkig, sőt akár az állami szereplőkig.

5.2. A K+F-be való beruházás létfontosságú, és az EGSZB üdvözli a Digitális Európa program, az Európai Védelmi Alap, a Horizont Európa és a nemzeti helyreállítási programok keretében a már e célra elkülönített alapokat. Az EGSZB szerint viszont több transznacionális projektre van szükség, amelyek valamennyi tagállamban a kibervédelmi rendszerek közötti együttműködésre és interoperabilitásra, valamint a – főleg az innovatív kkv-kat célzó – finanszírozási eszközök közötti szinergiák növelésére összpontosítanak.

5.3. Az EGSZB megjegyzi, hogy 2020-ban az uniós kiberbiztonsági stratégia 2023-at jelölte meg a közös kiberbiztonsági egység létrehozásának határidejeként, így az EGSZB várja a híreket e folyamat véglegesítéséről, illetve arról hogy hogyan alakul az EU felkészültsége a nagyszabású kiberbiztonsági eseményekre való reagálásra. Az EGSZB arra számít, hogy ennek az egységnek köszönhetően javul majd az EU helyzetismerete, valamint általános reagálási és helyreállítási képessége.

5.4. Az EGSZB egyetért azzal, hogy az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) megbízatását kiterjesszék az uniós Kibervédelmi Koordinációs Központ tevékenységének támogatására. Emellett ez a hálózat támogathatná Európa digitális szuverenitását azáltal, hogy versenyképes európai ipari bázist hoz létre a kulcsfontosságú technológiai képességek számára, részben a köz- és magánszféra közötti szerződéses partnerségek (PPP) munkájára alapozva. A köz- és magánszféra közötti partnerségek bizonyultak a leghatékonyabb megközelítésnek a teljes digitális ökoszisztéma kiberbiztonságának javítására, de ez nem lehet egyirányú: az állami intézményeknek is meg kell osztaniuk információikat a magánszektorral.

5.5. Az EGSZB megjegyzi, hogy a kvantumszámítógépek jövőbeli feltörési kísérleteinek kezelése érdekében az EU-nak haladéktalanul be kell ruháznia az olyan élvonalbeli technológiákba, mint a posztkvantumkriptográfia. Úgy véli, hogy Európa számára elengedhetetlen valamilyen középtávú megközelítés az autonómia kapcsán, és határozottan kiáll amellett, hogy uniós székhelyű vállalatok fejlesszenek ki kutatási és termelési létesítményeket. Az EGSZB fontosnak tartja a digitális K+I-re szánt uniós források növelését, valamint az üzemeltetők és a szolgáltatók új műszaki biztonsági funkciókba történő beruházásainak támogatását, amelyek olyan új trendekhez is kapcsolódnak, mint a kiterjesztett valóság és a metaverzum. Különösen fontos egy olyan európai megosztott felhőalapú infrastruktúra kiépítése, amely az adattárolással és -feldolgozással kapcsolatos európai szabályokon alapul ([3]).

5.6. Különös figyelmet kell fordítani a kkv-kra, és hozzáférést kell biztosítani számukra olyan finanszírozási programokhoz, amelyek fokozzák a kibertámadásokkal szembeni felkészültségüket, valamint olyan támogatási, képzési és oktatási programokhoz, amelyek segítenek nekik megérteni a kiberkockázatokat és megvédeni magukat. Az EU-nak olyan ösztönző mechanizmust kell biztosítania, amely elősegíti, hogy a kkv-k fokozatosan megismerkedjenek az előbb említettekkel.

5.7. Az Európai Bizottság becslése szerint a kiberbiztonság terén meglévő készséghiány félmillió emberre tehető, és az EGSZB nagyra értékeli a Kiberkészségek Akadémiájának létrehozására irányuló javaslatot. Egyértelmű, hogy a tagállami szintű erőfeszítések nem elegendőek a készséghiány csökkentéséhez, ezért az EGSZB azt javasolja, hogy az Európai Bizottság az Akadémia elindításával együtt, kihasználva a készségek európai éve által kínált lendületet, uniós szinten valamennyi tagállam bevonásával koordináljon és finanszírozzon nagyszabású képzési és szakképzési programokat, amelyekkel képzett munkaerőt lehet biztosítani a kibervédelemben részt vevő valamennyi ügynökség és szerv, valamint a polgári magánhálózatok számára. Különös hangsúlyt kell fektetni a munkaerő képzésére, különösen a természettudományok, a technológia, a műszaki tudományok és a matematika (STEM) területén.

5.8. Az EGSZB úgy véli továbbá, hogy a kibertámadásoknak való kitettség csökkentése érdekében létfontosságú felhívni a polgárok figyelmét a kiberbiztonságra, különös tekintettel a lakosságot célzó egyszerűbb kiberbűncselekményekre. Az EGSZB olyan kiberbiztonsági oktatási tanterveket és egész életen át tartó kiberbiztonsági képzési programokat szorgalmaz, amelyek a kiberkészségek fejlesztésére, valamint a kiberbiztonság ismertebbé és vonzóbbá tételére összpontosítanak a polgárok, különösen a fiatalabb generáció számára. Az EGSZB támogatja, hogy a kiberbiztonsági megfontolásokat valamennyi jövőbeli uniós közpolitikában általánosan érvényesítsék, és hogy tájékoztassák a nagyközönséget a kiberfenyegetésekről, többek között a lakosság számára szervezett ingyenes képzési programok, ingyenes mobiltelefonos információs alkalmazások vagy főműsoridőben történő televíziós kommunikáció révén. Ezekkel az intézkedésekkel párhuzamosan elő kell mozdítani, hogy a „kiberbiztonság-orientált” megközelítés széles körben elterjedjen a társadalomban.

5.9. Az EGSZB úgy véli, hogy alapvető fontosságú a beszállítók kockázati profiljának értékelése és a magas kockázatúnak tekintett beszállítókra vonatkozó korlátozások alkalmazása, beleértve az összehangolt uniós kockázatértékelésben kritikusként és érzékenyként meghatározott, kulcsfontosságú eszközök és alkalmazások szükséges betiltását, valamint a megbízható hardver- és szoftverszolgáltatók tanúsítását.

6. **Összefogás a közös kihívások kezelése érdekében**

6.1. A jövőbeli kibertámadásokra való felkészültség szintje tagállamonként rendkívül eltérő. Az EGSZB szerint azonnal létre kell hozni egy uniós kommunikációs platformot a bevált gyakorlatok megosztására, ahol a kibertér legfejlettebb tagállamai megoszthatják ismereteiket más tagállamokkal, így azokat a többi ország azonnal át tudja venni. Ez hozzájárulna a nemzeti szervezetek közötti kölcsönös bizalom javításához. Másodszor, az EGSZB úgy véli, hogy EU-szerte szorosabb együttműködésre van szükség az állami és a nem állami szereplők között annak érdekében, hogy a belső piacon javuljon a termékek és szolgáltatások kiberbiztonsága. Az EGSZB közös uniós platform létrehozását javasolja a kiberbiztonsági események bejelentésére, beleértve a kiberbűnöző aktivisták feketelistáját is.

([3]) Például Gaia-X, a francia-német kezdeményezés.

6.2. Az EGSZB úgy véli, hogy a NATO-szövetségeseinkkel a katonai területen folytatott szoros együttműködésnek nemcsak a kapacitásépítésre és a korai felismerésre kell összpontosítania, hanem közös K+F+I projektekre, a bevált gyakorlatok megosztására és szakértők közötti cseréjére, nagyszabású képzési programokra és a kibertámadások szimulációjára is. A 2016. évi varsói és 2018. évi brüsszeli együttes nyilatkozatok értelmében a fő cél a közös reagálási kapacitás bővítése és szinergiák létrehozása a jövőbeli hibrid fenyegetésekkel szembeni fellépés érdekében. Az EU és a NATO közötti együttműködésnek még mindig számos kiaknázatlan lehetősége van, és az azonnali előrelépés valódi változást hozhat polgáraink és társadalmaink biztonságának szavatolása terén.

6.3. Az EGSZB úgy véli, hogy a globális szinten és nemzetközi partnereinkkel folytatott megbeszéléseknek meg kell teremteniük a terepet egy olyan globális és nyitott kibertér előmozdításához, amely védi az emberi jogokat, az alapvető szabadságokat és a jogállamiságot, és a gyors digitális fejlődésű ágazatokban kötelező erejű nemzetközi normák kidolgozására összpontosít. Az EGSZB azt tanácsolja a főképviselőnek, hogy vizsgálja felül a meglévő kétoldalú kiberpárbeszédeket, és kezdjen további tárgyalásokat más országokkal és az érintett nemzetközi szervezetekkel annak érdekében, hogy előmozdítsa a nemzetközi jog kibertérben való alkalmazásának globális keretét, amely szigorú viszonossági feltételen alapul.

6.4. Végezetül az EGSZB úgy véli, hogy az EU van a legjobb helyzetben ahhoz, hogy vezető szerepet töltsön be a kiberbiztonság jövőjéről szóló nemzetközi, különösen az ENSZ keretében folytatott vitákban, mivel az EU-ban szilárd alapjai vannak az alapvető demokratikus szabadságoknak. Az EU-nak emellett küzdenie kell azon totalitárius rendszerek ellen, amelyek a polgárok adatainak nyomon követését végzik, és megsértik jogaikat és szabadságaikat, és határozottan fel kell lépnie a polgárokkal szembeni bármilyen társadalmi pontozási rendszer ellen. Az EGSZB egyértelműen kijelenti, hogy valódi demokrácia nem létezhet a személyes adatok hatékony védelme nélkül, és úgy véli, hogy a felelősségteljes és hatékony adatkezelés létfontosságú ahhoz, hogy a hiperkonnektivitás igazán hasznos eszközzé váljon.

Kelt Brüsszelben, 2023. június 14-én.

az Európai Gazdasági és Szociális Bizottság
elnöke
Oliver RÖPKE