Az Európai Unió
Tanácsa

Brüsszel, 2022. október 17.
(OR. en)

13664/22

CYBER 327
TELECOM 410
COSI 247
COPEN 354
DATAPROTECT 280
IND 413
RECH 547
HYBRID 99
JAI 1326
POLMIL 225
RELEX 1357

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2022. október 17.
Címzett:	a delegációk
Előző dok. sz.:	12930/22
Tárgy:	A Tanács következtetései az IKT-ellátási lánc biztonságáról – A Tanács által a 2022. október 17-i ülésén jóváhagyott tanácsi következtetések

Mellékelten továbbítjuk a delegációknak az IKT-ellátási lánc biztonságáról szóló, a Tanács által a 2022. október 17-i ülésén jóváhagyott tanácsi következtetéseket.

MELLÉKLET

A Tanács következtetései az IKT-ellátási lánc biztonságáról

AZ EURÓPAI UNIÓ TANÁCSA,

EMLÉKEZTETVE az alábbi tárgyakban kiadott következtetéseire:

– az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamentnek és a Tanácsnak címzett közös közleményről szóló, 2017. november 20-i következtetések,

– az uniós kiberbiztonsági kapacitás és képességek megerősítése,

– az 5G jelentősége az európai gazdaság számára és az 5G-hez kapcsolódó biztonsági kockázatok enyhítésének szükségessége,

– Európa digitális jövőjének alakítása,

– „A dinamikusabb, reziliensebb és versenyképesebb európai ipar felé való átmenetet elősegítő helyreállítás”,

– a csatlakoztatott eszközök kiberbiztonsága,

– a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégia,

– az Európai Unió kiberbiztonsági helyzetének javítása,

– az Európai Számvevőszék 03/2022. sz., „Az 5G bevezetése az Unióban: a hálózatok kiépítése késedelmes, egyes biztonsági kérdések továbbra is megoldatlanok” című különjelentése;

EMLÉKEZTETVE az Európai Tanácsnak az alábbi tárgyakban kiadott következtetéseire:

– Covid19, egységes piac, iparpolitika és digitális vonatkozások, valamint külkapcsolatok (2020. október 1–2.),

– az Ukrajna elleni orosz katonai agresszió, biztonság és védelem, energia, gazdasági kérdések, Covid19, valamint külkapcsolatok (2022. március 24–25.),

– Ukrajna, élelmezésbiztonság, biztonság és védelem, valamint energia (2022. május 30–31.);

1. tekintettel arra, hogy a geopolitika egyre nagyobb jelentőséggel bír a kiberbiztonság szempontjából, HANGSÚLYOZZA, hogy az Európai Uniónak és tagállamainak a kiberbiztonságot átfogó és stratégiai módon kell megközelíteniük. Oroszország Ukrajnával szembeni katonai agressziója nyomán komoly változás történt az Európai Unió stratégiai és biztonsági környezetében, valamint bebizonyosodott, hogy a biztonság és a védelem területén erősebb és cselekvőképesebb Európai Unióra van szükség. Rávilágított, hogy rendkívül fontos megfelelően figyelembe venni a geopolitikai környezetet nemcsak a rossz szándékú kibertevékenységekre való reagálás esetén, hanem az információs és kommunikációs technológiák (IKT) rezilienciájának kiépítése és fenntartása során is. Ez különösen fontos az IKT-termékek és -szolgáltatások ellátási láncai (IKT-ellátási láncok) esetében, amelyek geopolitikai rivalizálás miatt veszélybe kerülhetnek – amint azt a SolarWinds támadás is bizonyítja –, és amelyeket geopolitikai feszültségek és instabilitások is befolyásolhatnak, amint azt az Oroszország Ukrajnával szembeni katonai agressziója idején az orosz IKT-értékesítőktől való függőséggel kapcsolatos kockázat is mutatja;

2. MEGÁLLAPÍTJA, hogy az IKT-ellátási lánccal – amely a (az (EU) 2019/1020 rendeletben meghatározott) gazdasági szereplők erőforrásainak és folyamatainak egymáshoz kapcsolódó olyan készletéből áll, amely a nyersanyagok beszerzésétől kezdődően magában foglalja az IKT-termékek és -szolgáltatások gyártását, feldolgozását, kezelését és szállítását, ideértve az IKT-termékek és -szolgáltatások életciklusa során biztosított támogatást is – kapcsolatos kockázatok jellege egyedi kihívásokat támaszt és potenciálisan messzemenő következményeket von maga után. Az IKT-termékek – például az előállításukhoz szükséges kritikus fontosságú nyersanyagok és félvezetők hiánya miatt bekövetkező – hozzáférhetetlenségével kapcsolatos kockázatok mellett az IKT-termékek és -szolgáltatások ellátási láncai más fenyegetéseknek is ki vannak téve. Különösen rosszindulatú szereplők célba vehetik őket vagy visszaélhetnek velük olyan kifinomult, gyakran álcázott módszerekkel, amelyek hatással vannak a továbbított és tárolt érzékeny adatok bizalmas kezelésére, integritására és hozzáférhetőségére;

3. tudatában annak, hogy az IKT-eszközök biztonságáról való gondoskodás során az összes veszélyre kiterjedő megközelítésre van szükség, MEGÁLLAPÍTJA, hogy a kritikus fontosságú szervezetek rezilienciájáról szóló irányelvre irányuló javaslat releváns a kritikus fontosságú szervezetek fizikai biztonságának javítása szempontjából, és HANGSÚLYOZZA, hogy az ellátási láncokra irányuló, kibereszközökön keresztül végrehajtott támadásokkal szembeni reziliencia fokozása mellett ugyanilyen fontos az IKT-ellátási láncok általános rezilienciájának és biztonságának megerősítése a fenyegetések teljes skálájával – például a természeti eseményekkel, a rendszerhibákkal, a belső fenyegetésekkel vagy az emberi hibákkal – szemben. Ebben az értelemben TISZTÁBAN VAN AZZAL, hogy az IKT-ellátási láncok biztonsága magában foglalja az IKT-ellátási láncokban előállított, szállított, beszerzett és használt IKT-termékek és -szolgáltatások védelmének biztosítását, többek között az egyes összetevők és a továbbított adatok védelme révén;

4. az Európai Unió orosz fosszilis tüzelőanyagoktól való stratégiai függőségeiből eredő következményeknek, valamint az ellátási láncokban a Covid19-világjárvány idején – különösen a gyógyszerek és félvezetők tekintetében, ahol nyilvánvalóvá váltak az EU stratégiai függőségei – bekövetkezett zavarok hatásainak a tanulságaira építve arra ÖSZTÖNZI a tagállamokat, hogy törekedjenek arra, hogy az IKT-termékek és -szolgáltatások terén elkerüljék a hasonló, nem kívánt külső stratégiai függőségi helyzetek kialakulását. A társadalom fokozódó digitalizációja és az IKT-k kritikus infrastruktúrákban történő egyre szélesebb körű használata miatt folyamatosan értékelni kell az IKT-termékekhez és -szolgáltatásokhoz, valamint az azok ellátási láncaihoz kapcsolódó külső stratégiai függőségeket, és adott esetben kezelni kell azokat;

5. EMLÉKEZTET arra, hogy a nyitott gazdaság megőrzésével együtt a stratégiai autonómia megteremtése az Unió egyik kulcsfontosságú célkitűzése, amelynek részét képezi a stratégiai függőségek azonosítása és csökkentése, illetve a reziliencia növelése a legérzékenyebb ipari ökoszisztémákban, illetve egyes konkrét területeken, így például a digitális téren. Ez magában foglalja a stratégiai digitális kapacitások és infrastruktúrák fejlesztését és telepítését, valamint azon képesség megerősítését, hogy az EU autonóm technológiai döntéseket hozzon, az egyik fő pillérként pedig reziliens és biztonságos infrastruktúrák, termékek és szolgáltatások biztosítását annak érdekében, hogy bizalom alakuljon ki a digitális egységes piac iránt és az európai társadalmon belül, megőrizve ugyanakkor a nyitottságot, a hasonlóan gondolkodó partnerekkel való globális együttműködést és a versenyképességet, valamint kiaknázva az ezekből származó potenciális előnyöket. Az Európai Unió alapvető értékei védik különösen a magánéletet, a biztonságot, az egyenlőséget, az emberi méltóságot, a jogállamiságot és a nyílt internetet, amelyek a digitális dimenzió által vezérelt, emberközpontú társadalom, gazdaság és ipar megvalósításának előfeltételei;

6. MEGÁLLAPÍTJA, hogy a kiberfenyegetettségi helyzet terén bekövetkezett fejlemények – többek között az az utóbbi években megfigyelhető tendencia, hogy nagy hatással járó, kifinomult támadásokat intéznek az ellátási láncok ellen, mint például a SolarWinds, a Mimecast vagy a Kaseya támadások – miatt, amelyek az alapvető IKT-szolgáltatások kiszervezésével párhuzamosan jelennek meg, és amelyeket tovább fokoz a harmadik felek által gyártott, nyújtott vagy szervizelt IKT-termékekre és -szolgáltatásokra való általános támaszkodás, igen valószínű, hogy a jövőben több olyan, az ellátási láncot érintő támadás következik be, amelyek jelentős kárt okoznak a gazdaságnak és a társadalomnak. Ennek fényében HANGSÚLYOZZA egyrészt azt, hogy az egységes piac működése szempontjából fontos javítani az IKT-ellátási láncok biztonságát és rezilienciáját, másrészt pedig azt, hogy biztosítani kell az egységes piacon az IKT-termékek és -szolgáltatások rendelkezésre állását, biztonságát és sokféleségét. Következésképpen MEGÁLLAPÍTJA, hogy e célkitűzések elérése érdekében maximalizálni és észszerűsíteni kell a meglévő uniós eszközök és megközelítések alkalmazását, valamint hogy további – többek között a kialakulóban lévő és forradalmi technológiák lehetséges biztonsági kockázataival kapcsolatos – megfelelő intézkedések és mechanizmusok bevezetésével folyamatosan alkalmazkodni kell a változó kiberfenyegetettségi helyzethez. Arra ÖSZTÖNZI a tagállamokat, hogy e tekintetben kockázatalapú megközelítést alkalmazzanak az új technológiai fejlesztések kezelése érdekében;

7. TISZTÁBAN VAN AZZAL, hogy a folyamatosan változó kiberfenyegetettségi helyzetnek, valamint az ellátási láncokat érintő támadások összetettségének megértése elengedhetetlen az IKT-ellátási láncokkal kapcsolatos kockázatok hatékony csökkentéséhez. E tekintetben HANGSÚLYOZZA, hogy az ellátási lánccal kapcsolatos fenyegetettségi helyzet aktív és folyamatos nyomon követése, elemzése és értékelése révén alkalmazkodni kell az új fenyegetésekhez, növelni kell a fenyegetésekkel és a sebezhetőségekkel kapcsolatos tudatosságot és ismereteket, valamint testre szabott, proaktív módon figyelmeztetni kell az érintett szervezeteket. ÜDVÖZLI az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) által az IKT-ellátási lánc biztonságával kapcsolatban végzett munkát, és különösen annak az ellátási láncot érintő támadásokkal kapcsolatos fenyegetettségi helyzetről szóló jelentését;

ÁGAZATOKON ÁTÍVELŐ ESZKÖZÖK ÉS MEGKÖZELÍTÉSEK

8. ÚJÓLAG MEGERŐSÍTI annak fontosságát, hogy a tagállamok mérlegeljék a kritikus IKT-termékek, -szolgáltatások és -rendszerek beszállítói diverzifikálásának szükségességét annak érdekében, hogy elkerüljék, illetve korlátozzák az egyetlen beszállítótól – különösen a magas kockázatú beszállítóktól – való jelentős függőség kialakulását, mivel ez növeli a potenciális fennakadások következményeivel szembeni kitettséget. TUDATÁBAN VAN annak, hogy a vevőfogvatartás elkerülése és az IKT-beszállítók diverzifikálása a stabilitás biztosításának és a belső piac biztonsága garantálásának egyik fontos összetevője. KIEMELI az eladódiverzifikálás és a versenyképesség technológiasemleges módon történő elősegítésére irányuló, megfelelő stratégiák előmozdításának és végrehajtásának szükségességét. Emellett SZORGALMAZZA a vevőfogvatartás megelőzésével kapcsolatos szempontoknak az uniós jogszabályokba történő integrálását. E tekintetben NYUGTÁZZA a méltányos adathozzáférésre és adatfelhasználásra vonatkozó harmonizált szabályokról szóló rendeletre (adatmegosztási jogszabály) irányuló javaslatot, amelynek célja az adatfeldolgozási szolgáltatások interoperabilitásának növelése és az adatfeldolgozási szolgáltatók közötti váltás akadályainak felszámolása;

9. TUDATÁBAN VAN az IKT-ellátási lánc biztonsága és a közbeszerzések közötti kapcsolatnak. HANGSÚLYOZZA, hogy a közbeszerzési eljárások során megfelelően figyelembe kell venni az IKT-ellátási lánc biztonságának fontosságát, adott esetben az ajánlattevőknek a nyújtott szolgáltatások magas szintű biztonságának szavatolására vonatkozó képességével kapcsolatos, objektív és kockázatalapú kiválasztási szempontok előírása révén. SZORGALMAZZA az egyrészről a közforrások leghatékonyabb és legméltányosabb felhasználásához fűződő közérdek, másrészről pedig az információs rendszerek biztonságossá tételéhez és az egységes piac zökkenőmentes működéséhez fűződő közérdek kellő egyensúlyának megteremtését. A releváns közbeszerzési szabályoknak a kiberbiztonság fokozása mellett történő végrehajtásának elősegítése érdekében FELKÉRI a Bizottságot, hogy 2023 harmadik negyedévéig dolgozzon ki módszertani iránymutatásokat, amelyek arra ösztönzik az ajánlatkérő szerveket, hogy fordítsanak kellő figyelmet az ajánlattevők és alvállalkozóik kiberbiztonsággal kapcsolatos gyakorlatára, továbbá felkéri a Bizottságot arra, hogy vizsgálja meg a releváns közbeszerzési jogszabályokat, és szükség esetén terjesszen elő javaslatokat azok felülvizsgálatára vagy kiegészítésére vonatkozóan;

10. TUDATÁBAN VAN annak, hogy az IKT-termékekkel és -szolgáltatásokkal kapcsolatos közvetlen külföldi tőkebefektetések, habár gazdasági és társadalmi előnyökkel járnak a tagállamok, a vállalkozások és a polgárok számára, a biztonsággal és a közrenddel kapcsolatos kockázatokat is magukban rejthetnek, és MEGJEGYZI, hogy a közvetlen külföldi befektetésekre vonatkozó uniós átvilágítási mechanizmust – a nemzeti átvilágítási rendszerek mellett, amelyek eszközöket kínálnak e kockázatok kezelésére – szintén hasznos eszközként lehetne alkalmazni az IKT-ellátási lánc biztonságának és rezilienciájának megőrzése érdekében, mivel az hozzájárulna az említett biztonságot és rezilienciát esetlegesen befolyásoló magas kockázatú befektetések kizárásához. NYUGTÁZZA, hogy az említett mechanizmus keretében kicserélt és megosztott információk segíthetik a tagállamokat abban, hogy jobban fel tudják mérni az IKT-ellátási láncok biztonságát fenyegető esetleges veszélyeket, és meg tudják tenni a szükséges, megfelelő lépéseket. FELHÍVJA a releváns tagállami szereplőket, hogy adott esetben vegyék figyelembe az átvilágítási mechanizmus e dimenzióját is;

11. a védelmet illetően ÚJÓLAG MEGERŐSÍTI a Bizottsághoz intézett azon felkérését, hogy 2023-ban a tagállamokkal együtt számos területen – többek között a digitális területen – értékelje a kritikus infrastruktúrák ellátási láncaival kapcsolatos kockázatokat az EU biztonsági és védelmi érdekeihez kapcsolódóan, továbbá hogy tárja fel, milyen lehetőségek kínálkoznak a kiberbiztonság fokozására az EU védelmi technológiai és ipari bázisának teljes ellátási láncát érintően. Továbbá FELKÉRI a tagállamokat és a Bizottságot, hogy a stratégiai iránytű kötelezettségvállalásainak és intézkedéseinek végrehajtása során vegyék figyelembe az IKT-ellátási lánc biztonságának kérdését;

12. elismerve a kritikus fontosságú nyersanyagoknak, valamint a félvezetők minden fajtájának – mint az IKT-termékek alapvető építőelemeinek – fontosságát, SZORGALMAZZA az európai félvezető-ökoszisztéma megerősítését célzó intézkedési keret létrehozásáról szóló rendeletjavaslatról (a csipekről szóló európai jogszabály) és a közös vállalkozásoknak a Horizont Európa keretében történő létrehozásáról szóló (EU) 2021/2085 rendeletnek a csipekkel foglalkozó közös vállalkozás tekintetében történő módosításáról szóló tanácsi rendeletjavaslatról folytatandó konstruktív tárgyalásokat;

KIBERSPECIFIKUS ESZKÖZÖK

13. különös tekintettel a távközlési infrastruktúrára, ELISMERI az 5G-hálózatok ellátási lánca biztonságának javítása területén – különösen az 5G biztonsággal kapcsolatos uniós eszköztár (uniós 5G eszköztár) révén – uniós szinten elért eredményeket. FELHÍVJA a tagállamokat, hogy továbbra is osszák meg egymással az uniós 5G eszköztárban ajánlott intézkedések végrehajtására irányuló bevált gyakorlatokkal és módszerekkel kapcsolatos információkat, és különösen az uniós koordinált kockázatértékelésben kritikusnak és érzékenynek minősített kulcsfontosságú eszközök vonatkozásában alkalmazzák a magas kockázatú beszállítókra vonatkozó releváns korlátozásokat. KIEMELI, hogy az uniós 5G eszköztár olyan dinamikus kockázatalapú eszköz az azonosított biztonsági kihívások kezelésére, amely lehetővé teszi az 5G kiberbiztonsági szempontok időben és hatékonyan történő kezelését, tiszteletben tartva ugyanakkor a tagállamok hatásköreit, és ELISMERI, hogy az uniós 5G eszköztár értékes eszközt kínál a távközlési hálózatok ellátási lánca biztonságának koordinált és teljesen átlátható módon történő további javításához, ez pedig ösztönzőként szolgálhat az egyéb létfontosságú ágazatokkal kapcsolatos kockázatértékelési és -mérséklési eszközökhöz is. EMLÉKEZTET a releváns hatóságokhoz intézett azon felkérésére, hogy dolgozzanak ki kockázatértékelésen alapuló ajánlásokat a tagállamok és a Bizottság számára az Európai Unión belüli kommunikációs hálózatok és infrastruktúrák rezilienciájának megerősítése érdekében, ideértve az uniós 5G eszköztár folytatódó alkalmazását is;

14. NYUGTÁZZA az olyan interoperábilis megközelítések fontosságát, amelyek alkalmasak a vevőfogvatartás kezelésére és a koncentrációs kockázat csökkentésére, és ezzel egyidejűleg az ellátási lánc biztonságának fokozására az IKT-infrastruktúrák és -szolgáltatások teljes spektrumában. ELISMERI az „Open RAN” koncepció által e tekintetben kínált potenciális előnyöket, különösen az 5G hálózatokkal kapcsolatban, ugyanakkor EMLÉKEZTET az „Open RAN” kiberbiztonságáról szóló, a Kiberbiztonsági Együttműködési Csoport által közzétett jelentésre, megjegyezve, hogy ez a koncepció még fejlesztés alatt áll, és a biztonsága, az átláthatósága és a szabványosítása még az érettség kezdeti stádiumában jár, továbbá HANGSÚLYOZZA annak fontosságát, hogy bármilyen új szabványra vagy architektúrára való átállást megelőzően fel kell mérni a kockázatokat;

15. KIEMELI a kiberbiztonsággal kapcsolatos, már meglévő és a közeljövőben várható horizontális jogalkotási eszközök – nevezetesen az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló rendelet (kiberbiztonsági jogszabály), az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló, várható irányelv (NIS 2 irányelv), az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról szóló rendeletjavaslat, valamint a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló rendeletjavaslat (a kiberrezilienciáról szóló jogszabály) – relevanciáját az IKT-ellátási lánc biztonságának fokozása szempontjából. Emellett NYUGTÁZZA az ágazatspecifikus kiberbiztonsági rendeletek terén bekövetkezett fontos fejleményeket is, különös tekintettel a pénzügyi ágazat digitális működési rezilienciájáról szóló jövőbeli rendeletre (DORA-rendelet), amely rendelkezik a pénzügyi szervezetek számára kritikus fontosságú, harmadik félnek minősülő IKT-szolgáltatókra vonatkozó felvigyázási keretről. E rendeletek egyrészt általános kötelezettségeket írnak elő az ellátási lánc biztonsága tekintetében, másrészt pedig az érintett ágazatra vonatkozó részletes és egyedi követelményeket. Ezzel egyidejűleg HANGSÚLYOZZA, hogy a beszállítók gyakran nem csupán egy, hanem több különböző ágazat számára szállítják a termékeiket és nyújtják a szolgáltatásaikat. Ezért különösen fontos biztosítani azt, hogy az ellátási lánc biztonságára vonatkozó követelmények a lehetséges mértékben harmonizáltak legyenek minden érintett ágazat tekintetében, különös tekintettel a jövőbeli NIS 2 irányelv hatálya alá tartozó ágazatokra, a beszállítókra rótt kötelezettségek közötti eltérések elkerülése, valamint a kritikus ágazatok szereplőire háruló – a beszállítók e kötelezettségeknek való megfelelése értékelésével kapcsolatos – terhek könnyítése érdekében, figyelembe véve ugyanakkor az ágazati sajátosságokat;

16. ÜDVÖZLI a kiberrezilienciáról szóló jogszabályra irányuló javaslatot, mint a digitális elemeket tartalmazó termékek biztonságos fejlesztését előmozdító fontos jogalkotási eszközt, amely azt is hivatott biztosítani, hogy a digitális elemeket tartalmazó termékek teljes életciklusa során vegyék figyelembe a kiberbiztonságot. MEGÁLLAPÍTJA, hogy a kiberrezilienciáról szóló jogszabályra irányuló javaslat magában hordozza annak lehetőségét, hogy jelentősen hozzájáruljon az IKT-ellátási lánc biztonságának megerősítéséhez. SZORGALMAZZA a jogszabályra irányuló konstruktív tárgyalásokat és a jogszabály időben történő elfogadását;

17. e tekintetben ELISMERI az ENISA vezetésével zajló, a tagállamok és az egyéb érdekelt felek által együttesen folytatott munkát, amelynek célja, hogy az IKT-termékekre, -szolgáltatásokra és -folyamatokra alkalmazandó olyan tanúsítási rendszereket bocsássanak az EU rendelkezésére a kiberrezilienciáról szóló jogszabályra irányuló javaslattal összhangban, amelyek hozzájárulnak a kiberbiztonság általános szintjének növeléséhez a digitális egységes piacon. Minden érdekelt felet arra ÖSZTÖNÖZ, hogy vegyenek részt az egyes európai tanúsítási rendszerekkel kapcsolatos előkészítő munkában a biztonságos IKT-termékek, -folyamatok és -szolgáltatások iránti bizalom kiépítése és rezilienciájuk megerősítése érdekében, és FELHÍVJA a Bizottságot, hogy az előkészítő munka befejezését követően mielőbb dolgozzon ki végrehajtási jogi aktusokat az európai tanúsítási rendszerekre vonatkozóan, különös tekintettel a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszerre (EUCC). MEGJEGYZI, hogy az európai tanúsítási rendszereknek szükség esetén az ellátási lánc biztonságával kapcsolatos követelményeket kellene magukban foglalniuk, többek között a beszállítókkal való kapcsolat tekintetében;

18. KIEMELI, hogy a jövőbeli NIS 2 irányelvnek az IKT-ellátási lánc biztonságával kapcsolatos valamennyi rendelkezését maradéktalanul végre kell hajtani. E tekintetben HANGSÚLYOZZA a kritikus ellátási láncok uniós koordinált kockázatértékelésének (koordinált ellátásilánc-kockázatértékelés), az ellátási láncok biztonságával kapcsolatos nemzeti szakpolitikáknak és az ellátási láncokkal kapcsolatos biztonsági intézkedéseknek a relevanciáját. MEGJEGYZI, hogy az elsődleges beszállítók, illetve a végső ügyfelek biztonságát illető kockázatok tekintetében nem csupán az elsődleges beszállítókra kell figyelmet fordítani, hanem az érintett alvállalkozókra is. Az ellátásilánckockázat-kezelési intézkedések végrehajtásának elősegítése érdekében arra ÖSZTÖNZI az ENISA-t, hogy a Kiberbiztonsági Együttműködési Csoport támogatásával vegye számba az ellátásilánckockázat-kezelés legjobb gyakorlatait, és állítson össze azokból módszertani iránymutatásokat. Ezen túlmenően arra ÖSZTÖNZI az ENISA-t, hogy kísérje figyelemmel a jövőbeli NIS 2 irányelv által szabályozott szervezetek által az IKT-ellátási lánc biztonsága terén eszközölt beruházásokat;

19. KIEMELI továbbá a felügyelt szolgáltatók és a felügyelt biztonsági szolgáltatók igénybevételének az ellátási lánc biztonságával összefüggésben meglévő előnyeit és kockázatait. Bár e szolgáltatók igénybevétele jelentősen javíthatja a szervezeteken belüli biztonságot, és a kiberbiztonság magasabb szintjeihez vezethet, az IKT-rendszerek és -szolgáltatások távolból történő kezelése – kombinálva az ügyfél IKT-környezetéhez való kiemelt hozzáféréssel, amelyre a felügyelt szolgáltatóknak és a felügyelt biztonsági szolgáltatóknak adott esetben szükségük lehet – a feltört felügyelt szolgáltatók és felügyelt biztonsági szolgáltatók esetében jelentős továbbgyűrűző hatásokhoz vezethet számos ügyfél tekintetében. Ezért rendkívül fontos, hogy a felügyelt szolgáltatók és a felügyelt biztonsági szolgáltatók fenntartsák a saját belső biztonságuk és az általuk nyújtott szolgáltatások biztonságának magas szintjét, továbbá hogy az általuk nyújtott szolgáltatások tekintetében átlátható megközelítést alkalmazzanak ügyfeleik irányában. ÜDVÖZLI e tekintetben, hogy ezek a jövőben a leendő NIS 2 irányelv hatálya alá kerülnek;

20. ami a leendő NIS 2 irányelv szerinti koordinált ellátásilánc-kockázatértékelésekre vonatkozó mechanizmus végrehajtását illeti, ezen összefüggésben RÁMUTAT a nem technikai kockázati tényezők – mint például valamely harmadik állam által a beszállítókra és a szolgáltatókra gyakorolt jogtalan befolyásolás – relevanciájára, és ebben az összefüggésben TUDOMÁSUL VESZI az 5G-hálózatok kiberbiztonságára vonatkozó uniós koordinált kockázatértékelésben említett, a kockázati profil értékelésére felhasználható tényezőket. FELKÉRI a Bizottságot, hogy a Kiberbiztonsági Együttműködési Csoporttal és az ENISA-val való konzultációt követően 2023 második negyedévéig azonosítsa azokat a konkrét IKT-szolgáltatásokat, -rendszereket vagy -termékeket, amelyek adott esetben elsőbbséget élvező koordinált ellátásilánc-kockázatértékelések tárgyát képezhetik;

21. MEGÁLLAPÍTJA, hogy a kritikus fontosságú hálózatok és rendszerek működtetéséhez használt IKT-termékek és -szolgáltatások magas kockázatú beszállítóitól való függőségek olyan stratégiai fenyegetést jelentenek, amelyet – nemzeti és uniós szinten egyaránt – megfelelő szakpolitikák révén, valamint a tagállamok közötti és a hasonlóan gondolkodó nemzetközi partnerekkel folytatott együttműködés révén mérsékelni kell. E stratégiai kockázat mérséklésének elősegítése és a koordinált ellátásilánc-kockázatértékelések támogatása érdekében FELKÉRI a Kiberbiztonsági Együttműködési Csoportot, hogy a Bizottsággal és az ENISA-val együttműködésben dolgozzon ki intézkedési eszköztárat az IKT-ellátási láncot érintő kritikus kockázatok csökkentésére (IKT-ellátási láncra vonatkozó eszköztár). Az IKT-ellátási láncra vonatkozó eszköztárnak az IKT-ellátási láncok tekintetében azonosított fenyegetettségi forgatókönyvekre kell épülnie, továbbá intézkedéseket kell biztosítania az e forgatókönyvekre való reagálás érdekében, az 5G eszköztárból, valamint a nemzeti szinten szerzett tapasztalatok hasznosításával. Átlátható módon ki kell egészítenie a leendő NIS 2 irányelv szerinti, meghatározott IKT-szolgáltatásokra, -rendszerekre vagy -termékekre vonatkozó koordinált ellátásilánc-kockázatértékeléseket azáltal, hogy olyan általános kockázatcsökkentési intézkedéseket kínál, amelyek az egyes konkrét IKT-szolgáltatásokhoz, -rendszerekhez vagy -termékekhez igazíthatók, mégpedig méretezhető módon, az egyedi koordinált ellátásilánc-kockázatértékelések során azonosított kockázatok alapján;

22. HANGSÚLYOZZA, hogy a kutatás, az innováció, a beruházások és a vállalkozói tevékenységek fontos szerepet töltenek be a digitális területen és a kiberbiztonság területén csakúgy, mint az ilyen tevékenységek finanszírozása, tekintettel a lehetséges jövőbeli nem kívánt stratégiai függőségek elkerülésére, valamint az IKT-ellátási láncok általános rezilienciájának megerősítésére. KIEMELI ezen összefüggésben az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) és a nemzeti koordinációs központok hálózata mind a stratégiai, mind a végrehajtási feladatainak szerepét és relevanciáját az ahhoz való hozzájárulás tekintetében, hogy maximalizálni lehessen a beruházások hatásait az Unió vezető szerepének és nyitott stratégiai autonómiájának a kiberbiztonság területén történő megerősítése, az Unió technológiai kapacitásainak és készségeinek támogatása, valamint az Unió globális versenyképességének növelése érdekében. SZORGALMAZZA e tekintetben az ECCC gyors működőképessé tételét. FELHÍVJA az ECCC-t, hogy stratégiai menetrendjében vegye figyelembe az IKT-ellátási lánc biztonsági vonatkozásait, ideértve például a biztonságos szoftverek fejlesztését, egyidejűleg biztosítva az egységességet és a kiegészítő jelleget, valamint a párhuzamos erőfeszítések elkerülését. TÁMOGATJA az európai versenyképességnek a kiberbiztonság területén való javítását olyan finanszírozási programok által, mint a Horizont Európa kutatási és innovációs program, valamint az Unió digitális gazdasága, társadalma és demokráciája szempontjából alapvető kapacitások megerősítését, kiépítését és beszerzését célzó Digitális Európa program;

TÁMOGATÓ MECHANIZMUSOK

23. SZORGALMAZZA az IKT-ellátási lánc biztonságának megerősítését célzó intézkedésekhez kapcsolódó pénzügyi támogatási ösztönzők növelését. FELSZÓLÍTJA – a NIS 2 irányelv jövőbeli végrehajtására is figyelemmel – az ECCC-t, a Bizottságot és a releváns érdekelt feleket, hogy kezeljék kiemelt feladatként az arra való lehetőségek feltárását, hogy miként lehetne beépíteni az IKT-ellátási lánc biztonsági vonatkozásait a Digitális Európa program és a Horizont Európa program keretében várható kiberbiztonsági munkaprogramokon belüli jövőbeli pályázati felhívásokba, illetve bármely egyéb releváns finanszírozási lehetőségbe. E finanszírozási lehetőségeknek egyebek között arra kell irányulniuk, hogy az ellátási lánc teljes egésze tekintetében lehetővé tegyék a szervezetek számára az IKT-termékek és -szolgáltatások beszerzésével összefüggésben a magas szintű kiberbiztonság fenntartásának támogatását, különös tekintettel egyes kritikus fontosságú, a jövőbeli koordinált ellátásiánc-kockázatértékelésekkel összhangban magas kockázatúnak minősülő IKT-szolgáltatások, -rendszerek vagy -termékek helyettesítésére, illetve cseréjére;

24. MEGÁLLAPÍTJA, hogy a globalizáció és az IKT-szolgáltatások specializálódása, valamint a harmadik felek termékeitől és szolgáltatásaitól való megnövekedett függőség szükségessé teszi a szoros EU-n belüli és nemzetközi együttműködést a tudásnak és a tapasztalatoknak a releváns érdekelt felek közötti megosztása tekintetében, továbbá ÖSZTÖNZI őket arra, hogy alakítsanak ki olyan szilárd és koordinált álláspontot, amely átfogó módon biztosítja az IKT-ellátási lánc biztonságát. TISZTÁBAN VAN továbbá azzal, hogy szükség van a releváns legújabb megközelítések és technikák további feltárására, mind a megfelelő alapvető kiberhigiénia, mind a biztonságos és reziliens IKT-ellátási láncok elérésére szolgáló hosszú távú megoldások, valamint ezek előmozdításának és a szakpolitikai vagy egyéb kezdeményezésekbe való lehetséges beépítésük legmegfelelőbb módjai tekintetében. ELISMERI e tekintetben, hogy különös figyelmet kell fordítani az olyan szisztematikus megoldások előnyeinek és hátrányainak feltárására, mint amilyenek a „zéró bizalom” alapelvei, a szoftverelemjegyzék és más hasonló, hosszú távú megoldások. AJÁNLJA a Kiberbiztonsági Együttműködési Csoportnak az e célra való igénybevételét;

25. MEGJEGYZI, hogy a kiberbiztonsági események és fenyegetések nyomon követése és a rájuk vonatkozó információk hatékony megosztása előnyökkel jár az ellátási láncokkal szembeni támadások megelőzése, felderítése és a hatásaik enyhítése szempontjából. HANGSÚLYOZZA a tagállamok közötti további bizalomépítés szükségességét az ilyen információk hatékony megosztása végett. EMLÉKEZTET e tekintetben a Bizottság arra irányuló javaslatára, hogy támogassa a tagállamokat a biztonsági műveleti központok (SOC-ok) létrehozásában és megerősítésében annak érdekében, hogy EU-szerte létrejöjjön a SOC-ok hálózata, valamint hogy jobban nyomon lehessen követni és előre lehessen jelezni a hálózatok elleni támadásokra utaló jeleket. EMLÉKEZTET arra, hogy szükség van a meglévő hálózatokon és mechanizmusokon belüli komplementaritásra és koordinációra, és mindenekelőtt KIEMELI e tekintetben a CSIRT-ek hálózatának szerepét és azt, hogy szükséges alaposabban feltárni, milyen potenciállal rendelkeznek e hálózatok a hatékony, biztonságos és megbízható információmegosztási kultúra előmozdítására. EMLÉKEZTET a tagállamok által az EU támogatásával tett erőfeszítésekre, amelyek célja ágazati, nemzeti és regionális CSIRT-ek, valamint nemzeti vagy európai információmegosztási és -elemző központok (ISAC-k) létrehozása az uniós kiberbiztonsági partnerségek hatékony hálózatának részeként;

26. az IKT-ellátási láncot érintő fenyegetések egymáshoz kapcsolódó és globális jellegére tekintettel KIEMELI, hogy fontos az IKT-ellátási lánc biztonságának globális szintű megközelítése és fokozása. Erre figyelemmel AJÁNLJA a digitális partnerségek, a kiberdialógusok és az egyéb releváns uniós kezdeményezések (ideértve adott esetben a szabadkereskedelmi megállapodásokat is) igénybevételét az IKT-termékbeszállítók és IKT-szolgáltatók kockázatalapú értékeléseinek előmozdítása, megbízható beszállítók igénybevétele és egy nyílt, interoperábilis és átlátható szabványokon alapuló, egyszersmind biztonságos és innovatív digitális ökoszisztéma alkalmazása érdekében. MEGISMÉTLI továbbá a „Global Gateway” partnerségek, valamint az EU–USA Kereskedelmi és Technológiai Tanács elképzelését és a munkacsoportjai keretében folytatott tevékenységeket, amelyek a megbízható, illetve nem nagy kockázatú beszállítók igénybevételére és egy olyan finanszírozási mechanizmus kidolgozására irányulnak, mely olyan projekteket tenne lehetővé, amelyek biztonságosabbá, reziliensebbé és megbízhatóbbá tennék az IKT-infrastruktúrát és -szolgáltatásokat harmadik államokban, többek között azáltal, hogy technológiasemleges módon tartózkodnának a nem megbízható, illetve nagy kockázatú beszállítóktól történő beszerzések finanszírozásától;

27. ÚJÓLAG MEGERŐSÍTI elkötelezettségét a nyitott, szabad, globális, stabil és biztonságos kibertérhez való hozzájárulás és az ilyen kibertér előmozdítása, valamint a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó, az ENSZ keretében megállapított normák, szabályok és elvek tiszteletben tartása mellett. EMLÉKEZTET – különösen az IKT-ellátási lánc biztonságához kapcsolódóan – az ENSZ kormányzati szakértői csoportja (UN GGE) és nyitott munkacsoportja (OEWG) által jóváhagyott normára, mely arra ösztönzi az államokat, hogy – többek között objektív együttműködési intézkedések kidolgozásával – tegyenek észszerű lépéseket az ellátási lánc integritásának biztosítására, hogy a végfelhasználók bizalommal lehessenek az IKT-termékek biztonsága iránt, valamint arra, hogy törekedjenek a rosszindulatú IKT-eszközök és -technikák terjedésének és a káros rejtett funkciók használatának megakadályozására, továbbá SZORGALMAZZA annak széles körű végrehajtását.