Az Európai Unió
Tanácsa

Brüsszel, 2021. március 9.
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

FELJEGYZÉS AZ „I/A” NAPIRENDI PONTHOZ

Küldi:	a Tanács Főtitkársága
Címzett:	az Állandó Képviselők Bizottsága/a Tanács
Tárgy:	Tervezet – A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról

1. A Bizottság és az Unió külügyi és biztonságpolitikai főképviselője 2020. december 16-án közzétette „Az EU kiberbiztonsági stratégiája a digitális évtizedre” című, az Európai Parlamentnek és a Tanácsnak címzett közös közleményét[1]. Az új kiberbiztonsági stratégia célja, hogy megerősítse Európa kiberfenyegetésekkel szembeni kollektív rezilienciáját, valamint biztosítsa, hogy minden polgár és vállalkozás megbízható szolgáltatásokat és digitális eszközöket vehessen igénybe, és ezek előnyeit teljes mértékben ki tudja használni.

[1] 14133/20.

2. A Bizottság és az EKSZ a kiberkérdésekkel foglalkozó horizontális munkacsoport (HWPCI) 2020. december 17-i és 2021. január 12-i nem hivatalos videokonferenciáján ismertette a közös közleményt. A HWPCI 2020. december 17-i nem hivatalos videokonferenciáján a soron következő portugál elnökség bejelentette, hogy tanácsi következtetéstervezetet kíván készíteni az EU digitális évtizedre szóló kiberbiztonsági stratégiájáról.

3. Az elnökség a tanácsi következtetések első tervezetét a HWPCI 2021. február 2-i nem hivatalos videokonferenciáján terjesztette elő. A következtetések ezen első változatáról ezután egyeztetésre került sor a HWPCI 2021. február 9-i, 2021. február 19-i, valamint 2021. március 1-ji és 9-i nem hivatalos videokonferenciái alkalmával.

4. Mivel a következtetéstervezet (a 30. pontban) utalást tartalmaz az Unió védelmi politikájára is, erről a pontról a katonapolitikai kérdésekkel foglalkozó csoport is egyeztetett a 2021. február 10-i ülésén.

5. Számos pont (az 1., a 4., a 7., a 8., a 9., a 20., a 23., a 24., a 26., a 27., a 28., a 29., a 30., a 31., a 32. és a 33.) a közös kül- és biztonságpolitika területéhez tartozó kérdéseket tárgyal, ezért e pontokat az elnökség benyújtotta a Politikai és Biztonsági Bizottsághoz, amely a 2021. március 4-i ülésén jóváhagyta azokat.

6. A HWPCI a 2021. március 9-i nem hivatalos videokonferenciáján megállapodásra jutott a tanácsi következtetéseknek a 6722/21 dokumentumban foglalt tervezetéről.

7. A fentiek alapján felkérjük az Állandó Képviselők Bizottságát, hogy nyújtsa be a tanácsi következtetések mellékletben foglalt tervezetét a Tanácsnak, és javasolja a következtetéstervezet „A” napirendi pontként történő elfogadását.

MELLÉKLET

Tervezet – A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról

AZ EURÓPAI UNIÓ TANÁCSA,

EMLÉKEZTETVE az alábbi tárgyakban kiadott következtetéseire:

– „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér” című, az Európai Parlamentnek és a Tanácsnak címzett, 2013. június 25-i közös közlemény[2],

– Az internet irányítása[3],

– az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamentnek és a Tanácsnak címzett, 2017. november 20-i közös közlemény[4],

– az uniós kiberbiztonsági kapacitás és képességek megerősítése[5],

– az 5G jelentősége az európai gazdaság számára és az 5G-hez kapcsolódó biztonsági kockázatok enyhítésének szükségessége[6],

– a nagymértékben digitalizált Európa jövője 2020 után: „A digitális és gazdasági versenyképesség fokozása Unió-szerte és a digitális kohézió”[7],

– a reziliencia megerősítésére és a hibrid fenyegetések elleni küzdelemre irányuló kiegészítő jellegű erőfeszítések[8],

– Európa digitális jövőjének alakítása[9],

---

2 12109/13.
3 16200/14.
4 14435/17 + COR 1.
5 7737/19.
6 14517/19.
7 9596/19.
8 14972/19.
9 8711/20.

– a digitális diplomácia[10],

– a reziliencia megerősítése és a Covid19-világjárvány összefüggésében felmerülő hibrid fenyegetések, többek között a dezinformáció elleni küzdelem[11],

– a kiberdiplomácia[12],

– a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás[13],

– a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete („kiberdiplomáciai eszköztár”)[14],

– a külső kiberkapacitás-építésre vonatkozó uniós iránymutatások[15],

– a dinamikusabb, reziliensebb és versenyképesebb európai ipar felé való átmenetet elősegítő helyreállítás[16],

– a csatlakoztatott eszközök kiberbiztonsága[17],

– Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása[18],

– valamint: a Tanács állásfoglalása a titkosításról – Biztonság titkosítással és biztonság a titkosítás ellenére[19],

---

10 12804/20.
11 14064/20.
12 6122/15 + COR 1.
13 10085/18.
14 10474/17.
15 10496/18.
16 13004/20.
17 13629/20.
18 14540/16.
19 13084/1/20 REV 1.

– továbbá: az uniós vállalkozások és közszféra céljait szolgáló új generációs felhő létrehozásáról szóló, a tagállamok által 2020. október 15-én tett nyilatkozat,

EMLÉKEZTETVE az Európai Tanács azon következtetéseire, amelyeket 2020. október 1–2-án a Covid19-válságról, az egységes piacról, az iparpolitikáról, a digitális vonatkozásokról és a külkapcsolatokról[20], valamint azokra, amelyeket 2019. június 20-án a dezinformációról és a hibrid fenyegetésekről, valamint a 2019–2024-es időszakra szóló új stratégiai menetrendről[21] fogadott el,

EMLÉKEZTETVE a „Közös jövőkép, közös fellépés: erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan” című, 2016. június 28-i dokumentumra,

EMLÉKEZTETVE az Európai Bizottság „Európa digitális jövőjének megtervezése” című, 2020. december 19-i[22], valamint „A biztonsági unióra vonatkozó uniós stratégia” című, 2020. július 24-i[23] közleményére,

EMLÉKEZTETVE az Európai Bizottság és a főképviselő „A globális változásra irányuló új EU–USA program” című, 2020. december 2-i közös közleményére[24],

1. KIEMELI azt a tényt, hogy a kiberbiztonság alapvető fontosságú ahhoz, hogy reziliens, zöld és digitális Európát tudjunk építeni, és ÜDVÖZLI „Az EU kiberbiztonsági stratégiája a digitális évtizedre” című, az Európai Parlamentnek és a Tanácsnak címzett közös közleményt, amely új keretet vázol fel egyrészt a „reziliencia, technológiai szuverenitás és vezető szerep” területére irányuló uniós intézkedésekhez, másrészt arra vonatkozóan, hogy az EU miként tudja megvédeni a lakóit, a vállalkozásokat és az intézményeket a kiberbiztonsági eseményektől, illetve támadásoktól, ugyanakkor pedig megerősíteni az egyének és a szervezetek bizalmát az iránt, hogy az EU képes előmozdítani a hálózati és információs rendszerek és infrastruktúrák, illetve a konnektivitás biztonságosságát és megbízhatóságát, és elősegíteni egy, az emberi jogokon, az alapvető szabadságokon, a demokrácián és a jogállamiságon alapuló globális, nyitott, szabad, stabil és biztonságos kibertér létrejöttét, és megvédeni azt;

---

20 EUCO 13/20.
21 EUCO 9/19.
22 2020. február 19., COM(2020) 67 final.
23 2020. július 24., COM(2020) 605 final.
24 2020. december 2., JOIN(2020) 22 final.

2. ELISMERI, hogy a Covid19-világjárvány következtében kiemelt helyre került mindennapi életünkben az információs és kommunikációs (IKT) technológiai eszközök és rendszerek iránti bizalommal és azok biztonságosságával kapcsolatos megnövekedett igény. HANGSÚLYOZZA, hogy a kiberbiztonság és a globális, nyílt internet mind nemzeti, mind uniós szinten létfontosságú a közigazgatás és az intézmények működése szempontjából, valamint társadalmaink és a gazdaság egésze számára;

3. HANGSÚLYOZZA, hogy a politikai és stratégiai döntéshozatali szinteken fokozottabb tudatosságnövelésre van szükség a kibertér kérdéseivel kapcsolatban – a döntéshozók releváns ismeretekkel és információkkal való ellátása révén –, valamint KIEMELI a köztájékozottság javításának és a kiberhigiénia előmozdításának a szükségességét;

4. SZORGALMAZZA a legfőbb uniós értékek – a demokrácia, a jogállamiság, az emberi jogok és az alapvető szabadságok, valamint ezeken belül a véleménynyilvánítás és a tájékozódás szabadságához, a gyülekezés és az egyesülés szabadságához, valamint a magánélet tiszteletben tartásához való jog – kibertérben való előmozdításának és védelmének biztosítását. ÜDVÖZLI e tekintetben, hogy azoknak az emberijog-védőknek, valamint a civil társadalom és a tudományos élet azon képviselőinek a védelme érdekében, akik olyan kérdéseken dolgoznak, mint például a kiberbiztonság, az adatvédelem, a kibertér felügyelete és az online cenzúra, további, tartós erőfeszítésekre kerül sor – folytatódó gyakorlati iránymutatás révén, a legjobb gyakorlatok előmozdításával, valamint az emberi jogok megsértésének és az azokkal való visszaélésnek, valamint a kialakulóban lévő technológiák helytelen használatának a megelőzésére irányuló uniós erőfeszítések fokozásával, különösen szükség szerint diplomáciai intézkedések alkalmazása, illetve az ilyen technológiák kivitelének az ellenőrzése révén. HANGSÚLYOZZA ezzel összefüggésben az emberi jogokra vonatkozó 2020–2024-es uniós cselekvési terv, valamint az abban foglalt, az online és offline véleménynyilvánítás szabadságáról szóló emberi jogi iránymutatások fontosságát;

5. ALÁHÚZZA, hogy az Unió egyik kulcsfontosságú célkitűzését képezi az, hogy a nyitott gazdaság megőrzése mellett megteremtse stratégiai autonómiáját, hogy ezáltal maga határozhassa meg gazdasági pályáját és érdekeit. Ez magában foglalja annak a képességnek a megerősítését is – az EU digitális vezető szerepének és stratégiai képességeinek a megerősítése céljával –, hogy az Unió önálló választásokkal élhessen a kiberbiztonság területén. EMLÉKEZTET arra, hogy ennek részét képezi a stratégiai függőségek azonosítása és csökkentése, illetve a reziliencia növelése a legérzékenyebb ipari ökoszisztémákban, illetve egyes konkrét területeken. NYOMATÉKOSÍTJA, hogy ez magában foglalhatja továbbá a termelési és ellátási láncok diverzifikálását, az Európán belüli termelés és beruházás fokozását, az alternatív megoldások és a körforgásos modellek feltárását, valamint a tagállamok közötti széles körű ipari együttműködés előmozdítását;

6. a munkaerő digitális és kiberbiztonsági készségeinek hiányára tekintettel HANGSÚLYOZZA, hogy a digitális és kiberbiztonsági területen képzett munkaerő iránti keresletet elsősorban a legkiválóbb tehetségek – például oktatással és képzéssel történő – fejlesztése, megtartása és vonzása révén kell kielégíteni, hogy társadalmunkat a kiberbiztonság garantálása mellett tudjuk digitalizálni. ÖSZTÖNZI a nők és lányok nagyobb arányú részvételét a természettudományok, a technológia, a műszaki tudományok, a matematika (TTMM-tárgyak) oktatásában, valamint a digitális munkahelyeken szükséges digitális készségeket javító továbbképzésben és átképzésben, ami a nemek közötti digitális szakadék áthidalásának egyik eszköze;

7. EMLÉKEZTET arra, hogy a kiberdiplomácia közös és átfogó uniós megközelítésének célja, hogy hozzájáruljon a konfliktusmegelőzéshez, a kiberbiztonsági fenyegetések mérsékléséhez és a nemzetközi kapcsolatok stabilizálásához. Ezzel összefüggésben ÚJÓLAG MEGERŐSÍTI elkötelezettségét a kibertérrel kapcsolatos nemzetközi viták békés úton történő rendezése iránt, és hogy az EU valamennyi diplomáciai erőfeszítésének elsődleges célja a kibertér biztonságának és stabilitásának előmozdítása fokozott nemzetközi együttműködés révén, valamint az IKT-eseményekből eredő félreértések, eszkaláció és konfliktusok kockázatának csökkentése, továbbá TÁMOGATJA a bizalomépítő intézkedések regionális és nemzetközi szintű továbbfejlesztését és működőképessé tételét. ÚJÓLAG HANGSÚLYOZZA, hogy az ENSZ Közgyűlésének konszenzussal elfogadott felhívása szerint az ENSZ-tagállamokat az ENSZ-közgyűlés jelentéseiben foglalt ajánlásoknak kell vezérelniük az IKT alkalmazása során, és ÚJÓLAG MEGERŐSÍTI, hogy a nemzetközi jog, különösen az ENSZ Alapokmánya teljes körűen alkalmazandó a kibertérben;

8. ÚJÓLAG MEGERŐSÍTI, hogy a normák és szabványok Unión belüli továbbfejlesztése elengedhetetlen ahhoz, hogy jelentősen alakítani lehessen a kialakulóban lévő technológiák területén a nemzetközi normákat és szabványokat, valamint az internet magját alkotó nyilvános elemek általános hozzáférhetőségéhez és integritásához elengedhetetlen műszaki és logikai infrastruktúrát, hogy azok összhangban legyenek az egyetemes és uniós értékekkel, és kialakításuk több érdekelt fél bevonásával történjen. Ez biztosítani fogja, hogy az internet globális, nyitott, szabad, stabil és biztonságos maradjon, valamint hogy a digitális technológiák használata és fejlesztése az emberi jogok tiszteletben tartásával történjen, használatuk pedig jogszerű, biztonságos és etikus legyen. NYUGTÁZZA a hamarosan elkészülő szabványosítási stratégiát, és VÁLLALJA, hogy proaktív és koordinált tájékoztatási tevékenységet folytat az EU vezető szerepének és célkitűzéseinek nemzetközi szintű előmozdítása érdekében, többek között a különböző nemzetközi szabványügyi testületekben, valamint a hasonlóan gondolkodó partnerekkel, a civil társadalommal, a tudományos körökkel és a magánszektorral folytatott együttműködés révén;

9. HATÁROZOTTAN TÁMOGATJA az internetirányítás és kiberbiztonság többszereplős modelljét, és vállalja, hogy megerősíti az érdekelt felekkel – többek között a magánszektorral, a tudományos körökkel és a civil társadalommal – a nemzetközi fórumokon folytatott rendszeres és strukturált információcserét, többek között a „Párizsi felhívás a kibertérbeli bizalom és biztonság érdekében” című kezdeményezés keretében. ELŐMOZDÍTJA az internethez való egyetemes, megfizethető és egyenlő hozzáférést, amellyel áthidalhatók a digitális szakadékok, és különösen a nők és lányok, valamint a kiszolgáltatott vagy marginalizált helyzetű személyek társadalmi szerepvállalásának növelését mind a szakpolitikák kidolgozása, mind az internet használata során;

10. HANGSÚLYOZZA, hogy az elkövetkező években a kiberbiztonságot be kell építeni a digitális beruházásokba és kezdeményezésekbe, valamint hogy fokozatosan hozzá kell járulni az egyenlő versenyfeltételek megteremtéséhez a kiberbiztonság területén, és TUDOMÁSUL VESZI a Bizottság arra irányuló tervét, hogy növelje a kiberbiztonságra fordított közkiadásokat és fellendítse az ilyen magánberuházásokat. KIEMELI a kis- és középvállalkozások (kkv-k) kiberbiztonsági ökoszisztémában betöltött jelentőségét, és MÉLTÁNYOLJA azokat a releváns pénzügyi eszközöket, amelyek a 2021–2027-re szóló többéves pénzügyi keret, valamint a Helyreállítási és Rezilienciaépítési Eszköz keretében támogatják a kiberbiztonságnak a digitális átállásban játszott erőteljes szerepét;

11. VÁRAKOZÁSSAL TEKINT az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontról és a nemzeti koordinációs központok hálózatáról (CCCN) szóló rendelet gyors végrehajtása, és többek között a bukaresti Európai Kiberbiztonsági Kompetenciaközpont gyors felállítása és működőképessé tétele elé. Munkatervének mielőbbi elfogadása hozzá fog járulni az Unió kiberbiztonsági vezető szerepének és stratégiai autonómiájának megerősítésére irányuló beruházások hatásának maximalizálásához, a technológiai kapacitások és készségek támogatásához, valamint az Unió globális versenyképességének növeléséhez a kiberbiztonság területén működő iparágak és tudományos közösségek – többek között a kkv-k és a kutatóközpontok – hozzájárulásával, amelyek az Unió és valamennyi tagállama kohézióját szem előtt tartva szisztematikusabb, inkluzívabb és stratégiaibb együttműködésre számíthatnak a jövőben;

12. ÜDVÖZLI az ENISA vezetésével zajló, a tagállamok és az érdekelt felek által együttesen folytatott munkát, amelynek célja, hogy az IKT-termékekre, -szolgáltatásokra és -folyamatokra alkalmazandó olyan tanúsítási rendszereket bocsássanak az EU rendelkezésére, amelyek hozzájárulnak a kiberbiztonság általános szintjének növeléséhez a digitális egységes piacon. Ezzel összefüggésben VÁRAKOZÁSSAL TEKINT az Unió gördülő munkaprogramja elé, amelynek célja a kiberbiztonsági jogszabályon (CSA) belüli uniós kiberbiztonsági tanúsítási rendszerek kidolgozása. Ezzel kapcsolatban ELISMERI, hogy az EU kulcsszerepet játszik az olyan szabványok kidolgozásában, amelyek képesek alakítani a kiberbiztonsági környezetet, és amelyek hozzájárulnak a tisztességes verseny biztosításához az EU-n belül és a globális színtéren is, továbbá előmozdítják a piacra jutást és kezelik a biztonsági kockázatokat, és egyúttal biztosítják az uniós jogszabályi keret alkalmazhatóságát;

13. ÚJÓLAG HANGSÚLYOZZA, hogy fontos felmérni, hogy hosszú távon szükség van-e a forgalombahozatali feltételek meghatározására is kiterjedő horizontális jogszabályra annak érdekében, hogy megoldás szülessen a csatlakoztatott eszközökkel kapcsolatos összes releváns kiberbiztonsági szempontra, például az elérhetőség, az integritás és a bizalmas jelleg. ÜDVÖZLI e tekintetben azt a megbeszélést, amelynek keretében feltérképezik majd az említett jogszabály hatályát és a kiberbiztonsági jogszabályban meghatározott kiberbiztonsági tanúsítási keretrendszerrel való kapcsolatait abból a célból, hogy növelni lehessen a biztonság szintjét a digitális egységes piacon. HANGSÚLYOZZA, hogy a kiberbiztonsági követelményeket a vonatkozó uniós jogszabályokkal, többek között a kiberbiztonsági jogszabállyal, az új jogszabályi kerettel, az európai szabványosításról szóló rendelettel és egy esetleges jövőbeli horizontális jogszabállyal összhangban kell meghatározni annak érdekében, hogy biztosítani lehessen az egyértelmű és egységes jogi szabályozást;

14. ELISMERI egy olyan átfogó és horizontális kiberbiztonsági megközelítés fontosságát az Unióban, amely teljes mértékben tiszteletben tartja a tagállamok hatásköreit és szükségleteit, valamint a technikai segítségnyújtás és együttműködés folyamatos támogatásának fontosságát a tagállamok kapacitásépítése érdekében. Figyelembe véve a kiberfenyegettségi helyzet alakulását, NYUGTÁZZA az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló új irányelvjavaslatot, amely a kiberbiztonsági irányelvre épül, és ismételten hangsúlyozza, hogy támogatja a nemzeti kiberbiztonsági keretek megerősítését és harmonizálását, valamint a tagállamok közötti tartós együttműködést. Továbbá HANGSÚLYOZZA, hogy ezen a területen szükség van az ágazati jogszabályok összehangolására és koherenciájára;

15. TUDOMÁSUL VESZI a Bizottság arra irányuló javaslatát, 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. Ezzel összefüggésben VÁRAKOZÁSSAL TEKINT a Bizottságnak a SOC-ok hálózatára vonatkozó – a tagállami hatásköröket tiszteletben tartó – részletes tervei elé. 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; VÁRAKOZÁSSAL TEKINT annak feltárása elé, – a hatékony, biztonságos és megbízható információmegosztási kultúra előmozdítása érdekében – hogy e hálózat milyen potenciállal rendelkezik a SOC-ok megerősítésére, valamint hogy mennyiben biztosított a meglévő hálózatokkal és szereplőkkel (elsősorban a CSIRT-hálózattal) való komplementaritása és koordinációja. HANGSÚLYOZZA, hogy ez a folyamat a mesterséges intelligenciával és a nagy teljesítményű számítástechnikával kapcsolatos kezdeményezések keretében, valamint az európai digitális innovációs központok által végzett munkára fog épülni.

16. TUDOMÁSUL VESZI az európai kvantumkommunikációs infrastruktúrára (EuroQCI) és az Európai Unió állami műholdas kommunikációjára (GOVSATCOM) épülő, biztonságos összeköttetési rendszer lehetséges kifejlesztését, és ELISMERI, hogy minden lehetséges jövőbeli fejlesztésnek szilárd kiberbiztonsági kereten kell alapulnia, és figyelembe kell vennie a teljes elektronikus hírközlési infrastruktúrát, például az űr-, a szárazföldi és a tengeralatti hálózati rendszereket.

17. VÁRAKOZÁSSAL TEKINT a Bizottsággal, az ENISA-val, a két uniós DNS gyökérszerver-üzemeltetővel és a több érdekelt felet tömörítő közösséggel folytatott megbeszélések elé, amelyek célja annak értékelése, hogy a két uniós DNS gyökérszerver-üzemeltető milyen szerepet játszik abban, hogy az internet globálisan hozzáférhető maradjon és ne legyen széttagolt. ÜDVÖZLI a Bizottságnak egy olyan globális internet-hozzáférést biztosító alternatív európai szolgáltatás (DNS4EU kezdeményezés) kidolgozására irányuló szándékával kapcsolatos további megbeszéléseket, amely a legújabb biztonsági, adatvédelmi, illetve beépített és alapértelmezett adatvédelmi szabványoknak és szabályoknak megfelelő átlátható modellen alapul, annak érdekében, hogy hozzájáruljon a reziliencia növeléséhez, miközben fenntartja és javítja a nemzetközi összeköttetéseket valamennyi tagállam számára;

18. ELISMERI, hogy a Bizottság és a tagállamok közös erőfeszítésére van szükség a kulcsfontosságú internetszabványok, köztük az IPv6 és a régóta használatos internetbiztonsági szabványok elterjedésének felgyorsítása érdekében, mivel ezek alapvető szerepet játszanak a globális internet általános biztonságának, rezilienciájának, nyitottságának és interoperabilitásának növelésében, miközben növelik az uniós iparnak és különösen az internetes infrastruktúra üzemeltetőinek versenyképességét;

19. HANGSÚLYOZZA a koordinált megközelítés, valamint az 5G hálózatok kiberbiztonságának megerősítésére irányuló hatékony nemzeti szintű intézkedések kidolgozásának és végrehajtásának fontosságát. TÁMOGATJA az 5G hálózatok kiberbiztonságával kapcsolatban teendő következő lépéseket, amelyeket az EU kiberbiztonsági stratégiájának függeléke tartalmaz, és amelyek az 5G hálózatok biztonságára vonatkozó bizottsági ajánlás hatásairól szóló jelentés eredményein alapulnak, például a teljes 5G értékláncra és ökoszisztémára kiterjedő hosszú távú és átfogó megközelítés meghatározása tekintetében. Az 5G hálózatok biztonságával kapcsolatos koordinált megközelítés további megerősítése érdekében arra SÜRGETI a tagállamokat, az uniós intézményeket és más érdekelt feleket, hogy folytassák az időszakos helyzetfelméréseket, valamint a Kiberbiztonsági Együttműködési Csoport 5G kiberbiztonsággal foglalkozó ágán belül cseréljenek információkat és osszák meg a legjobb gyakorlatokat, és rendszeresen tegyenek jelentést a Tanácsnak az elért eredményekről. KIEMELI, hogy miközben hangsúlyozza a tagállamok nemzetbiztonság védelméért viselt felelősségét, határozottan elkötelezett az uniós 5G eszköztár intézkedéseinek alkalmazása és végrehajtásának gyors befejezése, valamint az 5G hálózatok biztonságának garantálása és a jövőbeli hálózati generációk fejlesztése érdekében tett erőfeszítések folytatása iránt. A tagállamok, a Bizottság és az ENISA között az 5G hálózatok biztonságával kapcsolatban folyó szoros együttműködés példaként szolgálhat a kiberbiztonság területén felmerülő egyéb kérdések tekintetében, tiszteletben tartva ugyanakkor a tagállamok hatásköreit, valamint a szubszidiaritás és az arányosság elvét;

20. TUDATÁBAN VAN annak, hogy a kiberbiztonságot még jobban be kell építeni az uniós válságelhárítási mechanizmusokba, és hogy e mechanizmusokat gyakorlati tesztelésnek kell alávetni, valamint HANGSÚLYOZZA, hogy fokozni kell az együttműködést és az információmegosztást az EU-n belüli különböző kiberközösségek között, továbbá össze kell kapcsolni a meglévő kezdeményezéseket, struktúrákat és eljárásokat (mint például az IPCR, a CSIRT-hálózat, a Kiberbiztonsági Együttműködési Csoport, a CyCLONe, a Kiberbűnözés Elleni Európai Központ, az EU INTCEN és más érintett uniós szervek) a nagyszabású és határokon átnyúló kiberbiztonsági események és kiberveszélyek esetében. Figyelembe véve az e területen már elért eredményeket, ÉRDEKLŐDÉSSEL VÁRJA a közös kiberbiztonsági egység (JCU) kialakításának folyamatára, mérföldköveire és ütemtervére vonatkozó bizottsági javaslatot annak érdekében, hogy az hozzáadott értéket és egyértelmű fókuszt biztosítson és észszerűsítse az uniós kiberbiztonsági válságkezelési keretet, többek között a felkészültség, a közös helyzetismeret, valamint a koordinált reagálás és gyakorlatok megerősítése révén, átlátható és fokozatos módon, elkerülve ugyanakkor a párhuzamosságot és az átfedéseket, és tiszteletben tartva a tagállamok hatásköreit;

21. HANGSÚLYOZZA, hogy elő kell mozdítani az érintett kiberbiztonsági szereplők és az illetékes hatóságok – például a bűnüldöző és igazságügyi hatóságok – közötti együttműködést és információcserét a biztonság és a büntető igazságszolgáltatás területén, valamint hogy ki kell bővíteni és javítani kell e hatóságok kiberbűnözéssel kapcsolatos nyomozási és védeljárási kapacitásait, továbbá elő kell mozdítani az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférésre vonatkozó nemzetközi tárgyalásokat és uniós szabályokat. Elengedhetetlen, hogy a biztonsági és büntető igazságügyi hatóságoknak az aktuális technológiai környezettől függetlenül mindig módjukban álljon jogszerűen hozzáférni az ilyen adatokhoz feladataik ellátása keretében, törvényes felhatalmazásuknak megfelelően. A bűnüldözési jogköröket meghatározó jogszabályoknak minden esetben teljes mértékben tiszteletben kell tartaniuk a jogszerű eljárás követelményét és az egyéb biztosítékokat, csakúgy mint az alapvető jogokat, különösen a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogot, valamint a személyes adatok védelméhez fűződő jogot;

22. ÚJÓLAG MEGERŐSÍTI, hogy támogatja az erős titkosítás fejlesztését, bevezetését és alkalmazását, amely az egyének, az állam, az ipar és a társadalom alapvető jogainak és digitális biztonságának védelméhez szükséges eszköz, ugyanakkor ELISMERI, hogy biztosítani kell, hogy a biztonság és a büntető igazságszolgáltatás terén illetékes hatóságok – például a bűnüldöző és igazságügyi hatóságok – akár online, akár offline gyakorolni tudják törvényes hatásköreiket társadalmaink és polgáraink védelme érdekében. A kiberbiztonság garantálása mellett lehetővé kell tenni az illetékes hatóságok számára, hogy az alapvető jogok és a vonatkozó adatvédelmi jogszabályok teljes körű tiszteletben tartásával, jogszerűen és célzottan hozzáférjenek az adatokhoz. HANGSÚLYOZZA, hogy ezeket az érdekeket valamennyi meghozott intézkedés esetében gondosan egyensúlyba kell hozni a szükségesség, az arányosság és a szubszidiaritás elvével;

23. TÁMOGATJA és ELŐMOZDÍTJA a számítástechnikai bűnözésről szóló budapesti egyezményt, valamint az annak második kiegészítő jegyzőkönyvével kapcsolatos munkát. Ezen túlmenően továbbra is részt vesz a kiberbűnözéssel kapcsolatos többoldalú együttműködésben, többek között az Európa Tanáccsal, az ENSZ Kábítószer- és Bűnügyi Hivatalával (UNODC) és a Bűnmegelőzési és Büntető Igazságszolgáltatási Bizottsággal (CCPCJ) kapcsolatos folyamatokban, hogy ezáltal – az emberi jogok és az alapvető szabadságok tiszteletben tartása, előmozdítása és védelmezése mellett – fokozott nemzetközi együttműködésre kerüljön sor a kiberbűnözés elleni küzdelem terén, beleértve a legjobb gyakorlatok és a technikai ismeretek cseréjét, valamint a kapacitásépítés támogatását;

24. bár a nemzetbiztonság továbbra is az egyes tagállamok kizárólagos felelőssége marad, ELISMERI a kiberveszélyekre és a kibertevékenységekre vonatkozó stratégiai hírszerzési együttműködés fontosságát, és FELKÉRI a tagállamokat, hogy illetékes hatóságaikon keresztül továbbra is járuljanak hozzá az EU INTCEN-nek az Uniót érintő kiberkérdésekkel kapcsolatos helyzetismeret és fenyegetésértékelés központjaként végzett munkájához, és fontolják meg a tagállamok kiberhírszerzéssel foglalkozó munkacsoportjának abból a célból történő esetleges létrehozására irányuló javaslatot, hogy – a tagállami hatáskörök sérelme nélkül – erősödjenek az INTCEN erre a területre vonatkozó célzott kapacitásai a hírszerzési információknak a tagállamok általi önkéntes rendelkezésre bocsátásával;

25. KIEMELI, hogy átfogó, következetes és egységes szabályokon alapuló, szilárd és következetes biztonsági keretre van szükség valamennyi uniós alkalmazott, adat, kommunikációs hálózat és információs rendszer, valamint döntéshozatali folyamat védelme érdekében. Ezt mindenekelőtt az EU kiberveszélyekkel szembeni rezilienciájának fokozásával és biztonsági kultúrájának javításával, valamint a minősített és nem minősített uniós hálózatok biztonságának megerősítésével kell elérni, biztosítva ugyanakkor a megfelelő irányítást, valamint azt, hogy elegendő erőforrás és kapacitás álljon rendelkezésre, többek között a CERT-EU megbízatásának megerősítésével összefüggésben. ÜDVÖZLI e tekintetben az információbiztonságra vonatkozó közös szabályok létrehozásáról folyó megbeszéléseket, amelyek során kellően figyelembe veszik az EU-minősített adatok védelmét szolgáló tanácsi biztonsági szabályokat, valamint az összes uniós intézményre, szervre és ügynökségre vonatkozó közös, kötelező erejű kiberbiztonsági szabályok meghatározását;

26. az uniós kiberdiplomáciai erőfeszítésekre ÉPÍTVE VÁLLALJA, hogy növeli a kiberdiplomáciai eszköztár hatékonyságát és eredményességét, és VÁRAKOZÁSSAL TEKINT az elé, hogy az eszköz alkalmazása során eddig levont tanulságokra építve mélyrehatóbb megbeszélésekre kerüljön sor az eszköztár hatályára és felhasználására vonatkozóan. E megbeszéléseknek hozzá kell járulniuk a biztonság azáltal történő, nemzetközi szintű fokozásához, hogy előmozdítjuk a párbeszédet és a kiberbiztonsági kérdésekkel kapcsolatos közös elképzeléseket, megerősítjük a megelőzést, a stabilitást és az együttműködést, valamint fokozzuk a bizalmat és a kapacitásépítést, valamint szükség esetén korlátozó intézkedéseket alkalmazunk annak érdekében, hogy megelőzzük az EU és tagállamai integritását és biztonságát veszélyeztető, rossz szándékú kibertevékenységeket, visszatartsuk és elrettentsük a potenciális elkövetőket az ilyen tevékenységektől, illetve reagáljunk azokra, hozzájárulva ezáltal a nemzetközi biztonsághoz és stabilitáshoz, valamint megszilárdítva az EU kiberbiztonsági helyzetét, teljes mértékben tiszteletben tartva ugyanakkor a nemzeti hatásköröket és előjogokat. Különös figyelmet kell fordítani az olyan rendszerszintű hatású kibertámadások megelőzésére és leküzdésére, amelyek hatással lehetnek ellátási láncainkra, kritikus infrastruktúráinkra és alapvető szolgáltatásaikra, valamint demokratikus intézményeinkre és folyamatainkra, illetve alááshatják gazdasági biztonságunkat, ideértve a szellemi tulajdon kibertérben elkövetett eltulajdonítását is. A tagállamoknak és az uniós intézményeknek további megfontolás tárgyává kell tenniük az uniós kiberbiztonsági válságkezelési keret, a kiberdiplomáciai eszköztár, valamint az EUSZ 42. cikke (7) bekezdésének és az EUMSZ 222. cikkének rendelkezései közötti kapcsolatot, különösen olyan, forgatókönyveken alapuló munka révén, amelynek az EUSZ 42. cikke (7) bekezdésének végrehajtására vonatkozó gyakorlati szabályok közös értelmezésének kialakítását célozza;

27. TUDATÁBAN VAN annak, hogy fontos megerősíteni a nemzetközi szervezetekkel és a partnerországokkal folytatott együttműködést a kiberfenyegetettségi helyzet közös megismerésének előmozdítása, párbeszédek és együttműködési mechanizmusok kialakítása, adott esetben együttműködésen alapuló diplomáciai válaszintézkedések azonosítása, valamint az információmegosztás javítása érdekében, többek között oktatás, képzés és gyakorlatok révén. Ezzel összefüggésben HANGSÚLYOZZA, hogy a kiberbiztonság területére vonatkozó erős transzatlanti partnerség hozzájárul közös biztonságunkhoz, stabilitásunkhoz és jólétünkhöz, és NYUGTÁZZA az EU és az Egyesült Királyság közötti kereskedelmi és együttműködési megállapodásban foglalt, a kiberbiztonsági együttműködésre vonatkozó rendelkezéseket. Emlékeztetve a 2016. évi varsói és a 2018. évi brüsszeli együttes nyilatkozatok végrehajtása keretében a kiberbiztonság területén folytatott EU–NATO együttműködés fő eredményeire, ISMÉTELTEN HANGSÚLYOZZA annak fontosságát, hogy a két fél az átláthatóság, a kölcsönösség és az inkluzivitás elve alapján mélyreható, mindkettőjüket erősítő és kölcsönösen előnyös együttműködést folytasson oktatás, képzés, gyakorlatok és a rossz szándékú kibertevékenységekre való koordinált reagálás révén, teljes mértékben tiszteletben tartva mindkét szervezet döntéshozatali autonómiáját és eljárásait;

28. A globális, nyitott, szabad, stabil és biztonságos kibertérhez való hozzájárulás érdekében – amely egyre nagyobb jelentőséggel bír társadalmaink további jóléte, növekedése, biztonsága, jólléte, összekapcsoltsága és integritása szempontjából – VÁLLALJA, hogy folyamatosan részt vesz a nemzetközi szervezetek – különösen az ENSZ Első Bizottságához kapcsolódó folyamatok – keretében zajló normaalkotásban, valamint hogy előmozdítja a nemzetközi jog kibertérben való alkalmazását és a kibertérben tanúsított felelősségteljes állami magatartás normáinak, szabályainak és elveinek tiszteletben tartását és hozzájárul ezekhez, többek között azáltal, hogy előmozdítja a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó cselekvési program gyors kidolgozását, amely az ENSZ kormányzati szakértői csoportja (UN GGE) és nyitott munkacsoportja (OEWG) keretében jelenleg zajló folyamatok konstruktív, inkluzív és konszenzuson alapuló eredményeként jönne létre;

29. EMLÉKEZTET arra, hogy határozottan elkötelezett a hatékony multilateralizmus és a szabályokon alapuló globális rend mellett, amelynek középpontjában az Egyesült Nemzetek Szervezete áll, valamint hogy eltökélt szándéka megerősíteni az együttműködést és a koordinációt a nemzetközi és regionális szervezetekkel, nevezetesen az ENSZ-rendszerrel, a NATO-val, az Európa Tanáccsal, az EBESZ-szel, az AU-val, az Amerikai Államok Szervezetével (OAS), az ASEAN-nal, az ASEAN regionális fórummal (ARF), az ÖET-tel és az Arab Ligával egyrészt a kiberkérdésekről folytatott megbeszéléseket, másrészt pedig a harmadik országokkal folytatott strukturált uniós kiberpárbeszédek és -konzultációk folytatását és kiterjesztését illetően. HANGSÚLYOZZA, hogy aktívan támogatja az ENSZ-t, különösen a 2030-ig tartó időszakra szóló – a fenntartható fejlődési célokat is meghatározó – menetrenddel kapcsolatban, és ÜDVÖZLI az ENSZ főtitkárának a digitális együttműködésre vonatkozó ütemtervét és leszerelési programját, amelyek előmozdítják az elszámoltathatóságot és a normák betartását a kibertérben, valamint hozzájárulnak a kibertérben folytatott rossz szándékú tevékenységekből eredő konfliktusok megelőzéséhez, illetve békés rendezéséhez. ÜDVÖZLI a külügyi és biztonságpolitikai főképviselő arra irányuló javaslatát, hogy hozzanak létre egy informális uniós kiberdiplomáciai hálózatot az EU és a tagállamok nemzetközi kiberkérdésekkel kapcsolatos szerepvállalásának és szakértelmének fejlesztése céljából, a koordinált fellépés elősegítése érdekében;

30. VÁRAKOZÁSSAL TEKINT a kibervédelmi szakpolitikai keret (CDPF) felülvizsgálatára irányuló, a közeljövőben előterjesztendő javaslat elé, és VÁLLALJA, hogy folytatja a kiberbiztonsági és kibervédelmi dimenziók megerősítésére irányuló erőfeszítéseket annak biztosítása érdekében, hogy ezek teljes mértékben beépüljenek a biztonság és a védelem tágabb területébe, különösen a stratégiai iránytűvel kapcsolatos munkával összefüggésben. ÚGY VÉLI, hogy a kibertérrel mint műveleti területtel kapcsolatos, hamarosan bemutatandó katonai koncepció és stratégia hozzá fog járulni e megbeszélések továbbviteléhez. ÜDVÖZLI az Európai Védelmi Ügynökségnek (EVÜ) a katonai CERT-ek közötti együttműködés előmozdítására irányuló kezdeményezését, és TÁMOGATJA azokat az erőfeszítéseket, amelyek célja a kibervédelemmel és a kiberbiztonsággal kapcsolatos polgári-katonai szinergiáknak és – az űrrel kapcsolatos aspektusokra is kiterjedő – koordinációnak többek között célzott PESCO-projektek keretében történő fokozása;

31. ÜDVÖZLI az EU külső kiberkapacitás-építési menetrendjének kidolgozására irányuló javaslatot, az uniós kiberkapacitás-építési testület létrehozására irányuló javaslatot, valamint az EU CyberNet (az EU kiberkapacitás-építési hálózata) létrehozását és kiépítését, mivel ezek hozzá fognak járulni a kibertámadásokkal szembeni reziliencia és a kiberkapacitások világszerte történő növeléséhez. E tekintetben ÜDVÖZLI a tagállamokkal, valamint a köz- és magánszektorbeli partnerekkel, különösen a globális kiberszakértői fórummal (GFCE) és más érintett nemzetközi szervekkel folytatott együttműködést, amely hozzájárul a koordinációhoz és az átfedések elkerüléséhez. Ezzel összefüggésben együttműködést SZORGALMAZ a nyugat-balkáni partnerekkel, valamint az EU keleti és déli szomszédságának országaival;

32. Annak biztosítása érdekében, hogy valamennyi ország élvezhesse az internet és a technológiák használatának társadalmi, gazdasági és politikai előnyeit, VÁLLALJA, hogy – többek között az európai demokráciáról szóló cselekvési terv keretében tett erőfeszítésekkel összhangban – támogatja a partnerországokat a rossz szándékú kibertevékenységek jelentette növekvő kihívás kezelésében, különös tekintettel azon tevékenységekre, amelyek károsak ezen országok gazdaságának és társadalmának fejlődésére, valamint a demokratikus rendszerek integritására és biztonságára nézve;

33. Az EU kiberbiztonsági stratégiájában előterjesztett javaslatok kidolgozásának, végrehajtásának és nyomon követésének biztosítása érdekében, valamint figyelembe véve egyes kezdeményezések többéves jellegét, arra ÖSZTÖNZI a Bizottságot és az Unió külügyi és biztonságpolitikai főképviselőjét, hogy dolgozzanak ki olyan részletes végrehajtási tervet, amely meghatározza a prioritásokat és a tervezett intézkedések ütemezését. FIGYELEMMEL FOGJA KÍSÉRNI az e következtetések végrehajtása terén elért eredményeket egy olyan cselekvési terv révén, amelyet a Tanács az Európai Bizottsággal és a főképviselővel szoros együttműködésben rendszeresen felül fog vizsgálni és frissíteni fog.