Európai Parlament
2014-2019

ELFOGADOTT SZÖVEGEK

P8_TA(2017)0366

A kiberbűnözés elleni küzdelem

Az Európai Parlament 2017. október 3-i állásfoglalása a kiberbűnözés elleni küzdelemről (2017/2068(INI))

Az Európai Parlament,

– tekintettel az Európai Unióról szóló szerződés (EUSZ) 2., 3. és 6. cikkére,

– tekintettel az Európai Unió működéséről szóló szerződés (EUMSZ) 16., 67., 70., 72., 73., 75., 82., 83., 84., 85., 87. és 88. cikkére,

– tekintettel az Európai Unió Alapjogi Chartájának 1., 7., 8., 11., 16., 17., 21., 24., 41., 47., 48., 49., 50. és 52. cikkére,

– tekintettel a gyermek jogairól szóló, 1989. november 20-i ENSZ-egyezményre,

– tekintettel a gyermekek eladásáról, a gyermekprostitúcióról és a gyermekpornográfiáról szóló, a gyermek jogairól szóló egyezményhez fűzött, 2000. május 25-i fakultatív jegyzőkönyvre,

– tekintettel a gyermekek kereskedelmi célú szexuális kizsákmányolása elleni 1. világkongresszus által elfogadott stockholmi nyilatkozatra és cselekvési tervre, a gyermekek kereskedelmi célú szexuális kizsákmányolása elleni 2. világkongresszus által elfogadott jokohamai globális kötelezettségvállalásra, valamint a gyermekek kereskedelmi célú szexuális kizsákmányolása elleni 2. világkongresszus előkészítő konferenciáján elfogadott budapesti kötelezettségvállalásra és cselekvési tervre,

– tekintettel az Európa Tanácsnak a gyermekek szexuális kizsákmányolással és szexuális visszaéléssel szembeni védelméről szóló, 2007. október 25-i egyezményére,

– tekintettel „A gyermekek védelme a digitális világban” című, 2012. november 20-i állásfoglalására[1],

– tekintettel a gyermekekkel szemben elkövetett internetes szexuális visszaélésről szóló, 2015. március 11-i állásfoglalására[2],

---

1 HL C 419., 2015.12.16., 33. o.
2 HL C 316., 2016.8.30., 109. o.

– tekintettel a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló, 2001. május 28-i 2001/413/IB tanácsi kerethatározatra[1],

– tekintettel a számítástechnikai bűnözésről szóló, 2001. november 23-i Budapesti Egyezményre[2] és az ahhoz csatolt kiegészítő jegyzőkönyvre,

– tekintettel az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló, 2004. március 10-i 460/2004/EK európai parlamenti és tanácsi rendeletre[3],

– tekintettel az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvre[4],

– tekintettel az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelvre[5],

– tekintettel a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról szóló, 2011. december 13-i 2011/93/EU európai parlamenti és a tanácsi irányelvre[6],

– tekintettel „Az Európai Unió kiberbiztonsági stratégiája: nyílt, megbízható és biztonságos kibertér” című (JOIN(2013)0001), az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának címzett, a Bizottság és a Bizottság alelnöke/az Unió külügyi és biztonságpolitikai főképviselője által kiadott, 2013. február 7-i közös közleményre,

– tekintettel az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló, 2013. augusztus 12-i 2013/40/EU európai parlamenti és tanácsi irányelvre[7],

– tekintettel a büntetőügyekben kibocsátott európai nyomozási határozatról szóló, 2014. április 3-i 2014/41/EU európai parlamenti és tanácsi irányelvre[8] (ENYH-irányelv),

– tekintettel az Európai Unió Bíróságának (EUB) 2014. április 8-i ítéletére[9], amely érvénytelenítette az uniós adatmegőrzési irányelvet,

– tekintettel 2013. szeptember 12-i, „az Európai Unió kiberbiztonsági stratégiája: nyílt, megbízható és biztonságos kibertér” témájú állásfoglalására[10],

---

1 HL L 149., 2001.6.2., 1. o.
2 Európa Tanács, Európai szerződések sorozat, 185. szám, 2001.11.23.
3 HL L 77., 2004.3.13., 1. o.
4 HL L 345., 2008.12.23., 75. o.
5 HL L 201., 2002.7.31., 37. o.
6 HL L 335., 2011.12.17., 1. o.
7 HL L 218., 2013.8.14., 8. o.
8 HL L 130., 2014.5.1., 1. o.
9 ECLI:EU:C:2014:238.
10 HL C 93., 2016.3.9., 112. o.

– tekintettel a Bizottság „Európai digitális egységes piaci stratégia” című, 2015. május 6-i közleményére (COM(2015)0192),

– tekintettel „Az európai biztonsági stratégia” című, 2015. április 28-i bizottsági közleményre (COM(2015)0185), illetve az azt követő, „A hatékony és valódi biztonsági unió megvalósítása” című eredményjelentésre,

– tekintettel a kibertérben gyakorolt joghatóságról 2016. március 7-én és 8-án Amszterdamban tartott konferenciáról szóló jelentésre,

– tekintettel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendeletre (általános adatvédelmi rendelet)[1],

– tekintettel a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelvre[2],

– tekintettel a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol) szóló, 2016. május 11-i (EU) 2016/794 európai parlamenti és tanácsi rendeletre[3],

– tekintettel a Bizottság 2016. július 5-i határozatára a Bizottság által képviselt Európai Unió és az érdekelt szervezetek közötti, kiberbiztonsági ipari kutatás és innováció témájú köz-magán társulásra vonatkozó szerződéses megállapodás aláírásáról (C(2016)4400),

– tekintettel a Bizottság és a Bizottság alelnöke/ az Unió külügyi és biztonságpolitikai főképviselője „A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz” című, az Európai Parlamentnek és a Tanácsnak címzett, 2016. április 6-i közös közleményére (JOIN(2016)0018),

– tekintettel a gyermekbarát internet európai stratégiájára (COM(2012)0196) és a Bizottság 2016. június 6-i, Az internetet és egyéb kommunikációs technológiákat használó gyermekek védelmére irányuló többéves uniós program végső értékelése (biztonságosabb internet) című jelentésére (COM(2016)0364),

– tekintettel az Europol és az ENISA 2016. május 20-i közös nyilatkozatára a 21. századi adatvédelmet tiszteletben tartó jogszerű bűnügyi nyomozásról,

– tekintettel a Tanács 2016. június 9-i, a számítástechnikai bűnözés elleni európai igazságügyi hálózatról szóló következtetéseire,

---

1 HL L 119., 2016.5.4., 1. o.
2 HL L 119., 2016.5.4., 89. o.
3 HL L 135., 2016.5.24., 53. o.

– tekintettel a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelvre[1],

– tekintettel az ENISA 2016. decemberi „Titkosítás – Az erős titkosítás védi digitális identitásunkat” című véleményére,

– tekintettel az Európa Tanács számítástechnikai bűnözésről szóló egyezménnyel foglalkozó bizottságának a felhőben található bizonyítékokkal foglalkozó csoportja (Cloud Evidence Group) által kiadott „A büntető igazságszolgáltatás hozzáférése a felhőben található elektronikus bizonyítékokhoz: a T-CY ajánlásai” című, 2016. szeptember 16-i végleges jelentésre,

– tekintettel a Számítástechnikai Bűnözés Elleni Közös Akció Munkacsoport (J-CAT) tevékenységére,

– tekintettel a súlyos és szervezett bűnözés általi fenyegetettség értékeléséről (EU SOCTA) szóló, 2017. február 28-i, illetve az internetes szervezett bűnözés általi fenyegetettség értékeléséről (IOCTA) szóló, 2016. szeptember 28-i Europol-jelentésekre,

– tekintettel az EUB a C-203/15. számú ügyben hozott, 2016. december 21-i ítéletére (TELE2 ítélet)[2],

– tekintettel az Európai Parlament és a Tanács 2017. március 15-i (EU) 2017/541 irányelvére a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról[3],

– tekintettel eljárási szabályzata 52. cikkére,

– tekintettel az Állampolgári Jogi, Bel- és Igazságügyi Bizottság jelentésére és a Belső Piaci és Fogyasztóvédelmi Bizottság véleményére (A8-0272/2017),

A. mivel a kiberbűnözés egyre jelentősebb társadalmi és gazdasági károkat okoz, ami sérti az egyének alapvető jogait, illetve veszélyt jelent a jogállamiságra a kibertérben és a demokratikus társadalmak stabilitására egyaránt;

B. mivel a kiberbűnözés egyre nagyobb probléma a tagállamokban;

C. mivel a 2016-os IOCTA rávilágított arra, hogy folyamatosan növekszik kiberbűnözés intenzitása, összetettsége és mértéke, hogy egyes uniós tagállamokban a bejelentett számítógépes bűncselekmények száma meghaladja a hagyományos bűncselekményekét, hogy a kiberbűnözés a bűnözés egyéb területeire is kiterjed, például az emberkereskedelemre, hogy terjed a titkosításra és anonimizálásra szolgáló eszközök bűnözési célokra való felhasználása, és hogy a zsarolóvírus-támadások száma

---

1 HL L 194., 2016.7.19., 1. o.

2 A Bíróság 2016. december 21-én hozott ítélete a *Tele2 Sverige AB* kontra *Post- och telestyrelsen* és a *Secretary of State for the Home Department kontra Tom Watson és társai* ügyben, C-203/15, ECLI:EU:C:2016:970.

3 HL L 88., 2017.3.31., 6. o.

meghaladja a rosszindulatú számítógépes programok hagyományos fajtáival, például trójai programmal elkövetett támadások számát;

D. mivel az Európai Bizottság szerverei elleni támadások 2016-ra 20%-kal nőttek a 2015. évhez képest;

E. mivel a számítógépek támadásokkal szembeni kiszolgáltatottsága egyrészt az információtechnológia elmúlt évekbeli sajátos fejlődéséből, másrészt az online vállalkozások növekedéséből és a kormányzati fellépés hiányából ered;

F. mivel a számítógépes zsarolás, a felbérelt zombihálózatok és hackertámadások, valamint a lopott digitális termékek feketepiaca egyre nő;

G. mivel a kibertámadások fő formája továbbra is az olyan vírusok, mint a banki trójai programok, azonban egyre nő az ipari vezérlőrendszerek és hálózatok elleni támadások száma és hatása is, aminek célja a létfontosságú infrastruktúrák, gazdasági szerkezetek megsemmisítése és társadalmak destabilizációja, mint például a 2017 májusában bekövetkezett WannaCry zsarolóvírus-támadás esetében, ennélfogva ezek egyre nagyobb fenyegetést jelentenek a biztonságra, védelemre és egyéb fontos ágazatokra nézve; mivel a nemzetközi bűnüldöző hatóságok adatkéréseinek többsége csalásokhoz és pénzügyi bűncselekményekhez köthető, megelőzve az erőszakos és súlyos bűncselekményeket;

H. mivel bár az emberek, helyek és tárgyak folyamatosan fejlődő összekapcsoltsága számos előnnyel jár, fokozza a kiberbűnözés kockázatát; mivel a dolgok internetéhez kapcsolódó eszközök, például az intelligens hálózatok, hálózatba kapcsolt hűtőgépek, orvosi eszközök vagy segédeszközök, gyakran nem olyan jól védettek, mint a hagyományos internetes eszközök, ezért ideális célpontként szolgálnak a kiberbűnözők számára, különösen mivel a hálózatba kapcsolt eszközökre vonatkozó biztonsági frissítések gyakran hiányosak, néha pedig teljes mértékben elmaradnak; mivel a hackertámadás áldozatául esett, dolgok internetéhez kapcsolódó azon eszközök, amelyek fizikai aktuátorokkal is rendelkeznek, vagy fizikai aktuátorokat tudnak irányítani, konkrétan veszélyeztethetik az emberek életét;

I. mivel az adatvédelem hatékony jogi kerete elengedhetetlen az online világba vetett bizalom építéséhez, mivel egyszerre teszi lehetővé a fogyasztóknak és a vállalkozásoknak, hogy teljes mértékben kihasználhassák a digitális egységes piac előnyeit és kezelhessék a kiberbűnözést;

J. mivel a vállalkozások nem tudnak megbirkózni a hálózatba kapcsolt világ biztonságosabbá tételével, és a kormányzatnak rendeletekkel és a felhasználók biztonságosabb viselkedését elősegítő ösztönzőkkel hozzá kellene járulnia a kiberbiztonsághoz;

K. mivel a kiberbűnözés, a kiberkémkedés, a kiberhadviselés, a kiberszabotázs és a kiberterrorizmus közötti válaszvonal egyre homályosabb; mivel a kiberbűnözés egyformán célba vehet egyéneket és köz- vagy magánszervezeteket, és bűncselekmények széles skáláját ölelheti fel, ideértve a magánélet megsértését, a gyermekek online szexuális bántalmazását, az erőszakra és a gyűlöletre való nyilvános uszítást, a szabotázst, a kémkedést, a pénzügyi bűncselekményeket és csalásokat,

többek között fizetési csalásokat, lopást, személyazonosság-lopást, illetve az informatikai rendszereket érintő jogellenes beavatkozást;

L. mivel a Világgazdasági Fórum globális kockázatokról szóló 2017. évi jelentése a tömeges adatcsalást és -lopást az öt legfontosabb globális kockázat közé sorolja a valószínűség szempontjából;

M. mivel a számítógépes bűncselekmények jelentős része büntetlenül marad; mivel még mindig nagyon alacsony a bejelentési arány, hosszú az észlelési idő, ami lehetővé teszi a kiberbűnözők számára több belépési és kilépési pont vagy hátsó ajtó létrehozását, nehéz az e-bizonyítékokhoz való hozzáférés és azok begyűjtése és bírósági felhasználása, valamint a kiberbűnözés határokon átívelő természetéből adódó összetett eljárások és joghatósági kihívások állnak fenn;

N. mivel a Tanács 2016. júniusi következtetéseiben kiemelte, hogy a kiberbűnözés határokon átnyúló természete és az Uniót érő közös kiberbiztonsági fenyegetések miatt a rendőri és igazságügyi hatóságok és a számítógépes bűncselekményekkel foglalkozó szakértők közötti együttműködés elengedhetetlen ahhoz, hogy eredményes nyomozást folytassanak a kibertérben és begyűjtsék az elektronikus bizonyítékokat;

O. mivel az EUB-nak az adatmegőrzési irányelv érvénytelenítésére vonatkozó 2014. április 8-i ítélete és az EUB az adatok általános és különbségtétel nélküli megőrzésének tiltását megerősítő 2016. december 21-i TELE2-ítélete szigorú korlátokat szab a távközlési adatok tömeges kezelésének, valamint az illetékes hatóságok adatokhoz való hozzáférésének;

P. mivel az EUB Max Schrems-ítélete[1] kiemeli, hogy a tömeges megfigyelés az alapvető jogok megsértése;

Q. mivel a kiberbűnözés elleni küzdelemnek ugyanazokat az eljárási és anyagi biztosítékokat, valamint alapvető jogokat – nevezetesen az adatvédelmet és a szólásszabadságot – kell tiszteletben tartania, mint más területek bűncselekményei elleni küzdelemnek;

R. mivel a gyerekek egyre fiatalabb korban kezdik használni az internetet, és különösen kiszolgáltatottak az online csábítás és az online szexuális kizsákmányolás egyéb formáival (az internetes zaklatással, szexuális erőszakkal, szemérem elleni erőszakkal és zsarolással), a személyes adatok hűtlen kezelésével, valamint az olyan veszélyes kampányokkal szemben, amelyek az önkárosítás különböző formáinak népszerűsítését célozzák – mint a „kék bálna” esetében, és ezért különleges védelemre szorulnak; mivel az internetes bűnözők gyorsabban megtalálják és magukhoz csábítják az áldozatokat a csevegőszobák, e-mailek, online játékok és közösségi hálózati oldalak segítségével, és a rejtett fájlcserélő („peer-to-peer”) hálózatok jelentik továbbra is a gyermekek elleni szexuális bűncselekményeket elkövetők számára a gyermekek szexuális kizsákmányolásával kapcsolatos anyagok hozzáférésének, kommunikációjának, tárolásának és megosztásának fő színtereit;

[1] ECLI:EU:C:2015:650.

S. mivel a szemérem elleni erőszak és a zsarolás növekvő tendenciáját továbbra is kevéssé vizsgálják és kevés bejelentés érkezik ilyen cselekményekről, főleg a bűncselekmény természeténél fogva, az áldozatok által érzett szégyen és bűntudat miatt;

T. mivel az egyenes adásban közvetített gyermekbántalmazás a jelentések szerint egyre növekvő veszély; mivel az egyenes adásban közvetített gyermekbántalmazás nyilvánvalóan kapcsolatba hozható a gyermekek szexuális kizsákmányolását ábrázoló anyagok kereskedelmi forgalmazásával;

U. mivel a brit Nemzeti Bűnüldözési Hivatal tanulmánya megállapította, hogy a hackertevékenységekkel foglalkozó fiatalokat nem igazán a pénz hajtja, hanem gyakran azért támadnak meg számítógépes hálózatokat, hogy kivívják barátaik elismerését vagy hogy próbára tegyenek egy politikai rendszert;

V. mivel a kiberbűnözés veszélyei iránti tudatosság ugyan nőtt, azonban az egyének, a közintézmények és a gazdálkodási szervezetek részéről egyaránt továbbra is teljességgel elégtelenek az elővigyázatossági intézkedések, főleg a tudás és a források hiánya miatt;

W. mivel a kiberbűnözés és a jogellenes online tevékenységek elleni küzdelem nem homályosíthatja el a szabad és nyílt kibertér pozitív aspektusait, amelyek új lehetőségeket nyitnak a tudásmegosztás, valamint a politikai és szociális integráció elősegítése előtt világszerte;

Általános megfontolások

1. hangsúlyozza, hogy a zsarolóvírus-támadások számában, a zombihálózatok használatában és a számítógépes rendszerek jogosulatlan károsításának számában bekövetkezett éles növekedés hatással van az egyének biztonságára, személyes adataik elérhetőségére és integritására, valamint a magánélet és az alapvető szabadságjogok védelmére és a kritikus jelentőségű – többek között, de nem kizárólag az energiához és a villamosenergia-ellátáshoz, valamint a pénzügyi struktúrákhoz, például az értéktőzsdéhez kapcsolódó – infrastruktúra integritására is; ezzel kapcsolatban emlékeztet arra, hogy a kiberbűnözés elleni küzdelem a 2015. április 28-i európai biztonsági stratégia egyik prioritása;

2. hangsúlyozza, hogy egységesíteni kell a kiberbűnözés, kiberhadviselés, kiberbiztonság, kiberzaklatás és kibertámadás közös meghatározásait annak érdekében, hogy az uniós intézmények és az uniós tagállamok egységes jogi meghatározással rendelkezzenek;

3. hangsúlyozza, hogy a kiberbűnözés elleni küzdelem céljának elsősorban és leginkább a kritikus jelentőségű infrastruktúrák és hálózatba kapcsolt egyéb eszközök védelmének és erősítésének, nem csupán megtorló intézkedések kidolgozásának kell lennie;

4. ismételten hangsúlyozza azon európai szintű jogi intézkedések jelentőségét, melyeknek célja az információs rendszerek elleni támadásokhoz vagy a gyermekek online szexuális bántalmazásához és kizsákmányolásához kapcsolódó bűncselekmények definícióinak harmonizációja, valamint a tagállamok kötelezése egy olyan rendszer létrehozására, amely az említett bűncselekményekre vonatkozó statisztikai adatokat rögzíti, előállítja és elérhetővé teszi a bűncselekmények elleni küzdelmet célzó hatékony fellépés érdekében;

5. nyomatékosan kéri azokat a tagállamokat, amelyek még nem tették meg, hogy sürgősen és megfelelően ültessék át és hajtsák végre a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelvet; kéri a Bizottságot, hogy szigorúan ellenőrizze és biztosítsa a 2004/68/IB tanácsi kerethatározatot felváltó nevezett irányelv maradéktalan és hatékony végrehajtását, és megfelelő időben készítsen jelentést a megállapításairól a Parlament és az illetékes bizottsága számára; hangsúlyozza, hogy az Eurojust és az Europol számára megfelelő erőforrásokat kell biztosítani az áldozatok jobb azonosítása, a szexuális erőszak elkövetőinek szervezett hálózata elleni küzdelem, illetve a gyermekek bántalmazását ábrázoló anyagok online és offline kiszűrése, elemzése és továbbküldése céljából;

6. sajnálja, hogy Európában a vállalkozások 80%-a tapasztalt már legalább egy kiberbiztonsági incidenst, és hogy a vállalatok elleni kibertámadások gyakran észrevétlenek maradnak vagy nem kerülnek bejelentésre; emlékeztet arra, hogy számos tanulmány becslése szerint a kibertámadások éves költsége jelentős a világgazdaság szempontjából; úgy véli, hogy a vállalkozásoknak, különösen a kkv-knak nyújtott támogatás révén segíthet a probléma megoldásában a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló (EU) 2016/679 rendelet (az általános adatvédelmi rendelet) és a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 irányelv (a hálózati és információs rendszerek biztonságáról szóló (NIS) irányelv) által bevezetett kötelezettség, mely szerint a biztonság megsértését minden esetben jelenteni kell és meg kell osztani a kockázatokkal kapcsolatos információkat;

7. hangsúlyozza, hogy a kiberfenyegetés helyzetének folyamatosan változó természete minden érdekelt felet komoly jogi és technológiai kihívások elé állít; úgy véli, hogy az új technológiákban rejlő lehetőségeket nem szabad fenyegetésnek tekinteni, és elismeri, hogy a titkosítási technológiák fejlődése javítja informatikai rendszereink általános biztonságát, többek között azáltal, hogy lehetővé teszi a végfelhasználók adatainak és kommunikációjának hatékonyabb védelmét; rámutat ugyanakkor, hogy továbbra is jelentős hiányosságok tapasztalhatóak a kommunikáció biztosítása terén és hogy az onion-routinghoz (hagyma-elosztáshoz) és a rejtett hálózatokhoz hasonló technikákat rosszindulatú felhasználók, például terroristák és gyermekek elleni szexuális bűncselekményeket elkövetők, nem baráti államok, illetve szélsőséges politikai vagy vallási csoportok által támogatott hackerek bűnözési célokra használhatják fel, és e technológiák segítségével rejthetik el jogsértő tevékenységüket és személyazonosságukat, súlyosan hátráltatva a nyomozásokat;

8. mélységesen aggasztja a közelmúltbeli globális zsarolóvírus-támadás, amely a jelek szerint több tízezer számítógépet érintett közel 100 országban és számos szervezetnél, beleértve az Egyesült Királyság Nemzeti Egészségügyi Szolgálatát (NHS), a kiterjedt vírustámadás legnagyobb figyelmet felkeltő áldozatát; ezzel összefüggésben felismeri, mennyire fontos munkát végez a No More Ransom (NMR) kezdeményezés, amely 40 különböző visszafejtő eszközt biztosít, lehetővé téve világszerte a zsarolóvírus-támadások áldozatainak, hogy visszafejtsék érintett eszközeik titkosítását;

9. hangsúlyozza ugyanakkor, hogy a rejtett hálózatok és az onion-routing teret ad újságírók, politikai aktivisták és emberijog-védők számára bizonyos országokban az elnyomó államhatalom figyelmének elkerülésére;

10. megjegyzi, hogy a bűnözői- és terroristahálózatok egyelőre csak korlátozott mértékben folyamodnak kiberbűnözési eszközökhöz; kiemeli azonban, hogy ez a valószínűleg változni fog a terrorizmus és a szervezett bűnözés közötti erősödő kapcsolat, illetve a lőfegyverek és robbanóanyag-prekurzorok rejtett hálózaton történő elérhetőségének fényében;

11. határozottan elítéli az informatikai rendszerek elleni összes olyan beavatkozást, amelyet egy ország demokratikus folyamatainak megzavarása céljából végez vagy irányít egy külföldi állam vagy annak ügynökei;

12. hangsúlyozza, hogy a domének lefoglalására, tartalmak eltávolítására és a felhasználói adatokhoz való hozzáférésre vonatkozó, határokon átívelő kérelmek komoly kihívást jelentenek és hatalmas tétjük miatt sürgős intézkedést kívánnak; ezzel összefüggésben hangsúlyozza, hogy az online és offline egyaránt érvényes nemzetközi emberi jogi keretek jelentős globális mércét képviselnek;

13. felhívja a tagállamokat annak biztosítására, hogy az egyes kibertámadások áldozatai teljes mértékben élhessenek a 2012/29/EU irányelvben foglalt valamennyi joggal, és hogy fokozzák az áldozatazonosítással és áldozatok támogatására összpontosító szolgáltatásokkal kapcsolatos erőfeszítéseiket és továbbra is támogassák az Europol áldozatok azonosításával foglalkozó munkacsoportját; felhívja a tagállamokat, hogy az Europollal együttműködve sürgősen hozzanak létre kapcsolódó platformokat annak biztosítása érdekében, hogy minden internet-felhasználó tudja, hogyan kérjen segítséget, ha illegális támadás éri online; felhívja a Bizottságot, hogy tegyen közzé tanulmányt a határokon átívelő kiberbűnözés következményeiről a 2012/29/EU irányelv alapján;

14. kiemeli, hogy a 2014-es Europol IOCTA szerint a kölcsönös jogsegély-megállapodás (Mututal Legal Assistance Treaty – MLAT) folyamatának jelenlegi korlátozásaira való tekintettel hatékonyabb és hatásosabb jogi eszközökre, valamint a jogszabályok további uniós harmonizációjára van szükség bizonyos területeken;

15. kiemeli, hogy a kiberbűnözés súlyosan aláássa a digitális egységes piac működését, mivel csökkenti a digitális szolgáltatók iránti bizalmat, aláássa a határokon átívelő ügyleteket és súlyosan sérti a digitális szolgáltatások fogyasztóinak érdekeit;

16. hangsúlyozza, hogy a kiberbiztonsági stratégiák és intézkedések csak akkor lehetnek hatékonyak és eredményesek, ha összhangban vannak az Európai Unió Alapjogi Chartájában foglalt alapvető jogokkal és szabadságokkal, valamint az Unió alapértékeivel;

17. hangsúlyozza, hogy jogos és jelentős szükség mutatkozik az egyének közötti, valamint az egyének és köz- vagy magánintézmények közötti kommunikáció védelmezésére a kiberbűnözés megelőzése érdekében; kiemeli, hogy az erős kriptográfia képes kielégíteni ezt a szükségletet; hangsúlyozza továbbá, hogy a kriptográfiai eszközök alkalmazásának korlátozása vagy azok gyengítése bűnözői visszaéléseknek helyt adó sebezhetőségeket fog teremteni, valamint csökkenteni fogja az elektronikus szolgáltatások iránti bizalmat, ami káros hatással lesz a civil társadalomra és az ágazatra egyaránt;

18. kéri a gyermekek jogainak a kibertérben való online és offline védelmére vonatkozó cselekvési terv kidolgozását, és emlékeztet arra, hogy a bűnüldöző hatóságoknak a

kiberbűnözés ellen folytatott küzdelemben különös figyelmet kell szentelniük a gyermekek elleni bűncselekményeknek; hangsúlyozza ezzel összefüggésben, hogy meg kell erősíteni az igazságszolgáltatási és rendőrségi együttműködést a tagállamok között, valamint az Europollal és annak Számítástechnikai Bűnözés Elleni Európai Központjával (EC3) a kiberbűnözésnek és különösen a gyermekek online szexuális kizsákmányolásának a megakadályozása, valamint az azok ellen folytatott küzdelem céljából;

19. sürgeti a Bizottságot és a tagállamokat, hogy hozzanak meg minden szükséges jogi és bírósági intézkedést a nőkkel szemben elkövetett online erőszak és az internetes erőszak elleni küzdelem érdekében; elsősorban arra kéri az Uniót és a tagállamokat, hogy egyesítsék erőiket, és alakítsanak ki egy olyan bűnüldözési keretet, amely arra kötelezi az online vállalatokat, hogy töröljék a lealacsonyító, sértő és megalázó tartalmakat, és akadályozzák meg ezek terjesztését; azt kéri továbbá, hogy nyújtsanak pszichológiai támogatást az online erőszak női áldozatai, valamint az internetes zaklatástól szenvedő lányok számára;

20. hangsúlyozza, hogy az illegális online tartalmat megfelelő jogi eljárás révén haladéktalanul el kell távolítani; felhívja a figyelmet az infokommunikációs technológiáknak, az internetszolgáltatóknak és az internetes tárhelyszolgáltatóknak az illegális online tartalmak gyors és hatékony, az illetékes bűnüldöző hatóság kérésére történő eltávolításában játszott szerepére;

Megelőzés

21. felszólítja a Bizottságot, hogy az európai kiberbiztonsági stratégia felülvizsgálatának vonatkozásában folytassa a kritikus európai infrastruktúra hálózati és információs sebezhetőségeinek azonosítását és a reziliens rendszerek fejlesztésének ösztönzését, valamint értékelje ki a kiberbűnözés elleni uniós és tagállami küzdelem helyzetét, elősegítve a kibertér bűncselekményeihez köthető tendenciák változásának jobb megértését;

22. hangsúlyozza, hogy a számítógépes támadások elleni reziliencia kulcsfontosságú, ezért annak a legmagasabb prioritást kell élveznie; felszólítja a tagállamokat, hogy fogadjanak el proaktív szakpolitikákat és intézkedéseket a hálózatok és a kritikus infrastruktúra védelmében, valamint olyan átfogó európai megközelítést kér a kiberbűnözés elleni küzdelemben, ami összeegyeztethető az alapvető jogokkal, az adatvédelemmel, a kiberbiztonsággal, a fogyasztóvédelemmel és az e-kereskedelemmel;

23. ezzel összefüggésben üdvözli, hogy az Európai Unió támogatási forrásokat nyújt a kiberbiztonsági köz-magán társuláshoz (kiberbiztonsági köz-magán társulás) hasonló kutatási projektekhez, innováción és kapacitásbővítésen keresztül növelve a számítógépes támadások elleni rezilienciát Európában; elismeri különösen a köz- és magánszféra közötti kiberbiztonsági partnerség erőfeszítéseit a nulladik napi sebezhetőségek kezelését célzó, megfelelő válaszlépések kialakítására;

24. hangsúlyozza e tekintetben az ingyenes és nyílt forráskódú szoftverek fontosságát; kéri, hogy az informatikai biztonság területe több uniós forrást kapjon kifejezetten az ingyenes és nyílt forráskódú szoftverek fejlesztésére;

25. aggodalommal állapítja meg, hogy több képzett informatikai szakemberre lenne szükség a kiberbiztonság területén; sürgeti a tagállamokat, hogy fektessenek be az oktatásba;

26. úgy véli, hogy a szabályozásnak jelentősebb szerepet kellene játszania a kiberbiztonsági kockázatok kezelésében a tervezésre és a későbbi frissítésekre vonatkozó, hatékonyabb termék- és szoftverszabványokon keresztül, valamint az alapértelmezett felhasználónevekre és jelszavakra vonatkozó minimumszabályok lefektetése által;

27. sürgeti a tagállamokat, hogy fokozzák az Eurojuston, az Europolon és az ENISA-n keresztül folytatott információcserét, valamint a legjobb gyakorlatok megosztását az európai CSIRT (számítógépes biztonsági eseményekre reagáló csoport) hálózaton és a CERT-eken (hálózatbiztonsági vészhelyzeteket elhárító csoport) keresztül a kiberbűnözés elleni harc kihívásaival kapcsolatban, valamint az e problémák kezelésére szolgáló konkrét jogi és technikai megoldásokról és a kibertámadásokkal szembeni ellenálló képesség megerősítése érdekében; ezzel összefüggésben felszólítja a Bizottságot, hogy a kiberbiztonsági irányelvvel összhangban mozdítsa elő az eredményes együttműködést, valamint segítse az információcserét a lehetséges kockázatok előrejelzése és kezelése céljából;

28. aggodalmának ad hangot az Europol azon megállapításai kapcsán, melyek szerint az egyéneket érő sikeres támadások többsége a digitális higiénia és a felhasználói tudatosság hiánya, illetve a technikai biztonsági intézkedésekre – pl. beépített biztonság – fordított figyelem elégtelensége miatt következik be; kiemeli, hogy a nem megfelelően biztosított hardverek és szoftverek elsődleges áldozatai a felhasználók;

29. kéri a Bizottságot és a tagállamokat, hogy minden releváns szereplő és érdekelt fél bevonásával indítsanak figyelemfelkeltő kampányt azzal a céllal, hogy felvilágosítsák a gyermekeket és támogassák a szülőket, gondozókat és oktatókat az online kockázatok megértésében és kezelésében, valamint a gyermekek online védelmének biztosításában, továbbá, hogy támogassák a tagállamokat a gyermekekkel szemben elkövetett internetes szexuális visszaélés megelőzésére irányuló programok beindításában, előmozdítsák a közösségi médiában való felelősségteljes magatartásra vonatkozó figyelemfelhívó kampányokat, valamint ösztönözzék a fő keresőprogramokat és a közösségimédia-hálózatokat a gyermekek online védelmére vonatkozó proaktív megközelítés alkalmazására;

30. felszólítja a Bizottságot és a tagállamokat, hogy indítsanak figyelemfelhívó és megelőző kampányokat és ösztönözzék a bevált gyakorlatok alkalmazását annak biztosítása érdekében, hogy a polgárok, különösen a gyermekek és egyéb veszélyeztetett felhasználók, de a központi és helyi kormányzatok, a kritikus szolgáltatók és a magánszektor szereplői is tisztában legyenek a kiberbűnözés veszélyeivel, tudják, hogyan lehetnek biztonságban online és hogyan védhetik meg eszközeiket; felszólítja továbbá a Bizottságot és a tagállamokat, hogy ösztönözzék gyakorlati biztonsági intézkedések bevezetését, így titkosítás vagy egyéb, a biztonságot és a magánélet védelmét megerősítő technológiák és anonimizálásra szolgáló eszközök használatát;

31. hangsúlyozza, hogy a figyelemfelhívó kampányokat az információs technológiai eszközök „tudatos használatával” foglalkozó oktatókampányoknak kell kísérnie; ösztönzi a tagállamokat, hogy iskolai tanterveikbe építések be a kiberbiztonság és a személyes adatok online használatával járó kockázatok és következmények kérdését;

ezzel összefüggésben hangsúlyozza a gyermekbarát internet európai stratégiájának (2012-es Gyermekbarát internet stratégia) keretében tett erőfeszítéseket;

32. hangsúlyozza, hogy a kiberbűnözés elleni küzdelem során sürgősen jelentősebb erőfeszítéseket kell tenni a hálózat- és információbiztonsághoz kapcsolódó oktatásban és képzésben, aminek keretében szükség van hálózat- és információbiztonsági képzés, informatikus-hallgatókat célzó, biztonságos szoftverfejlesztésre és a személyes adatok védelmére összpontosító képzések, valamint a közigazgatásban dolgozóknak szóló, alapvető hálózat- és információbiztonsági képzések bevezetésére;

33. úgy véli, hogy a hekkelés elleni biztosítás lehetne az egyik olyan eszköz, amely a biztonság területén való cselekvésre serkenthetné a szoftverek tervezéséért felelőssé tett vállalkozásokat és a helyes szoftverhasználatra ösztökélt felhasználókat;

34. hangsúlyozza, hogy a vállalatoknak rendszeres értékelésekkel kell azonosítaniuk a sebezhetőségeket és kockázatokat, valamint termékeiket és szolgáltatásaikat a sebezhetőségek azonnali kijavításával, többek között frissítéskezelési politikák és adatvédelmi frissítések révén kell megvédeniük, a zsarolóvírusok hatását átfogó adatmentési rendszerek kialakításával kell enyhíteniük, és következetesen jelenteniük kell az őket ért kibertámadásokat;

35. sürgeti a tagállamokat, hogy hozzanak létre CERT-eket, amelyeknek a vállalkozások és fogyasztók a kiberbiztonsági irányelvnek megfelelően jelenthetik a rosszindulatú e-maileket és weboldalakat, hogy a tagállamok rendszeres tájékoztatást kapjanak a biztonsági incidensekről és a saját rendszereiket érintő kockázatok kezelésére és csökkentésére rendelkezésre álló intézkedésekről; ösztönzi a tagállamokat, hogy vegyék fontolóra olyan adatbázis létrehozását, amelynek célja a számítástechnikai bűnözés különböző formáinak regisztrálása és a vonatkozó jelenségek fejlődésének figyelemmel kísérése;

36. sürgeti a tagállamokat, hogy fektessenek be a kritikus infrastruktúrájuk és az ahhoz kapcsolódó adatok biztonságának fejlesztésébe, hogy képesek legyenek ellenállni a kibertámadásoknak;

A szolgáltatók hatáskörének és felelősségének erősítése

37. kulcsfontosságúnak tartja az illetékes hatóságok és a szolgáltatók közti együttműködés elmélyítését a kölcsönös jogsegély és a kölcsönös elismerési eljárások felgyorsítása és hatékonyabbá tétele szempontjából, az európai jogi keret által előírt hatáskörökön belül; felhívja az uniós székhellyel nem rendelkező, elektronikus hírközlési szolgáltatást nyújtó szolgáltatókat, hogy írásban jelöljenek ki uniós képviselőket;

38. megismétli, hogy a dolgok internetét illetően elsősorban a gyártók szintjén kell szigorítani a felelősségi szabályokat, ami a termékminőség javulásához, továbbá a külső hozzáférés és a dokumentált frissítési eszköz tekintetében biztonságosabb környezetet eredményez majd;

39. úgy véli, hogy az innovációs trendek és a dolgok internetéhez kapcsolódó eszközök növekvő elérhetősége miatt különleges figyelmet kell szentelni minden eszköz biztonságának, beleértve a legegyszerűbbeket is; úgy véli, hogy a kiberbűnözés megelőzésére irányuló megoldásokba történő beruházás és a kiberbiztonsági

fenyegetésekkel kapcsolatos információcsere a hardvergyártók és az innovatív szoftverek fejlesztőinek érdekében áll; sürgeti a Bizottságot és a tagállamokat, hogy ösztönözzék a beépített biztonság elve szerinti megközelítést, valamint sürgeti az iparág szereplőit, hogy minden ilyen eszközben alkalmazzanak a beépített biztonság elvét alkalmazó megoldásokat; ebben az összefüggésben ösztönzi a magánszektort, hogy vezessen be a vonatkozó uniós jogszabályokon, így a kiberbiztonsági irányelven alapuló, nemzetközileg elismert szabványoknak megfelelő olyan, önkéntes intézkedéseket, mint a dolgok internete bizalmi jegy, a szoftverek és az eszközök biztonságosságába vetett bizalom növelése érdekében;

40. ösztönzi a szolgáltatókat, hogy csatlakozzanak a jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódexhez és felhívja a Bizottságot és a résztvevő vállalatokat, hogy továbbra is működjenek együtt ezzel a kérdéssel kapcsolatban;

41. emlékeztet rá, hogy az Európai Parlament és a Tanács a belső piacon az információs társadalommal összefüggő szolgáltatások, különösen az elektronikus kereskedelem egyes jogi vonatkozásairól szóló, 2000. június 8-i 2000/31/EK irányelve [1] (Elektronikus kereskedelemről szóló irányelv) kizárólag abban az esetben mentesíti a közvetítőket a tartalommal kapcsolatban viselt felelősség alól, ha a közvetített és/vagy tárolt tartalommal kapcsolatos szerepük semleges és passzív, de emellett azt is előírja, hogy ha a közvetítő jogsértésről vagy jogellenes tevékenységről vagy információról tényleges tudomást szerez, haladéktalanul intézkednie kell a tartalom eltávolításáról, illetve az ahhoz való hozzáférés megszüntetéséről;

42. kiemeli a bűnüldözői adatbázisok védelmének feltétlen szükségességét a biztonság megsértésével és a jogszerűtlen hozzáféréssel szemben, mivel ez az egyének számára aggodalomra okot adó kérdés; aggodalmának ad hangot azzal kapcsolatban, hogy a bűnüldöző hatóságok nyomozás keretében területen kívüli hatókörrel rendelkeznek az adatokhoz való hozzáférés tekintetében, továbbá hangsúlyozza, hogy ezzel kapcsolatban szigorú szabályokra van szükség;

43. úgy véli, hogy a jogsértő online tevékenységekkel kapcsolatos ügyeket sürgősséggel és hatékonyan, többek közt eltávolítási eljárások alkalmazásával kell kezelni, amennyiben a tartalomra nincs vagy már nincs szükség nyomozás, felderítés és vádeljárás lefolytatása céljából; emlékeztet rá, hogy amikor a tartalom eltávolítása nem kivitelezhető, a tagállamok szükséges és arányos intézkedéseket hoznak az ilyen tartalom uniós területről való hozzáférésének megakadályozására; hangsúlyozza, hogy az ilyen intézkedéseknek meg kell felelniük a meglévő jogalkotási és bírósági eljárásoknak és a Chartának, továbbá biztosítani kell a megfelelő biztosítékok, így a bírósági jogorvoslat lehetőségét;

44. felhívja a figyelmet a digitális információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatóknak az illegális online tartalmak gyors és hatékony, az illetékes bűnüldöző hatóság kérésére történő eltávolításában játszott szerepére és üdvözli az e tekintetben többek közt az uniós internetfórum révén elért eredményeket; hangsúlyozza, hogy az illetékes hatóságoknak és az információs társadalommal összefüggő szolgáltatást nyújtó szolgáltatóknak erősebben el kel kötelezniük magukat és fokozottabban együtt kell működniük annak érdekében, hogy az ágazati szereplők gyorsan és hatékonyan eltávolítsák a tartalmakat, valamint hogy elkerüljék az illegális

[1] HL L 178., 2000.7.17., 1. o.

tartalmak kormányzati intézkedésekkel való blokkolását; felhívja a tagállamokat, hogy az előírásokat nem teljesítő platformokat vonják jogi felelősségre; megismétli, hogy a jogellenes online tartalom eltávolítását célzó valamennyi, szerződéses feltételeket megállapító intézkedés csak akkor megengedhető, ha a nemzeti eljárási szabályok lehetőséget adnak a felhasználóknak jogaik bíróság előtt történő érvényesítésére, miután tudomást szereztek ezen intézkedésekről;

45. felhívja a figyelmet arra, hogy a digitális egységes piaci intézkedéscsomag megvalósításáról szóló, 2016. január 19-i parlamenti állásfoglalással[1] összhangban a közvetítők korlátozott felelőssége alapvető fontosságú az internet nyitottságának, az alapvető jogoknak, a jogbiztonságnak és az innovációnak a védelme szempontjából; üdvözli a Bizottság arra vonatkozó szándékát, hogy iránymutatást ad az értesítési és eltávolítási eljárásokat illetően, valamint hogy segítséget nyújt az online platformoknak az elektronikus kereskedelemre vonatkozó irányelvben (2000/31/EC) meghatározott feladataik teljesítésében és a felelősségre vonatkozó szabályok betartásában; felhívja a Bizottságot, hogy terjesszen elő jogalkotási javaslatot ebben a tárgyban;

46. felhív a „kövesd a pénz útját” megközelítés alkalmazására az Európai Parlament „A szellemitulajdon-jogok érvényesítésére vonatkozó megújított konszenzus felé” című uniós cselekvési tervről szóló 2015. június 9-i állásfoglalásában[2] megfogalmazottak szerint, az elektronikus kereskedelemről szóló irányelv szabályozási kerete, valamint a szellemi tulajdonhoz fűződő jogok érvényesítéséről szóló irányelv alapján;

47. hangsúlyozza annak alapvető fontosságát, hogy folyamatos és célzott képzést, valamint pszichológiai támogatást biztosítsanak a magán- és közszervezeteknél a kifogásolható vagy illegális online tartalmak értékeléséért felelős moderátorok számára, hiszen e területen őket kell az elsődleges beavatkozóknak tekinteni;

48. felhívja a szolgáltatókat, hogy rendelkezzenek egyértelmű bejelentés-típusok kialakításáról és állítsanak fel megfelelően meghatározott háttértámogatási infrastruktúrát, amely lehetővé teszi a bejelentésekre való gyors és megfelelő reagálást;

49. felhívja a szolgáltatókat, hogy fokozzák az internethasználatban, főleg a gyermekek számára rejlő kockázatokkal kapcsolatos tudatosságra irányuló erőfeszítéseiket interaktív eszközök és tájékoztató anyagok kidolgozása révén;

A rendőrségi és igazságügyi együttműködés megerősítése

50. aggodalmát fejezi ki azzal kapcsolatban, hogy a számítógépes bűncselekmények jelentős része büntetlenül marad; sajnálja, hogy az internetszolgáltatók által használt olyan technológiák, mint a NAT CGN súlyosan nehezítik a vizsgálatokat, mivel technikailag lehetetlenné teszik az IP-cím használójának, azaz az internetes bűncselekmény elkövetőjének pontos meghatározását; hangsúlyozza, hogy fontos biztosítani a bűnüldöző hatóságok számára a jogszerű hozzáférést a releváns információhoz – akkor is, ha az titkosított – azon korlátozott esetekben, amikor az biztonsági vagy igazságszolgáltatási szempontból szükséges és arányos; hangsúlyozza,

---

1 Elfogadott szövegek, P8_TA(2016)0009.
2 HL C 407., 2016.11.4., 25. o.

hogy a bűnüldöző és az igazságügyi hatóságok számára megfelelő képességeket kell biztosítani a jogszerű nyomozások lefolytatásához;

51. sürgeti a tagállamokat, hogy ne írjanak elő olyan kötelezettséget – például „hátsó kapuk” létrehozását vagy elősegítését – a titkosítás szolgáltatói számára, amelyeknek eredményeképpen gyengülne hálózataik vagy szolgáltatásaik biztonsága; hangsúlyozza, hogy kivitelezhető megoldásokat kell nyújtani – mind a jogalkotás, mind a folyamatos technológiai fejlődés révén – azokban az esetekben, amikor ezek megtalálása kulcsfontosságú az igazságszolgáltatás számára és a biztonság szempontjából; felhívja a tagállamokat, hogy az igazságszolgáltatással és az Eurojusttal egyeztetve működjenek együtt a nyomozati eszközök jogszerű, online használatára vonatkozó feltételek összehangolásában;

52. hangsúlyozza, hogy a jogszerű lehallgatás rendkívül hatékony eszköz lehet a jogszerűtlen feltöréssel szembeni küzdelemben, amennyiben az szükséges, arányos, megfelelő jogi eljáráson alapul és maradéktalanul megfelel az alapvető jogoknak, az Unió adatvédelmi jogszabályainak, valamint az uniós ítélkezési gyakorlatnak; felszólítja a tagállamokat, hogy éljenek a gyanúsítottakra irányuló jogszerű lehallgatás adta lehetőségekkel, állapítsanak meg egyértelmű szabályokat a jogszerű lehallgatási tevékenységek előzetes igazságügyi engedélyezési eljárásához, ideértve a jogszerű feltörőeszközök használati körének és időtartamának korlátozását, egy felügyeleti mechanizmus létrehozását, valamint hatékony jogorvoslati lehetőségek megteremtését a feltörési tevékenységek célpontjai számára;

53. ösztönzi a tagállamokat, hogy működjenek együtt az IKT biztonságával foglalkozó közösségekkel és ösztönözzék annak tagjait, hogy vállaljanak tevékenyebb szerepet az etikus feltörésben és az olyan jogszerűtlen tartalmak jelentésében, mint gyermekekkel szemben elkövetett szexuális visszaéléssel kapcsolatos anyagok;

54. ösztönzi az Europolt, hogy állítson össze olyan, a rejtett hálózatokon belüli, anonim jelentéstételi rendszert, amely lehetővé teszi az egyének számára, hogy a jogszerűtlen tartalmakról – többek között a gyermekekkel szemben elkövetett szexuális visszaélést ábrázoló anyagokról – jelentést tegyenek a hatóságoknak ugyanolyan technikai biztosítékok mellett, mint amilyet számos sajtószervezet is alkalmaz, amelyek ilyen rendszereket használnak az érzékeny adatok újságírókkal való cseréjének a hagyományos e-mailnél nagyobb fokú anonimitást és biztonságot lehetővé tevő elősegítésére;

55. hangsúlyozza, hogy minimalizálni kell annak a kockázatát, hogy a bűnüldöző hatóságok által jogszerű nyomozásaik részeként használt eszközök vagy megoldások kiszivárgása veszélyeztesse az internet-felhasználók magánéletét;

56. hangsúlyozza, hogy az igazságügyi és bűnüldöző hatóságokat megfelelő képességekkel és forrásokkal kell felvértezni a kiberbűnözés elleni hatékony küzdelemhez;

57. hangsúlyozza, hogy a sokféle, területileg elkülönülő nemzeti joghatóság megnehezíti a transznacionális esetekben alkalmazandó törvények megállapítását, illetve jogbizonytalanságnak ad teret, megakadályozva a határokon átívelő együttműködést, amelyre a számítástechnikai bűnözés elleni küzdelemben feltétlenül szükség lenne;

58. hangsúlyozza, hogy gyakorlati alapot kell kidolgozni a kibertérben gyakorolt joghatósággal kapcsolatos közös uniós megközelítés számára, az igazság- és belügyminiszterek 2016. január 26-i nem hivatalos ülésén megállapítottakkal összhangban;

59. e tekintetben hangsúlyozza, hogy közös eljárási előírásokat kell kialakítani, amelyek meghatározhatják azokat a területi tényezőket, amelyek alapul szolgálnak a kibertérben alkalmazandó jogszabályokhoz, valamint hogy olyan nyomozati intézkedéseket kell meghatározni, amelyek földrajzi határoktól függetlenül alkalmazhatók;

60. elismeri, hogy egy ilyen közös európai megközelítés, amelynek tiszteletben kell tartania az alapvető jogokat és a magánéletet, bizalmat teremt az érdekelt felek között, csökkenti a határokon átnyúló kérelmek feldolgozási időtartamát, interoperabilitást alakít ki heterogén szereplők között, valamint lehetőséget nyújt arra, hogy a jogszerű eljárásra vonatkozó követelményeket operatív keretekbe foglalják;

61. úgy véli, hogy hosszú távon, globális szinten a kibertérben gyakorolt végrehajtási joghatóságra vonatkozó közös eljárási szabályokat is ki kell alakítani; üdvözli e tekintetben az Európa Tanács felhőben található bizonyítékokkal foglalkozó csoportjának munkáját;

e-bizonyíték

62. hangsúlyozza, hogy a kibertérben való büntető igazságszolgáltatás közös európai megközelítése kiemelt fontosságú, mivel javítja a jogállamiság érvényesítését a kibertérben és megkönnyíti az e-bizonyítékok beszerzését a büntetőeljárások során, valamint hozzájárul az egyes ügyek a jelenleginél gyorsabb rendezéséhez;

63. hangsúlyozza, hogy meg kell találni az e-bizonyíték gyorsabb biztosításának és megszerzésének módját, valamint kiemeli a bűnüldöző hatóságok közti szoros, többek közt közös nyomozócsoportok, harmadik országok és az Európai területen tevékenykedő szolgáltatók fokozott igénybevételén keresztül, az általános adatvédelmi rendelettel ((EU) 2016/679), az (EU) 2016/680 irányelvvel (rendőrségi irányelv) és a meglévő, kölcsönös jogsegélyről szóló megállapodásokkal összhangban történő együttműködés fontosságát; hangsúlyozza, hogy valamennyi tagállamban egyablakos kapcsolattartási pontokat kell létrehozni a meglévő kapcsolattartási pontok igénybevételének optimalizálása érdekében, mivel ez elősegíti az e-bizonyítékokhoz való hozzáférést és az információmegosztást, javítja a szolgáltatókkal folytatott együttműködést, valamint felgyorsítja a kölcsönös jogsegélynyújtási eljárásokat;

64. elismeri, hogy a jelenlegi széttöredezett jogi keret kihívásokat jelenthet azon szolgáltatók számára, amelyek teljesíteni akarják a bűnüldöző hatóságok megkereséseit; felszólítja a Bizottságot, hogy terjesszen elő az e-bizonyítékokra vonatkozó európai jogi keretet, ideértve a szolgáltató belföldi vagy külföldi státuszának megállapítására szolgáló harmonizált szabályozást, valamint hogy kötelezze a szolgáltatókat, hogy válaszoljanak a más tagállamoktól érkező, megfelelő jogi eljárás alapján, az európai nyomozási határozattal összhangban benyújtott megkeresésekre, ugyanakkor vegye figyelembe az arányosság elvét, hogy ezáltal elkerülje a letelepedés és a szolgáltatásnyújtás szabadságának gyakorlását érintő káros hatásokat és biztosítson megfelelő védintézkedéseket, hogy ezáltal jogbiztonságot teremtsen és javítsa a

szolgáltatók és közvetítők a bűnüldöző hatóságok megkereséseire való reagálási képességét;

65. hangsúlyozza annak szükségességét, hogy az e-bizonyíték bármely keretrendszere megfelelő biztosítékokat tartalmazzon valamennyi érintett jogai és szabadságai tekintetében; kiemeli, hogy ennek magában kell foglalnia azt a követelményt, hogy az e-bizonyíték iránti kérelmekkel első fokon az adatkezelőkhöz vagy az adatbirtokosokhoz kell fordulni be annak biztosítása érdekében, hogy tiszteletben tartsák jogaikat és azok jogait, akikre az adatok vonatkoznak (például azon jogosultságukat, hogy éljenek előjogaikkal, és jogorvoslatot kérjenek aránytalan vagy más módon jogellenes hozzáférés miatt); szükségesnek tartja továbbá annak biztosítását, hogy bármely jogszabályi keret védelmet nyújtson a szolgáltatók és minden más fél számára azon kérelmekkel szemben, amelyek kollíziót okozhatnak, vagy más módon sértheti más államok szuverenitását;

66. felszólítja a tagállamokat a büntetőügyekben kibocsátott európai nyomozási határozatról szóló 2014/41/EU irányelv (ENYH-irányelv) maradéktalan végrehajtására az e-bizonyítékok hatékony biztosítása és begyűjtése érdekében az Európai Unióban, illetve arra, hogy az e-bizonyítékok bíróságokon való felhasználását megkönnyítendő foglaljanak a kibertérre vonatkozó rendelkezéseket nemzeti büntető törvénykönyveikbe és tegyék lehetővé, hogy a bírák egyértelműbb iránymutatást kapjanak a kiberbűnözés büntetéséről;

67. üdvözli a Bizottság folyamatos munkáját, amely egy olyan együttműködési fórumra irányul, amely biztonságos kommunikációs csatornával rendelkezik az e-bizonyítékokkal kapcsolatos európai nyomozási határozatok és válaszok uniós igazságügyi hatóságok közti digitális cseréje céljából; felkéri a Bizottságot, hogy a tagállamokkal, az Eurojusttal és a szolgáltatókkal együttműködve vizsgálja meg és hozza összhangba egymással az e-bizonyítékok biztosítására és beszerzésére szolgáló formanyomtatványokat, eszközöket és eljárásokat a hitelesítés elősegítése érdekében, gyors eljárásokat biztosítva és növelve az e-bizonyítékok biztosításának és beszerzésének átláthatóságát és elszámoltathatóságát; felhívja az Európai Unió Bűnüldözési Képzési Ügynökségét (CEPOL), hogy alakítson ki az e-bizonyítékok biztosítására és beszerzésére használt jelenlegi keret hatékony használatával kapcsolatos képzési modulokat; kiemeli ebben az összefüggésben, hogy a szolgáltatásnyújtói politikák egyszerűsítése segíti majd a megközelítések sokféleségének csökkentését, nevezetesen a kért adathoz való hozzáférés biztosításának eljárásai és feltételei tekintetében;

Kapacitásbővítés európai szinten

68. rámutat, hogy közelmúltbeli incidensek egyértelműen igazolták az EU – és különösen az uniós intézmények, a nemzeti kormányok és parlamentek, a jelentősebb európai vállalatok, az európai informatikai infrastruktúrák és hálózatok – akut sebezhetőségét az összetett szoftverekkel és a rosszindulatú számítógépes programokkal végrehajtott, kifinomult támadásokkal szemben; felhívja az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA), hogy folyamatosan értékelje a fenyegetési szintet, valamint kéri a Bizottságot, hogy ruházzon be az uniós intézmények kulcsfontosságú infrastruktúráinak IT-kapacitásába, védelmébe és ellenálló képességébe, hogy ezáltal csökkentse az EU nagy bűnözői szervezetek vagy terrorista

csoportok által végrehajtott kibertámadásokkal és államilag szponzorált támadásokkal szembeni sebezhetőségét;

69. elismeri az Europol és az Eurojust Számítástechnikai Bűnözés Elleni Európai Központja (EC3), illetve az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) a kiberbűnözés elleni küzdelemhez nyújtott fontos hozzájárulását;

70. felszólítja az Europolt, hogy támogassa a nemzeti bűnüldöző hatóságokat a biztonságos és megfelelő kommunikációs hálózatok felállításában;

71. sajnálja, hogy jelenleg nincsenek uniós képzési és képesítési normák; elismeri, hogy a kiberbűnözés jövőbeli tendenciái egyre magasabb szintű szakértelmet követelnek meg a szakemberektől; üdvözli, hogy a meglévő kezdeményezések, például a Számítástechnikai Bűnözés Elleni Európai Képzési és Oktatási Csoport (ECTEG), az oktatók képzésére irányuló TOT-projekt és az uniós szakpolitikai ciklus keretében folytatott képzési tevékenységek már egyengetik a szakértelem terén meglévő hiányosságok kezelését uniós szinten;

72. felszólítja a CEPOL-t és az Európai Igazságügyi Képzési Hálózatot, hogy a kiberbűnözéssel kapcsolatos témákkal foglalkozó képzéseiket tegyék elérhetővé Unió-szerte az illetékes bűnüldöző hatóságok és igazságügyi hatóságok számára is;

73. hangsúlyozza, hogy az Eurojust felé továbbított számítástechnikai bűncselekmények száma 30%-kal nőtt; kéri, hogy bocsássanak rendelkezésre elegendő forrást, szükség esetén több álláshely biztosításával annak érdekében, hogy az Eurojust megbirkózhasson a számítástechnikai bűnözéssel kapcsolatos növekvő munkateherrel, valamint hogy fejleszthesse és megerősíthesse a kiberbűnözésre szakosodott nemzeti ügyészeknek a határokon átívelő ügyekben nyújtott támogatását, többek közt a közelmúltban létrehozott számítástechnikai bűnözés elleni európai igazságügyi hálózaton keresztül;

74. kéri az ENISA megbízatásának felülvizsgálatát és a nemzeti kiberbiztonsági ügynökségek megerősítését; kéri az ENISA feladatok, alkalmazottak és források tekintetében való megerősítését; hangsúlyozza, hogy az új megbízatásnak magában kell foglalnia az Europolhoz és az ágazati érdekelt felekhez fűződő kapcsolatok erősítését is, hogy ezáltal az ügynökség jobban támogathassa az illetékes hatóságokat a kiberbűnözés elleni küzdelemben;

75. kéri az Európai Unió Alapjogi Ügynökségét (FRA), hogy állítson össze egy olyan gyakorlati és részletes kézikönyvet, amely iránymutatásokat ad a tagállamok számára a felügyeleti és ellenőrzési intézkedésekről;

Fokozottabb együttműködés harmadik országokkal

76. hangsúlyozza a kiberbűnözés elleni globális harc jegyében folytatott, harmadik országokkal való szoros együttműködés fontosságát, ideértve a bevált gyakorlatok megosztását, a közös nyomozásokat, a kapacitásbővítést, valamint a kölcsönös jogsegélyt;

77. felhívja a tagállamokat, hogy ha eddig még nem tették meg, ratifikálják és maradéktalanul hajtsák végre az Európa Tanács számítástechnikai bűnözésről szóló, 2001. november 23-i egyezményét (Budapesti Egyezmény) és annak kiegészítő

jegyzőkönyveit, és a Bizottsággal együttműködve hívják fel arra a figyelmet a megfelelő nemzetközi fórumokon;

78. hangsúlyozza, hogy komoly aggályai vannak a Tanács számítástechnikai bűnözésről szóló egyezmény (Budapesti Egyezmény) 32. cikkének értelmezésével foglalkozó bizottságában a tárolt számítógépes adatokhoz való, határokon átnyúló hozzáférés („felhőben található bizonyítékok”) tárgyában folytatott munkával kapcsolatban, és ellenzi olyan kiegészítő jegyzőkönyv vagy iránymutatás elfogadását, amely e rendelkezés hatályát az említett egyezmény által létrehozott hatályos rendszeren túlra is kiterjesztené, ami már jelenleg is a territorialitás elve alóli jelentős kivételt képez, mivel ez a bűnüldöző hatóságok akadálytalan távoli hozzáférését eredményezheti más államok joghatósága alá tartozó területen elhelyezkedő szerverekhez és számítógépekhez, anélkül hogy igénybe kellene venniük a kölcsönös jogsegélyről szóló megállapodásokat vagy az igazságügyi együttműködés más, az egyének alapvető jogainak – köztük az adatok védelméhez és a megfelelő eljáráshoz való jog – garantálása céljából létrehozott eszközöket, így különösen az Európa Tanács 108. egyezményét;

79. sajnálja, hogy a számítástechnikai bűnözés vonatkozásában nincs kötelező erejű nemzetközi jogszabály, és sürgeti a tagállamokat és az európai intézményeket, hogy dolgozzanak egy ilyen tárgyú egyezmény létrehozásán;

80. felhívja a Bizottságot, hogy tegyen javaslatot olyan kezdeményezésekre vonatkozó lehetőségekre, amelyek javítanák a kölcsönös jogsegélyről szóló szerződések hatékonyságát és előmozdítanák azok használatát, annak érdekében, hogy ellensúlyozzák a harmadik országok területen kívüli joghatóságára vonatkozó feltételezést;

81. felhívja a tagállamokat, hogy biztosítsanak elegendő kapacitást a kibertérben zajló nyomozásokhoz kapcsolódó kölcsönös jogsegély iránti kérelmek kezelésére, és alakítsanak ki megfelelő képzési programokat az ilyen kérelmek kezeléséért felelős személyzet számára;

82. hangsúlyozza, hogy a stratégiai és műveleti együttműködési megállapodások az Europol és harmadik országok között előmozdítják az információcserét és a gyakorlati együttműködést egyaránt;

83. megjegyzi, hogy a bűnüldöző hatóságok kérelmeik többségét az Egyesült Államok vagy Kanada felé nyújtják be; aggodalmának ad hangot azzal kapcsolatban, hogy az Egyesült Államok nagy szolgáltatóinak az európai bűnüldöző hatóságok kérelmeire vonatkozó önkéntes közzétételi rátája a 60%-ot sem éri el, továbbá emlékeztet rá, hogy az általános adatvédelmi rendelet V. fejezete szerint a külföldön tárolt személyes adatokhoz való hozzáférés lehetővé tételének előnyben részesített mechanizmusát a kölcsönös jogsegélyről szóló szerződések és egyéb nemzetközi megállapodások képezik;

84. felhívja a Bizottságot, hogy a kölcsönös jogsegélyt előmozdítandó javasoljon konkrét intézkedéseket a gyanúsítottak vagy vádlottak alapvető jogainak védelme érdekében az európai bűnüldöző hatóságok és harmadik országok közötti információcsere megvalósítása során, nevezetesen biztosítékokat a releváns bizonyítékok, az előfizető-specifikus információk, vagy részletes (amennyiben nem titkosított) meta- és tartalomadatok bírósági döntést követő, bűnüldöző hatóságok és/vagy szolgáltatók általi gyors átadása tekintetében;

85. felszólítja a Bizottságot, hogy a tagállamokkal, a kapcsolódó európai szervekkel és adott esetben a harmadik országokkal együttműködve vizsgálja meg a harmadik országokban tárolt e-bizonyítékok – az alapvető jogoknak és az EU adatvédelmi jogszabályainak teljes mértékben megfelelő – hatékony biztosításának és begyűjtésének új módjait a kölcsönös jogsegélyre irányuló eljárások alkalmazásának felgyorsításával és egyszerűsítésével;

86. kiemeli a NATO számítástechnikai incidenskezelő központjának fontosságát;

87. felszólítja a tagállamokat, hogy a kapacitásépítést célzó partnerségek létrehozásának elősegítése érdekében vegyenek részt a számítástechnikai szakértők világfóruma (GFCE) munkájában;

88. üdvözli az Unió keleti szomszédos országok számára nyújtott kapacitásbővítési támogatását, mivel számos kibertámadás ezen országokból indul ki;

°

° °

89. utasítja elnökét, hogy továbbítsa ezt az állásfoglalást a Tanácsnak és a Bizottságnak.