Utorok 3. októbra 2017

P8_TA(2017)0366

Boj proti počítačovej kriminalite

Uznesenie Európskeho parlamentu z 3. októbra 2017 o boji proti počítačovej kriminalite (2017/2068(INI))

(2018/C 346/04)

Európsky parlament,

— so zreteľom na články 2, 3 a 6 Zmluvy o Európskej únii (Zmluva o EÚ),

— so zreteľom na články 16, 67, 70, 72, 73, 75, 82, 83, 84, 85, 87 a 88 Zmluvy o fungovaní Európskej únie (ZFEÚ),

— so zreteľom na články 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 a 52 Charty základných práv Európskej únie,

— so zreteľom na Dohovor OSN o právach dieťaťa z 20. novembra 1989,

— so zreteľom na Opčný protokol k Dohovoru o právach dieťaťa o predaji detí, detskej prostitúcii a detskej pornografii z 25. mája 2000,

— so zreteľom na Štokholmskú deklaráciu a akčný program prijaté na prvom Svetovom kongrese proti komerčnému sexuálnemu vykorisťovaniu detí, Jokohamský globálny záväzok prijatý na druhom Svetovom kongrese proti komerčnému sexuálnemu vykorisťovaniu detí a Budapeštiansky záväzok a akčný plán prijaté na prípravnej konferencii na druhý Svetový kongres proti komerčnému sexuálnemu vykorisťovaniu detí,

— so zreteľom na Dohovor Rady Európy o ochrane detí pred sexuálnym vykorisťovaním a sexuálnym zneužívaním z 25. októbra 2007,

— so zreteľom na svoje uznesenie z 20. novembra 2012 o ochrane detí v digitálnom svete ([1]),

— so zreteľom na svoje uznesenie z 11. marca 2015 o sexuálnom zneužívaní detí na internete ([2]),

— so zreteľom na rámcové rozhodnutie Rady č. 2001/413/JAI z 28. mája 2001 o boji proti podvodom a falšovaniu bezhotovostných platobných prostriedkov ([3]),

— so zreteľom na Dohovor o počítačovej kriminalite podpísaný v Budapešti 23. novembra 2001 ([4]) a dodatkový protokol k nemu,

— so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií ([5]),

([1]) Ú. v. EÚ C 419, 16.12.2015, s. 33.
([2]) Ú. v. EÚ C 316, 30.8.2016, s. 109.
([3]) Ú. v. ES L 149, 2.6.2001, s. 1.
([4]) Rada Európy, Séria európskych zmlúv, č. 185, 23.11.2001.
([5]) Ú. v. EÚ L 77, 13.3.2004, s. 1.

Utorok 3. októbra 2017

— so zreteľom na smernicu Rady 2008/114/ES z 8. decembra 2008 o identifikácii a označení európskych kritických infraštruktúr a zhodnotení potreby zlepšiť ich ochranu ([1]),

— so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002, týkajúcu sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií ([2]),

— so zreteľom na smernicu Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV ([3]),

— so zreteľom na spoločné oznámenie Komisie a podpredsedníčky Komisie/vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov zo 7. februára 2013 s názvom Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor (JOIN(2013)0001),

— so zreteľom na smernicu Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV ([4]),

— so zreteľom na smernicu Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach ([5]) (smernica o EVP),

— so zreteľom na rozhodnutie Súdneho dvora Európskej únie z 8. apríla 2014 ([6]), ktorým sa zrušila platnosť smernice o uchovávaní údajov,

— so zreteľom na svoje uznesenie z 12. septembra 2013 s názvom Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor ([7]),

— so zreteľom na oznámenie Komisie zo 6. mája 2015 s názvom Stratégia pre jednotný digitálny trh v Európe (COM(2015)0192),

— so zreteľom na oznámenie Komisie z 28. apríla 2015 s názvom Európsky program v oblasti bezpečnosti (COM(2015)0185) a následnú správu o pokroku s názvom Smerom k účinnej a skutočnej bezpečnostnej únii,

— so zreteľom na správu z konferencie o jurisdikcii v kybernetickom priestore, ktorá sa konala 7. a 8. marca 2016 v Amsterdame,

— so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) ([8]),

([1]) Ú. v. EÚ L 345, 23.12.2008, s. 75.
([2]) Ú. v. ES L 201, 31.7.2002, s. 37.
([3]) Ú. v. EÚ L 335, 17.12.2011, s. 1.
([4]) Ú. v. EÚ L 218, 14.8.2013, s. 8.
([5]) Ú. v. EÚ L 130, 1.5.2014, s. 1.
([6]) ECLI:EU:C:2014:238.
([7]) Ú. v. EÚ C 93, 9.3.2016, s. 112.
([8]) Ú. v. EÚ L 119, 4.5.2016, s. 1.

— so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV ([1]),

— so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2016/794 z 11. mája 2016 o Agentúre Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol) ([2]),

— so zreteľom na rozhodnutie Komisie z 5. júla 2016 o podpísaní zmluvnej dohody o verejno-súkromnom partnerstve v oblasti priemyselného výskumu a inovácií kybernetickej bezpečnosti medzi Európskou úniou, ktorá bola zastúpená Komisiou, a organizáciou zúčastnených strán (C(2016)4400),

— so zreteľom na spoločné oznámenie Európskemu parlamentu a Rade zo 6. apríla 2016 podpredsedníčke Komisie / vysokej predstaviteľke Únie pre zahraničné veci a bezpečnostnú politiku s názvom Spoločný rámec pre boj proti hybridným hrozbám: reakcia Európskej únie (JOIN(2016)0018),

— so zreteľom na oznámenie Komisie s názvom Európska stratégia vytvárania lepšieho internetu pre deti (COM(2012)0196) a na správu Komisie zo 6. júna 2016 s názvom Záverečné hodnotenie viacročného programu EÚ na ochranu detí, ktoré používajú internet a iné komunikačné technológie (Bezpečnejší internet) (COM(2016)0364),

— so zreteľom na spoločné vyhlásenie Europolu a agentúry ENISA z 20. mája 2016 o zákonnom trestnom vyšetrovaní, ktoré rešpektuje ochranu údajov na úrovni 21. storočia,

— so zreteľom na závery Rady z 9. júna 2016 o Európskej justičnej sieti na boj proti počítačovej kriminalite,

— so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii ([3]),

— so zreteľom na stanovisko agentúry ENISA k šifrovaniu z decembra 2016 s názvom *Encryption – Strong Encryption Safeguards our Digital Identity,*

— so zreteľom na záverečnú správu výboru Rady Európy pre počítačovú kriminalitu (T-CY Cloud Evidence Group) zo 16. septembra 2016 s názvom *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY,*

— so zreteľom na činnosť spoločnej pracovnej skupiny pre boj proti počítačovej kriminalite (*Joint Cyber Crime Action Taskforce, J-CAT*),

— so zreteľom na hodnotenie hrozieb závažnej a organizovanej trestnej činnosti (EU SOCTA) z 28. februára 2017 a hodnotenie hrozieb internetovej organizovanej trestnej činnosti (IOCTA) z 28. septembra 2016, ktoré vypracoval Europol,

— so zreteľom na rozsudok Súdneho dvora Európskej únie vo veci C-203/15 (rozsudok TELE2) z 21. decembra 2016 ([4]),

([1]) Ú. v. EÚ L 119, 4.5.2016, s. 89.
([2]) Ú. v. EÚ L 135, 24.5.2016, s. 53.
([3]) Ú. v. EÚ L 194, 19.7.2016, s. 1.
([4]) Rozsudok Súdneho dvora z 21. decembra 2016, Tele2 Sverige AB proti Post- och telestyrelsen a i. a Secretary of State for the Home Department proti Tomovi Watsonovi a ďalším, C-203/15, ECLI:EU:C:2016:970.

Utorok 3. októbra 2017

— so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2017/541 z 15. marca 2017 o boji proti terorizmu, ktorou sa nahrádza rámcové rozhodnutie Rady 2002/475/SVV a mení rozhodnutie Rady 2005/671/SVV ([1]);

— so zreteľom na článok 52 rokovacieho poriadku,

— so zreteľom na správu Výboru pre občianske slobody, spravodlivosť a vnútorné veci a na stanovisko Výboru pre vnútorný trh a ochranu spotrebiteľa (A8-0272/2017),

A. keďže počítačová kriminalita spôsobuje čoraz výraznejšie sociálne a hospodárske škody, ktoré majú vplyv na základné práva jednotlivcov a v kybernetickom priestore predstavujú hrozbu pre právny štát a stabilitu demokratických spoločností;

B. keďže počítačová kriminalita je v členských štátoch EÚ čoraz väčším problémom;

C. keďže z hodnotenia IOCTA 2016 vyplýva, že počítačová kriminalita naberá na intenzite, komplexnosti a rozsahu, že v niektorých krajinách EÚ je rozšírenejšia než tradičné formy trestnej činnosti, že presahuje do iných oblastí trestnej činnosti, ako je obchodovanie s ľuďmi, že využívanie nástrojov na šifrovanie a anonymizáciu na účely trestnej činnosti narastá a že útoky prostredníctvom tzv. ransomvéru sú častejšie než obvyklé hrozby v podobe malvéru, napríklad trójske kone;

D. keďže v roku 2016 sa počet útokov na servery Komisie v porovnaní s rokom 2015 zvýšil o 20 %;

E. keďže zraniteľnosť počítačov na útoky súvisí s jedinečnosťou vývoja informačných technológií v priebehu uplynulých rokov, rýchlosťou rastu online obchodu a nedostatočnými opatreniami zo strany vlády;

F. keďže neustále rastie čierny trh s vydieraním prostredníctvom počítača, ako aj využívanie nájomných botnetov, hakerstva a kradnutého digitálneho tovaru;

G. keďže stredobodom kybernetických útokov je naďalej malvér, napríklad bankové trójske kone, ale takisto možno pozorovať rast počtu a následkov útokov na priemyselné kontrolné systémy a siete zamerané na zničenie kritickej infraštruktúry a hospodárskych štruktúr, ako aj destabilizáciu spoločností, ako to bolo v prípade útoku prostredníctvom ransomvéru s názvom WannaCry v máji 2017, a teda tieto útoky predstavujú čoraz väčšiu hrozbu pre bezpečnosť, obranu a ďalšie dôležité odvetvia; keďže väčšina žiadostí o údaje v oblasti presadzovania medzinárodného práva sa týka podvodov a finančnej trestnej činnosti, po ktorých nasleduje násilná a závažná trestná činnosť;

H. keďže i keď čoraz väčšia previazanosť ľudí, miest a vecí prináša mnoho výhod, takisto zvyšuje riziko počítačovej kriminality; keďže zariadenia pripojené na internet vecí, ktoré zahŕňajú inteligentné siete, pripojené chladničky, automobily či lekárske nástroje alebo pomôcky, často nie sú rovnako dobre chránené ako tradičné internetové zariadenia, a teda sú ideálnym cieľom pre páchateľov počítačovej trestnej činnosti, najmä preto, že režim bezpečnostných aktualizácií pre pripojené zariadenia je často neúplný alebo celkom chýba; keďže zariadenia internetu vecí zasiahnuté hakerským útokom, ktoré majú alebo môžu ovládať fyzické ovládače, môžu predstavovať konkrétnu hrozbu pre životy ľudí;

I. keďže účinný právny rámec na ochranu údajov je nevyhnutný na vybudovanie dôvery vo svet internetu a zároveň umožní spotrebiteľom, ako aj podnikom v plnej miere využívať výhody digitálneho jednotného trhu a riešiť problém počítačovej kriminality;

J. keďže podniky samotné nedokážu čeliť výzve zvyšovania bezpečnosti prepojeného sveta a vláda by mala prispievať ku kybernetickej bezpečnosti reguláciou a poskytovaním stimulov na podporu bezpečnejšieho správania používateľov;

([1]) Ú. v. EÚ L 88, 31.3.2017, s. 6.

K. keďže hranice medzi počítačovou kriminalitou, počítačovou špionážou, počítačovou vojnou, počítačovou sabotážou a počítačovým terorizmom sú čoraz nejasnejšie; keďže počítačová kriminalita môže byť zameraná na jednotlivcov, verejné alebo súkromné subjekty a môže zahŕňať širokú škálu trestných činov vrátane narušenia súkromia, sexuálneho zneužívania detí online, verejného podnecovania k násiliu alebo nenávisti, sabotáže, špionáže, finančnej trestnej činnosti a podvodov, napríklad platobných podvodov, krádeže a krádeže identity, ako aj protiprávneho zásahu do systému;

L. keďže v správe Svetového ekonomického fóra o globálnych rizikách z roku 2017 sa hromadný výskyt dátových podvodov a krádeže dát uvádza ako jedno z piatich hlavných globálnych rizík z hľadiska pravdepodobnosti;

M. keďže značný počet počítačových trestných činov zostáva nestíhaný a nepotrestaný; keďže možno konštatovať stále nízku mieru ohlasovania, dlhé obdobia odhaľovania umožňujúce páchateľom počítačovej kriminality zabezpečiť si niekoľko vchodov/východov alebo zadných dvierok, ťažký prístup k elektronickým dôkazom, problémy s ich získavaním a prípustnosťou na súde, ako aj zložité postupy a jurisdikčné výzvy v súvislosti s cezhraničným charakterom počítačovej kriminality;

N. keďže Rada vo svojich záveroch z júna 2016 zdôraznila, že vzhľadom na cezhraničnú povahu počítačovej kriminality, ako aj na hrozby spoločnej kybernetickej bezpečnosti, ktorým čelí EÚ, je zlepšená spolupráca a výmena informácií medzi policajnými a súdnymi orgánmi a odborníkmi z oblasti počítačovej kriminality nevyhnutná pre účinné vyšetrovanie v kybernetickom priestore a získavanie elektronických dôkazov;

O. keďže zrušením smernice o uchovávaní údajov rozhodnutím Súdneho dvora EÚ z 8. apríla 2014, ako aj zákazom všeobecného, nerozlišujúceho a necieleného uchovávania údajov, ktorý bol potvrdený rozhodnutím Súdneho dvora EÚ vo veci TELE2 z 21. decembra 2016, sa stanovujú prísne obmedzenia pre hromadné spracovanie telekomunikačných údajov, ako aj pre prístup príslušných orgánov k týmto údajom;

P. keďže v rozsudku Súdneho dvora EÚ vo veci Maximillian Schrems ([1]) sa zdôrazňuje, že hromadné sledovanie je porušením základných práv;

Q. keďže boj proti počítačovej kriminalite musí rešpektovať rovnaké procesné a hmotnoprávne záruky a základné práva, konkrétne v oblasti ochrany údajov a slobody slova, rovnako ako boj proti všetkým ostatným oblastiam trestnej činnosti;

R. keďže deti používajú internet v čoraz mladšom veku a sú osobitne zraniteľné, takže sa môžu stať obeťami tzv. groomingu a ďalších foriem sexuálneho zneužívania na internete (kybernetické šikanovanie, sexuálne zneužívanie, sexuálny nátlak a vydieranie), zneužívania osobných údajov, ako aj nebezpečných výziev zameraných na podporu rôznych druhov sebapoškodzovania, ako v prípade hry Blue whale, a preto potrebujú osobitnú ochranu; keďže páchatelia na internete môžu obete rýchlejšie vyhľadávať a klamať prostredníctvom četovacích fór, e-mailov, online hier a sociálnych sietí a keďže skryté peer-to-peer (P2P) siete zostávajú pre páchateľov sexuálnych trestných činov na deťoch hlavnými platformami na prístup, komunikáciu, ukladanie a výmenu materiálu zobrazujúceho sexuálne vykorisťovanie detí a na sledovanie nových obetí bez toho, aby boli odhalení;

S. keďže rastúci trend sexuálneho nátlaku a vydierania stále nie je dostatočne preskúmaný ani sa o ňom v dostatočnej miere neinformuje, väčšinou pre povahu tohto trestného činu, čo spôsobuje, že obete pociťujú zahanbenie a vinu;

T. keďže naživo prenášané zneužívanie detí na diaľku sa považuje za čoraz väčšiu hrozbu; keďže naživo prenášané zneužívanie detí na diaľku úplne zjavne súvisí s komerčným šírením materiálov z oblasti sexuálneho vykorisťovania detí;

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

Utorok 3. októbra 2017

U. keďže v rámci nedávnej štúdie Národnej kriminálnej agentúry Spojeného kráľovstva sa zistilo, že mladí ľudia zapojení do hakerských aktivít sú menej motivovaní peniazmi a často napádajú počítačové siete preto, aby zapôsobili na svojich priateľov alebo spochybnili politický systém;

V. keďže informovanosť o rizikách, ktoré počítačová kriminalita priniesla, sa zvýšila, ale preventívne opatrenia zo strany individuálnych používateľov, verejných inštitúcií a podnikov sú naďalej úplne nedostatočné, a to najmä pre nedostatok znalostí a zdrojov;

W. keďže boj proti počítačovej kriminalite a nelegálnym aktivitám na internete by nemal zakryť pozitívne aspekty slobodného a otvoreného kybernetického priestoru, ktorý ponúka nové možnosti výmeny vedomostí a presadzovania politického a sociálneho začleňovania na celom svete;

Všeobecné úvahy

1. zdôrazňuje, že prudký nárast ransomvéru, botnetov a neoprávneného narušania počítačových systémov má vplyv na bezpečnosť jednotlivcov, dostupnosť a integritu ich osobných údajov, ako aj na ochranu súkromia a základných slobôd a na integritu kritickej infraštruktúry, okrem iného vrátane štruktúr zabezpečujúcich dodávky energie a elektrickej energie a finančných štruktúr, ako je burza cenných papierov; v tejto súvislosti pripomína, že boj proti počítačovej kriminalite je prioritou v rámci Európskeho programu v oblasti bezpečnosti z 28. apríla 2015;

2. zdôrazňuje, že treba zjednodušiť spoločné vymedzenia pojmov počítačová kriminalita, kybernetická vojna, kybernetická bezpečnosť, kybernetické obťažovanie a kybernetické útoky s cieľom stanoviť spoločné právne vymedzenie v inštitúciách EÚ a členských štátoch EÚ;

3. zdôrazňuje, že boj proti počítačovej kriminalite by mal byť predovšetkým o ochrane a posilňovaní kritickej infraštruktúry a iných sieťových zariadení, a nielen o prijímaní represívnych opatrení;

4. pripomína dôležitosť právnych opatrení prijatých na európskej úrovni s cieľom harmonizovať vymedzenie trestných činov spojených s útokmi na informačné systémy, ako aj so sexuálnym zneužívaním a vykorisťovaním detí online a zaviazať členské štáty, aby zriadili systém na zaznamenávanie, výrobu a poskytovanie štatistických údajov o týchto trestných činoch v záujme účinnejšieho boja proti týmto druhom trestnej činnosti;

5. dôrazne žiada tie členské štáty, ktoré tak ešte neurobili, aby urýchlene a náležite transponovali a vykonávali smernicu 2011/93/EÚ o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a detskej pornografii; vyzýva Komisiu, aby dôsledne monitorovala a zabezpečila jej úplné a účinné vykonávanie a včas podala Európskemu parlamentu a gestorskému výboru správu o svojich zisteniach a zároveň nahradila rámcové rozhodnutie Rady 2004/68/SVV; zdôrazňuje, že Eurojust a Europol musia dostať primerané zdroje na zlepšenie identifikácie obetí, na boj proti organizovaným sieťam osôb, ktoré sa dopúšťajú sexuálneho zneužívania, a na urýchlenie odhaľovania, analýzy a postupovania materiálu zobrazujúceho zneužívanie detí na internete aj mimo neho;

6. vyjadruje hlboké poľutovanie nad tým, že 80 % podnikov v Európe zažilo aspoň jeden incident v oblasti kybernetickej bezpečnosti, a nad tým, že kybernetické útoky proti podnikom často ostávajú neodhalené alebo neohlásené; pripomína, že na základe rôznych štúdií sa odhaduje, že kybernetické útoky predstavujú značné ročné náklady pre svetové hospodárstvo; domnieva sa, že povinnosť zverejňovať prípady narušenia bezpečnosti a vymieňať si informácie o rizikách, zavedená nariadením (EÚ) 2016/679 o ochrane fyzických osôb so zreteľom na spracovanie osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov) a smernicou (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (smernica o bezpečnosti sietí a informačných systémov (smernica NIS)), pomôže riešiť tento problém poskytovaním podpory podnikom, najmä MSP;

7. zdôrazňuje, že neustále sa meniaca povaha kybernetických hrozieb prináša pre všetky zainteresované strany závažné právne a technologické výzvy; domnieva sa, že nové technológie by sa nemali vnímať ako hrozba, a uznáva, že technologický pokrok v oblasti šifrovania zlepší celkovú bezpečnosť našich informačných systémov, a to aj tým, že umožnia koncovým používateľom lepšiu ochranu ich dát a komunikácie; poukazuje však na to, že stále existujú značné nedostatky pri zabezpečovaní komunikácie a že techniky, ako sú tzv. onion routing a skryté siete, môžu používať

zlomyseľní používatelia vrátane teroristov a páchateľov sexuálnych trestných činov zameraných na deti, hakeri sponzorovaní nie spriatelenými cudzími štátmi alebo extrémistické politické alebo náboženské organizácie na trestné účely, najmä na utajenie svojich aktivít v oblasti trestnej činnosti alebo totožnosti, čo spôsobuje vážne problémy pri vyšetrovaní;

8. je veľmi znepokojený nedávnym celosvetovým útokom prostredníctvom ransomvéru, ktorý zrejme postihol desaťtisíce počítačov v takmer 100 krajinách a mnoho organizácií, okrem iného aj národný zdravotnícky systém (NHS) v Spojenom kráľovstve, čo je najvýznamnejšia obeť tohto rozsiahleho zásahu malvérom; v tejto súvislosti uznáva významnú činnosť v rámci iniciatívy No More Ransom, ktorá poskytuje viac než 40 bezplatných dešifrovacích nástrojov umožňujúcich obetiam ransomvéru na celom svete dešifrovať svoje zariadenia postihnuté útokom;

9. zdôrazňuje, že skryté siete a tzv. onion-routing takisto poskytujú slobodný priestor novinárom, politickým aktivistom a obhajcom ľudských práv v niektorých krajinách s cieľom zamedziť odhaleniu zo strany represívnych štátnych orgánov;

10. konštatuje, že využívanie nástrojov a služieb počítačovej kriminality zo strany zločineckých a teroristických sietí je stále obmedzené; zdôrazňuje však, že je veľmi pravdepodobné, že sa to zmení, vzhľadom na čoraz silnejšie väzby medzi terorizmom a organizovanou trestnou činnosťou a na širokú dostupnosť strelných zbraní a prekurzorov výbušnín na skrytých sieťach;

11. dôrazne odsudzuje akékoľvek zasahovanie do systému uskutočňované alebo riadené cudzou krajinou alebo jej agentmi s cieľom narušiť demokratický proces v inej krajine;

12. zdôrazňuje, že cezhraničné žiadosti o odňatie domény, odstránenie obsahu a prístup k údajom používateľov predstavujú závažné výzvy, ktoré si vyžadujú naliehavé kroky, keďže ide o veľa; v tejto súvislosti zdôrazňuje, že medzinárodné rámce ľudských práv, ktoré sa uplatňujú online i offline, predstavujú na globálnej úrovni významné kritérium;

13. vyzýva členské štáty, aby zabezpečili, aby obete kybernetických útokov mohli v plnej miere využívať všetky práva zakotvené v smernici 2012/29/EÚ, a zintenzívnili svoje úsilie, pokiaľ ide o identifikáciu obetí a služby poskytované obetiam, a to aj trvalou podporou osobitnej skupiny Europolu pre identifikáciu obetí; žiada členské štáty, aby v spolupráci s Europolom čo najskôr vytvorili takéto platformy s cieľom zabezpečiť, aby všetci používatelia internetu vedeli, ako požiadať o pomoc v situácii, keď sú terčom nelegálnych útokov na internete; vyzýva Komisiu, aby vydala štúdiu o dôsledkoch cezhraničnej počítačovej kriminality na základe smernice 2012/29/EÚ;

14. zdôrazňuje, že v hodnotení hrozieb internetovej organizovanej trestnej činnosti (IOCTA) Europolu z roku 2014 sa uvádza potreba efektívnejších a účinnejších právnych nástrojov s ohľadom na súčasné obmedzenia procesu zmluvy o vzájomnej právnej pomoci a takisto sa obhajuje ďalšia harmonizácia právnych predpisov v EÚ v príslušných prípadoch;

15. zdôrazňuje, že počítačová kriminalita závažným spôsobom narúša fungovanie digitálneho jednotného trhu znižovaním dôvery v poskytovateľov digitálnych služieb, narušením cezhraničných transakcií a vážnym poškodzovaním záujmov spotrebiteľov digitálnych služieb;

16. upozorňuje, že stratégie a opatrenia v oblasti kybernetickej bezpečnosti môžu byť kvalitné a účinné len v prípade, ak vychádzajú zo základných práv a slobôd zakotvených v Charte základných práv Európskej únie a zo základných hodnôt EÚ;

17. zdôrazňuje, že v záujme predchádzania počítačovej kriminalite existuje oprávnená a výrazná potreba chrániť komunikáciu medzi jednotlivcami a medzi jednotlivcami a verejnými a súkromnými organizáciami; poukazuje na to, že pri napĺňaní tejto potreby môže pomôcť silné šifrovanie; ďalej zdôrazňuje, že obmedzovanie používania alebo oslabovanie sily šifrovacích nástrojov vytvorí zraniteľné miesta, ktoré možno zneužiť na páchanie trestnej činnosti, a zníži dôveru v elektronické služby, čo bude mať zase škodlivý vplyv na občiansku spoločnosť a priemysel;

18. požaduje akčný plán na ochranu práv detí na internete aj mimo neho v kybernetickom priestore a pripomína, že v oblasti boja proti počítačovej kriminalite musia orgány presadzovania práva venovať osobitnú pozornosť trestným činom páchaným voči deťom; v tejto súvislosti zdôrazňuje, že v záujme predchádzania počítačovej kriminalite a boja proti nej,

Utorok 3. októbra 2017

a najmä proti sexuálnemu vykorisťovaniu detí na internete, je potrebné posilniť justičnú a policajnú spoluprácu medzi členskými štátmi a s Europolom a jeho Európskym centrom boja proti počítačovej kriminalite (EC3);

19. naliehavo vyzýva Komisiu a členské štáty, aby zaviedli všetky právne opatrenia na boj proti fenoménu násilia páchaného na ženách na internete a kybernetického šikanovania; osobitne žiada EÚ a členské štáty, aby spoločnými silami vytvorili trestnoprávny rámec stanovujúci online spoločnostiam povinnosť vymazať hanlivý, urážlivý a ponižujúci obsah alebo zastaviť jeho šírenie; takisto žiada, aby sa zaviedla psychologická podpora pre ženské obete násilia na internete a dievčatá vystavené kybernetickému šikanovaniu;

20. zdôrazňuje, že nelegálny online obsah by sa mal odstraňovať ihneď na základe riadneho právneho procesu; zdôrazňuje úlohu informačných a komunikačných technológií, poskytovateľov internetových služieb a poskytovateľov hostingových služieb pri zaisťovaní rýchleho a účinného odstraňovania nelegálneho online obsahu na žiadosť zodpovedného orgánu presadzovania práva;

Prevencia

21. vyzýva Komisiu, aby v kontexte preskúmania európskej stratégie kybernetickej bezpečnosti naďalej identifikovala zraniteľné miesta európskej kritickej infraštruktúry v oblasti sieťovej a informačnej bezpečnosti, stimulovala vývoj odolných systémov a posúdila situáciu v oblasti boja proti počítačovej kriminalite v EÚ a členských štátoch s cieľom dosiahnuť lepšie porozumenie trendov a vývoja v súvislosti s páchaním trestnej činnosti v kybernetickom priestore;

22. zdôrazňuje, že kybernetická odolnosť má zásadný význam z hľadiska predchádzania počítačovej kriminalite, a preto by sa jej mala venovať maximálna pozornosť; vyzýva členské štáty, aby prijali aktívne politiky a opatrenia zamerané na ochranu sietí a kritickej infraštruktúry; požaduje komplexný európsky prístup k boju proti počítačovej kriminalite v súlade so základnými právami, s ochranou údajov, kybernetickou bezpečnosťou, ochranou spotrebiteľa a elektronickým obchodom;

23. v tejto súvislosti víta investície fondov EÚ do výskumných projektov, ako je verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti, zameraných na posilnenie európskej kybernetickej odolnosti prostredníctvom inovácie a budovania kapacít; uznáva najmä úsilie verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti o primeranú reakciu na riešenie počiatočných zraniteľných miest;

24. v tomto smere zdôrazňuje dôležitosť bezplatného a slobodného softvéru; požaduje, aby sa viac prostriedkov z fondov EÚ poskytovalo osobitne na výskum bezpečnosti IT založený na bezplatnom a slobodnom softvéri;

25. so znepokojením berie na vedomie nedostatok kvalifikovaných IT-odborníkov v oblasti kybernetickej bezpečnosti; naliehavo žiada členské štáty, aby investovali do vzdelávania;

26. domnieva sa, že regulácia by mala zohrávať významnejšiu úlohu pri riadení rizík v oblasti kybernetickej bezpečnosti prostredníctvom zlepšených noriem pre produkty a softvér týkajúcich sa návrhu a následných aktualizácií, ako aj minimálnych noriem týkajúcich sa štandardných používateľských mien a hesiel;

27. naliehavo vyzýva členské štáty, aby zintenzívnili výmeny informácií prostredníctvom Eurojustu, Europolu a agentúry ENISA, ako aj výmenu najlepších postupov prostredníctvom európskej siete jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) a tímov reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT), pokiaľ ide o problémy, ktorým čelia v boji proti počítačovej kriminalite, ako aj o konkrétne právne a technické riešenia na ich odstránenie a zvýšenie kybernetickej odolnosti; v tomto smere vyzýva Komisiu, aby presadzovala účinnú spoluprácu a uľahčovala výmenu informácií s cieľom predvídať a riadiť potenciálne riziká, ako stanovuje smernica NIS;

28. vyjadruje znepokojenie v súvislosti so zistením Europolu, že väčšina úspešných útokov na jednotlivcov vzniká v dôsledku nedostatočnej digitálnej hygieny a informovanosti používateľov alebo nedostatočnej pozornosti venovanej technickým bezpečnostným opatreniam, napríklad bezpečnosti už v štádiu návrhu; zdôrazňuje, že používatelia sú prvými obeťami zle zabezpečeného hardvéru a softvéru;

29. vyzýva Komisiu a členské štáty, aby spustili informačnú kampaň so zapojením všetkých relevantných aktérov a zainteresovaných subjektov zameranú na posilnenie postavenia detí a podporu rodičov, opatrovníkov a pedagógov, pokiaľ ide o chápanie a zvládanie internetových rizík a ochranu bezpečnosti detí na internete, na podporu členských štátov pri vytváraní programov prevencie sexuálneho zneužívania online, na podporu informačných kampaní o zodpovednom správaní v sociálnych médiách a na nabádanie významných vyhľadávačov a sietí sociálnych médií k tomu, aby zaujali aktívny prístup k ochrane bezpečnosti detí na internete;

30. vyzýva Komisiu a členské štáty, aby spustili kampane zamerané na zvýšenie informovanosti a prevenciu a propagovali osvedčené postupy s cieľom zabezpečiť, aby si občania, najmä deti a iní zraniteľní používatelia, ale aj orgány ústrednej a miestnej vlády, kľúčoví prevádzkovatelia a subjekty súkromného sektora, najmä MSP, uvedomovali riziká počítačovej kriminality a vedeli, ako sa na internete chrániť a ako chrániť svoje zariadenia; ďalej vyzýva Komisiu a členské štáty, aby presadzovali praktické bezpečnostné opatrenia, napríklad šifrovanie, alebo iné bezpečnostné technológie, technológie na zlepšenie ochrany súkromia a nástroje anonymizácie;

31. zdôrazňuje, že kampane na zvýšenie informovanosti by mali byť sprevádzané vzdelávacími programami o „informovanom používaní“ nástrojov informačných technológií; odporúča členským štátom, aby do učebných plánov informatiky na školách zahrnuli kybernetickú bezpečnosť, ako aj riziká a dôsledky používania osobných údajov online; v tejto súvislosti poukazuje na úsilie vyvinuté v rámci európskej stratégie pre internet lepšie prispôsobený deťom (*Better Internet for Kids (BIK) Strategy 2012*);

32. zdôrazňuje, že v rámci boja proti počítačovej kriminalite je naliehavo potrebné venovať viac úsilia vzdelávaniu a odbornej príprave v oblasti sieťovej a informačnej bezpečnosti (NIS) zavedením školení venovaných NIS, bezpečnému vývoju softvéru a ochrane osobných údajov pre študentov informatiky, ako aj základných školení o NIS pre zamestnancov verejnej správy;

33. domnieva sa, že jedným z nástrojov podnecujúcich opatrenia v oblasti bezpečnosti tak zo strany podnikov, ktoré sa stávajú zodpovednými za návrh softvéru, ako aj používateľov, ktorým sa pripomína, aby softvér používali náležitým spôsobom, by mohlo byť poistenie proti počítačovému hakerstvu;

34. zdôrazňuje, že podniky by mali identifikovať zraniteľné miesta a riziká prostredníctvom pravidelných hodnotení, chrániť svoje produkty a služby tým, že zraniteľné miesta okamžite opravia, a to aj politikami riadenia opráv a aktualizáciami ochrany údajov, zmierňovať dôsledky útokov prostredníctvom ransomvéru tým, že vytvoria odolné záložné systémy, a dôsledne oznamovať kybernetické útoky;

35. naliehavo žiada členské štáty, aby zriadili tímy reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT), ktorým by podniky a spotrebitelia mohli oznamovať škodlivé e-maily a webové sídla, ako je stanovené v smernici o kybernetickej bezpečnosti (smernica NIS), aby členské štáty boli pravidelne informované o bezpečnostných incidentoch a opatreniach na boj proti rizikám pre ich vlastné systémy a na zmierňovanie takýchto rizík; nabáda členské štáty, aby zvážili vytvorenie databázy na zaznamenávanie všetkých druhov počítačovej kriminality a na monitorovanie vývoja príslušných javov;

36. naliehavo vyzýva členské štáty, aby investovali do lepšieho zabezpečenia svojej kritickej infraštruktúry a súvisiacich údajov, aby dokázali odolávať kybernetickým útokom;

Utorok 3. októbra 2017

Zvýšenie zodpovednosti poskytovateľov služieb

37. zastáva názor, že posilnená spolupráca príslušných orgánov s poskytovateľmi služieb je kľúčovým faktorom pri urýchlení a zefektívnení vzájomnej právnej pomoci a postupov vzájomného uznávania v medziach stanovených európskym právnym rámcom; vyzýva poskytovateľov elektronických komunikačných služieb, ktorí nemajú sídlo v Únii, aby písomne určili svojich zástupcov v Únii;

38. opakuje, že pokiaľ ide o internet vecí, sú výrobcovia kľúčovým východiskom pre sprísňovanie režimov zodpovednosti, čo povedie k vyššej kvalite produktov a bezpečnejšiemu prostrediu z hľadiska externého prístupu a možnosti zdokumentovanej aktualizácie;

39. domnieva sa, že s ohľadom na vývoj v oblasti inovácií a čoraz väčšiu prístupnosť zariadení internetu vecí by sa mala osobitná pozornosť venovať bezpečnosti všetkých, aj veľmi jednoduchých zariadení; nazdáva sa, že je v záujme výrobcov hardvéru a vývojárov inovatívneho softvéru investovať do riešení na predchádzanie počítačovej kriminalite a výmenu informácií týkajúcich sa hrozieb v oblasti kybernetickej bezpečnosti; naliehavo vyzýva Komisiu a členské štáty, aby presadzovali prístup založený na zaistení bezpečnosti už v štádiu návrhu, a žiada, aby odvetvie v prípade všetkých takýchto zariadení zahrnulo riešenia založené na zaistení bezpečnosti už v štádiu návrhu; v tejto súvislosti nabáda zástupcov súkromného sektora, aby vykonávali dobrovoľné opatrenia vyvinuté na základe príslušných právnych predpisov EÚ, ako je smernica o sieťovej a informačnej bezpečnosti, a v súlade s medzinárodne uznávanými normami s cieľom posilniť dôveru v bezpečnosť softvéru a zariadení, ako je značka dôvery internetu vecí;

40. nabáda poskytovateľov služieb, aby sa pripojili k etickému kódexu pre boj proti nelegálnym nenávistným prejavom na internete, a vyzýva Komisiu a zúčastnené podniky, aby v tejto veci naďalej spolupracovali;

41. pripomína, že podľa smernice Európskeho parlamentu a Rady 2000/31/ES z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode ([1]) (smernica o elektronickom obchode) platí pre sprostredkovateľov výnimka zo zodpovednosti za obsah len v prípade, ak vo vzťahu k prenášanému a/alebo uchovávanému obsahu zohrávajú neutrálnu a pasívnu úlohu, ale taktiež sa vyžaduje rýchla reakcia a odstránenie obsahu alebo zamedzenie prístupu k nemu v prípade, že sprostredkovateľ o porušení práva alebo nelegálnej činnosti, alebo informácii reálne vie;

42. zdôrazňuje, že je absolútne nevyhnutné chrániť databázy orgánov presadzovania práva pred bezpečnostnými incidentmi a nezákonným prístupom, keďže táto skutočnosť je pre jednotlivcov znepokojujúca; vyjadruje obavy, pokiaľ ide o extrateritoriálny dosah orgánov presadzovania práva pri prístupe k údajom v rámci vyšetrovania trestných činov, a zdôrazňuje, že v tejto oblasti treba zaviesť jasné pravidlá;

43. domnieva sa, že problémy týkajúce sa nelegálnej online aktivity treba riešiť rýchlo a účinne, a to aj prostredníctvom postupov odstraňovania obsahu, ak obsah už nie je potrebný na účely odhaľovania, vyšetrovania a stíhania; pripomína, že ak odstránenie obsahu nie je možné, členské štáty môžu prijať potrebné a primerané opatrenia na zablokovanie prístupu k nemu z územia Únie; zdôrazňuje, že takéto opatrenia musia byť v súlade s existujúcimi legislatívnymi a súdnymi postupmi, ako aj s chartou a že tiež sa na ne musia vzťahovať primerané záruky vrátane možnosti súdnych prostriedkov nápravy;

44. zdôrazňuje úlohu poskytovateľov služieb digitálnej informačnej spoločnosti pri zabezpečovaní rýchleho a účinného odstraňovania nelegálneho online obsahu na žiadosť zodpovedného orgánu presadzovania práva a víta pokrok, ktorý sa dosiahol v tomto smere, a to aj prostredníctvom prínosu internetového fóra EÚ; podčiarkuje potrebu väčšej angažovanosti a spolupráce príslušných orgánov a poskytovateľov služieb informačnej spoločnosti s cieľom dosiahnuť rýchle a efektívne odstránenie obsahu zo strany odvetvia a zabrániť zablokovaniu nelegálneho obsahu prostredníctvom vládnych opatrení; vyzýva členské štáty, aby vyvodili právnu zodpovednosť voči platformám porušujúcim príslušné pravidlá; opakuje, že akékoľvek opatrenia na odstránenie nelegálneho online obsahu, ktorými sa stanovujú podmienky, by mali byť povolené len v prípade, že vnútroštátne procesné pravidlá umožňujú používateľom uplatňovať svoje práva pred súdom po tom, ako sa dozvedeli o týchto opatreniach;

45. zdôrazňuje, že v súlade s uznesením Európskeho parlamentu z 19. januára 2016 o iniciatíve s názvom Smerom k aktu o jednotnom digitálnom trhu ([2]) je obmedzená zodpovednosť sprostredkovateľov zásadne dôležitá pre ochranu otvorenosti internetu, základných práv, právnej istoty a inovácie; víta zámer Komisie stanoviť usmernenie týkajúce sa postupov odstraňovania obsahu na základe upozornenia, podporiť online platformy pri plnení ich povinností a pravidiel

([1]) Ú. v. EÚ L 178, 17.7.2000, s. 1.
([2]) Prijaté texty, P8_TA(2016)0009.

o zodpovednosti podľa smernice o elektronickom obchode (2000/31/ES), posilniť právnu istotu a zvýšiť dôveru používateľov; naliehavo vyzýva Komisiu, aby v tejto veci predložila legislatívny návrh;

46. žiada uplatňovanie prístupu „sledovania toku peňazí“, ako sa uvádza v uznesení Európskeho parlamentu z 9. júna 2015 o oznámení „Cesta k obnovenému konsenzu o vymožiteľnosti práv duševného vlastníctva: Akčný plán EÚ“ ([1]) na základe regulačného rámca smernice o elektronickom obchode a smernice o vymožiteľnosti práv duševného vlastníctva;

47. zdôrazňuje zásadný význam poskytovania nepretržitej a osobitnej odbornej prípravy a psychologickej podpory tzv. moderátorom obsahu v súkromných a verejných subjektoch, ktorí sú zodpovední za posudzovanie sporného alebo nelegálneho online obsahu, keďže by mali byť považovaní za osoby poskytujúce prvotnú reakciu v tejto oblasti;

48. vyzýva poskytovateľov služieb, aby stanovili jednoznačné spôsoby oznamovania a zaviedli riadne vymedzenú vnútornú infraštruktúru, ktorá umožní rýchlu a primeranú reakciu na oznámenia;

49. vyzýva poskytovateľov služieb, aby zintenzívnili úsilie zamerané na zvýšenie informovanosti o rizikách spojených s pripojením na internet, najmä pre deti, a to tým, že vyvinie interaktívne nástroje a informačné materiály;

Posilnenie policajnej a justičnej spolupráce

50. je znepokojený výrazným počtom nepotrestaných počítačových trestných činov; vyjadruje hlboké poľutovanie nad tým, že využívanie technológií ako NAT CGN poskytovateľmi internetových služieb vážne poškodzuje vyšetrovania tým, že z technického hľadiska znemožňuje presnú identifikáciu používateľa IP adresy, a teda určenie osoby zodpovednej za trestné činy na internete; zdôrazňuje potrebu umožniť orgánom presadzovania práva zákonný prístup k relevantným informáciám, a to za obmedzených okolností, ak je takýto prístup potrebný a primeraný z dôvodu bezpečnosti a spravodlivosti; zdôrazňuje, že súdnym orgánom a orgánom presadzovania práva treba poskytnúť dostatočné kapacity na vykonávanie vyšetrovaní v súlade so zákonom;

51. naliehavo vyzýva členské štáty, aby poskytovateľom šifrovania neukladali žiadne povinnosti, ktoré by viedli k oslabeniu alebo ohrozeniu bezpečnosti ich sietí alebo služieb, napríklad povinnosť vytvoriť tzv. zadné vrátka alebo uľahčiť ich používanie; zdôrazňuje, že treba ponúkať realizovateľné riešenia, a to tak prostredníctvom právnych predpisov, ako aj neustáleho technologického vývoja, ak sú tieto riešenia nevyhnutné pre spravodlivosť a bezpečnosť; vyzýva členské štáty, aby v rámci konzultácií so súdnictvom a Eurojustom spolupracovali pri zosúlaďovaní podmienok pre zákonné používanie online vyšetrovacích nástrojov;

52. zdôrazňuje, že legálne odpočúvanie môže byť veľmi účinným opatrením na boj proti nelegálnemu hakerstvu, a to pod podmienkou, že je nevyhnutné, primerané, založené na riadnom právnom procese a v plnom súlade so základnými právami a právom a judikatúrou EÚ o ochrane údajov; vyzýva všetky členské štáty, aby využívali možnosti legálneho odpočúvania zameraného na podozrivých jednotlivcov, stanovili jasné pravidlá týkajúce sa postupu udelenia predchádzajúceho súdneho povolenia pre aktivity legálneho odpočúvania vrátane obmedzení používania a trvania legálnych nástrojov hakerstva, zriadili mechanizmus dohľadu a poskytovali účinné právne prostriedky nápravy pre ciele hakerských aktivít;

53. vyzýva členské štáty, aby spolupracovali s komunitou pre bezpečnosť IKT a nabádali ju, aby zohrávala aktívnejšiu úlohu v rámci tzv. etického hakerstva (white hat hacking) a pri oznamovaní nezákonného obsahu, ako je materiál z oblasti sexuálneho zneužívania detí;

54. nabáda Europol, aby vytvoril anonymný systém oznamovania zo skrytých sietí, ktorý umožní jednotlivcom oznamovať nezákonný obsah, napríklad materiál zobrazujúci sexuálne zneužívanie detí, príslušným orgánom prostredníctvom technických záruk podobných tým, ktoré zaviedli viaceré tlačové organizácie využívajúce takéto systémy na uľahčenie výmeny citlivých údajov s novinármi spôsobom, ktorý umožňuje vyššiu mieru anonymity a bezpečnosti, než aké poskytuje bežný e-mail;

([1]) Ú. v. EÚ C 407, 4.11.2016, s. 25.

Utorok 3. októbra 2017

55. zdôrazňuje, že je potrebné minimalizovať riziká pre súkromie používateľov internetu vyplývajúce z úniku riešení alebo nástrojov, ktoré využívajú orgány presadzovania práva v rámci svojich vyšetrovaní v súlade so zákonom;

56. upozorňuje, že súdne orgány a orgány presadzovania práva musia mať dostatočnú kapacitu a finančné prostriedky, aby mohli účinne reagovať na počítačovú kriminalitu;

57. zdôrazňuje, že zmes samostatných, územne vymedzených vnútroštátnych jurisdikcií spôsobuje problémy pri určovaní uplatniteľného práva v cezhraničných interakciách a vytvára právnu neistotu, čo bráni cezhraničnej spolupráci, ktorá je potrebná na účinné riešenie prípadov počítačovej kriminality;

58. zdôrazňuje, že treba vypracovať praktický základ pre spoločný prístup EÚ k otázke jurisdikcie v kybernetickom priestore, ako bolo zdôraznené na neformálnom stretnutí ministrov spravodlivosti a vnútra, ktoré sa konalo 26. januára 2016;

59. v tejto súvislosti upozorňuje, že treba jednak vypracovať spoločné procesné normy, ktorými možno stanoviť územné faktory, ktoré sú základom pre uplatniteľné právo v kybernetickom priestore, jednak vymedziť vyšetrovacie opatrenia, ktoré možno použiť bez ohľadu na geografické hranice;

60. uznáva, že takýmto spoločným európskym prístupom, ktorý musí rešpektovať základné práva a súkromie, sa vybuduje dôvera medzi zainteresovanými subjektmi, znížia sa oneskorenia pri vybavovaní cezhraničných žiadostí, zavedie sa interoperabilita medzi rôznorodými subjektmi a poskytne sa možnosť začleniť do operačných rámcov požiadavky týkajúce sa riadneho procesu;

61. vyjadruje presvedčenie, že spoločné procesné normy v oblasti presadzovania práva v kybernetickom priestore by sa mali v dlhodobom horizonte vyvinúť aj na globálnej úrovni; v tomto smere víta činnosť výboru Rady Európy pre počítačovú kriminalitu;

Elektronické dôkazy

62. zdôrazňuje, že spoločný európsky prístup k trestnému súdnictvu v kybernetickom priestore je prioritou, keďže zlepší presadzovanie zásady právneho štátu v kybernetickom priestore a uľahčí získavanie elektronických dôkazov v trestných konaniach a takisto prispeje k oveľa rýchlejšiemu vyšetreniu prípadov, než je tomu v súčasnosti;

63. vyzdvihuje potrebu nájsť prostriedky na rýchlejšie zabezpečenie a získanie elektronických dôkazov, ako aj dôležitosť úzkej spolupráce orgánov presadzovania práva, a to aj prostredníctvom intenzívnejšieho využívania spoločných vyšetrovacích tímov, tretích krajín a poskytovateľov služieb pôsobiacich na európskom území, v súlade s ustanoveniami všeobecného nariadenia o ochrane údajov ((EÚ) 2016/679), smernice (EÚ) 2016/680 (policajná smernica) a existujúcich dohôd o vzájomnej právnej pomoci; zdôrazňuje potrebu zriadiť jednotné kontaktné miesta vo všetkých členských štátoch a optimalizovať využívanie existujúcich kontaktných miest, keďže sa tým uľahčí prístup k elektronickým dôkazom, ako aj výmena informácií, zlepší sa spolupráca s poskytovateľmi služieb a urýchlia sa postupy vzájomnej právnej pomoci;

64. uznáva, že v súčasnosti roztrieštený právny rámec môže spôsobiť problémy poskytovateľom služieb, ktorí chcú plniť požiadavky v oblasti presadzovania práva; vyzýva Komisiu, aby predložila európsky právny rámec pre elektronické dôkazy vrátane harmonizovaných pravidiel na určenie postavenia poskytovateľa ako domáceho alebo zahraničného poskytovateľa a uložila poskytovateľom služieb povinnosť reagovať na žiadosti z iných členských štátov na základe riadneho právneho procesu a v súlade s európskym vyšetrovacím príkazom (EVP), pričom zohľadní zásadu proporcionality s cieľom zabrániť nepriaznivým účinkom na uplatňovanie slobody usadiť sa a slobody poskytovať služby a zabezpečí primerané záruky v záujme stanovenia právnej istoty, ako aj zlepšenia schopnosti poskytovateľov služieb a sprostredkovateľov reagovať na požiadavky v oblasti presadzovania práva;

65. zdôrazňuje, že je potrebné, aby akýkoľvek rámec pre elektronické dôkazy zahŕňal dostatočné záruky v oblasti práv a slobôd všetkých zúčastnených; zdôrazňuje, že by to malo zahŕňať požiadavku, aby žiadosti o elektronické dôkazy boli v prvom rade adresované prevádzkovateľom alebo vlastníkom údajov, aby sa zaistilo rešpektovanie ich práv, ako aj práv tých, s ktorými údaje súvisia (napríklad ich právo trvať na uplatňovaní povinnosti advokáta zachovávať mlčanlivosť a domáhať sa právneho prostriedku nápravy v prípade neprimeraného alebo inak nezákonného prístupu); zdôrazňuje tiež

potrebu zaistiť, aby každý právny rámec chránil poskytovateľov a všetky ostatné strany pred žiadosťami, ktoré by mohli spôsobiť kolíziu právnych poriadkov alebo inak narušiť zvrchovanosť iných štátov;

66. vyzýva členské štáty, aby v plnej miere vykonávali smernicu 2014/41/EÚ o európskom vyšetrovacom príkaze v trestných veciach (smernica o EVP) na účely účinného zabezpečovania a získavania elektronických dôkazov v EÚ a aby do svojich vnútroštátnych trestných kódexov zahrnuli konkrétne ustanovenia týkajúce sa kybernetického priestoru v záujme uľahčenia prípustnosti elektronických dôkazov na súde a aby umožnili vydávať jasnejšie usmernenia pre sudcov, pokiaľ ide o trestanie počítačovej kriminality;

67. víta pokračujúcu činnosť Komisie v súvislosti s platformou spolupráce s bezpečným komunikačným kanálom na digitálnu výmenu európskych vyšetrovacích príkazov týkajúcich sa elektronických dôkazov, ako aj odpovedí medzi súdnymi orgánmi EÚ; vyzýva Komisiu, aby spolu s členskými štátmi, Eurojustom a poskytovateľmi služieb preskúmala a zjednotila formuláre, nástroje a postupy žiadostí o zabezpečenie a získanie elektronických dôkazov s cieľom uľahčiť overovanie, zaistiť rýchle postupy a zvýšiť transparentnosť a spoľahlivosť procesu zabezpečovania a získavania elektronických dôkazov; vyzýva Agentúru Európskej únie pre odbornú prípravu v oblasti presadzovania práva (CEPOL), aby vytvorila moduly odbornej prípravy na účinné využívanie existujúcich rámcov používaných na zabezpečovanie a získavanie elektronických dôkazov; v tejto súvislosti zdôrazňuje, že zefektívnenie politík poskytovateľov služieb pomôže znížiť rôznorodosť prístupov, najmä v oblasti postupov a podmienok poskytovania prístupu k požadovaným údajom;

Budovanie kapacít na európskej úrovni

68. pripomína, že nedávne incidenty jasne poukázali na závažnú zraniteľnosť EÚ, najmä inštitúcií EÚ, národných vlád a parlamentov, významných európskych podnikov a európskej IT infraštruktúry a sietí voči sofistikovaným útokom využívajúcim zložitý softvér a malvér; vyzýva Agentúru Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), aby neustále hodnotila úroveň hrozby, a žiada Komisiu, aby investovala do kapacity v oblasti IT, ako aj ochrany a odolnosti kritickej infraštruktúry inštitúcií EÚ s cieľom znížiť zraniteľnosť EÚ voči závažným kybernetickým útokom veľkých zločineckých organizácií, štátom podporovaným útokom alebo teroristickým skupinám;

69. uznáva dôležitý prínos Európskeho centra boja proti počítačovej kriminalite (EC3) v rámci Europolu a Eurojustu, ako aj Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) k boju proti počítačovej kriminalite;

70. vyzýva Europol, aby podporoval vnútroštátne orgány presadzovania práva pri vytváraní bezpečných a vhodných prenosových kanálov;

71. vyjadruje hlboké poľutovanie nad tým, že v súčasnosti neexistujú žiadne normy EÚ pre odbornú prípravu a certifikáciu; uznáva, že budúci vývoj v oblasti počítačovej kriminality si od správcov vyžaduje čoraz vyššiu úroveň odborných znalostí; víta, že existujúce iniciatívy, ako sú Európska skupina pre vzdelávanie a odbornú prípravu v oblasti boja proti počítačovej kriminalite (ECTEG), projekt odbornej prípravy školiteľov a školenia v rámci politického cyklu EÚ, už dláždia cestu pre riešenie problému medzery v oblasti odborných znalostí na úrovni EÚ;

72. vyzýva agentúru CEPOL a Európsku sieť odbornej justičnej prípravy, aby rozšírili svoju ponuku kurzov odbornej prípravy venovaných témam súvisiacim s počítačovou kriminalitou pre príslušné orgány presadzovania práva a súdne orgány v celej Únii;

73. zdôrazňuje, že počet prípadov počítačovej kriminality oznámených Eurojustu sa zvýšil o 30 %; žiada o vyčlenenie dostatočných finančných prostriedkov a v prípade potreby aj o zvýšenie počtu pracovných miest s cieľom umožniť, aby Eurojust zvládal zvýšenú pracovnú záťaž v oblasti počítačovej kriminality a ďalej rozvíjal a posilňoval svoju podporu vnútroštátnych prokurátorov pre počítačovú kriminalitu v cezhraničných prípadoch, a to aj prostredníctvom nedávno zriadenej Európskej justičnej siete na boj proti počítačovej kriminalite;

74. požaduje preskúmanie mandátu agentúry ENISA a posilnenie vnútroštátnych agentúr pôsobiacich v oblasti kybernetickej bezpečnosti; vyzýva na posilnenie agentúry ENISA z hľadiska jej úloh, personálneho obsadenia a zdrojov; zdôrazňuje, že nový mandát by mal zahŕňať aj silnejšie väzby s Europolom a zainteresovanými stranami z odvetvia, aby agentúra mohla lepšie podporovať príslušné orgány v boji proti počítačovej kriminalite;

Utorok 3. októbra 2017

75. žiada Agentúru pre základné práva (FRA), aby vypracovala praktickú a podrobnú príručku obsahujúcu usmernenia pre členské štáty v oblasti dohľadu a dozoru;

Užšia spolupráca s tretími krajinami

76. zdôrazňuje dôležitosť úzkej spolupráce s tretími krajinami v rámci globálneho boja proti počítačovej kriminalite, a to aj prostredníctvom výmeny najlepších postupov, spoločných vyšetrovaní, budovania kapacít a vzájomnej právnej pomoci;

77. vyzýva členské štáty, ktoré tak ešte neurobili, aby ratifikovali a v plnej miere vykonávali Dohovor Rady Európy o počítačovej kriminalite z 23. novembra 2001 (Budapeštiansky dohovor), ako aj dodatočné protokoly k nemu a aby ho v spolupráci s Komisiou presadzovali na príslušných medzinárodných fórach;

78. poukazuje na vážne obavy súvisiace s činnosťou v rámci výboru Rady Európy pre Dohovor o počítačovej kriminalite, pokiaľ ide o výklad článku 32 Budapeštianskeho dohovoru o cezhraničnom prístupe k uchovávaným počítačovým údajom (tzv. cloudové dôkazy), a je proti akémukoľvek uzatváraniu dodatkového protokolu alebo usmernenia zameraného na rozšírenie rozsahu pôsobnosti tohto ustanovenia nad rámec súčasného režimu zavedeného týmto dohovorom, ktorý je už veľkou výnimkou zo zásady teritoriality, pretože by to mohlo viesť k neobmedzenému diaľkovému prístupu orgánov presadzovania práva k serverom a počítačom umiestneným v iných jurisdikciách bez využitia vzájomnej právnej pomoci a iných nástrojov justičnej spolupráce zavedených na zaistenie základných práv jednotlivca vrátane ochrany údajov a riadneho procesu, najmä dohovoru Rady Európy č. 108;

79. vyjadruje poľutovanie nad tým, že v oblasti počítačovej kriminality neexistuje žiadny záväzný medzinárodný právny predpis, a naliehavo žiada členské štáty a európske inštitúcie, aby vypracovali takýto dohovor;

80. vyzýva Komisiu, aby navrhla možnosti iniciatív na zlepšenie účinnosti a na podporu využívania zmlúv o vzájomnej právnej pomoci ako protiváhy k prevzatiu extrateritoriálnej jurisdikcie tretími krajinami;

81. vyzýva členské štáty, aby zaistili dostatočné kapacity na spracovanie žiadostí o vzájomnú právnu pomoc v súvislosti s vyšetrovaniami v kybernetickom priestore a aby vytvorili príslušné programy odbornej prípravy pre pracovníkov zodpovedných za spracovanie týchto žiadostí;

82. zdôrazňuje, že dohody o strategickej a operačnej spolupráci medzi Europolom a tretími krajinami uľahčujú tak výmenu informácií, ako aj praktickú spoluprácu;

83. berie na vedomie, že najvyšší počet žiadostí týkajúcich sa presadzovania práva sa zasiela do Spojených štátov amerických a Kanady; vyjadruje znepokojenie v súvislosti s tým, že miera zverejňovania údajov veľkými poskytovateľmi služieb v USA v reakcii na žiadosti európskych orgánov trestného súdnictva nedosahuje ani 60 %, a pripomína, že podľa kapitoly V všeobecného nariadenia o ochrane údajov sú uprednostňovaným mechanizmom, ktorý umožňuje prístup k osobným údajom uchovávaných v zahraničí, zmluvy o vzájomnej právnej pomoci a iné medzinárodné dohody;

84. vyzýva Komisiu, aby predložila konkrétne opatrenia na ochranu základných práv podozrivých alebo obvinených osôb pri výmene informácií medzi európskymi orgánmi presadzovania práva a tretími krajinami, najmä záruk, pokiaľ ide o rýchle získanie relevantných dôkazov na základe súdneho rozhodnutia, ako aj získanie informácií týkajúcich sa účastníka alebo podrobných metaúdajov a údajov o obsahu (ak nie sú zašifrované) od orgánov presadzovania práva a/alebo poskytovateľov služieb, s cieľom zlepšiť vzájomnú právnu pomoc;

85. vyzýva Komisiu, aby v spolupráci s členskými štátmi, príslušnými európskymi orgánmi a v prípade potreby aj tretími krajinami zvážila nové spôsoby efektívneho zabezpečovania a získavania elektronických dôkazov uchovávaných v tretích krajinách, v plnom súlade so základnými právami a s právnymi predpismi EÚ o ochrane údajov, a to tým, že urýchli a zjednoduší využívanie postupov vzájomnej právnej pomoci a prípadne i vzájomné uznávanie;

86. zdôrazňuje dôležitosť centra NATO pre reakciu na kybernetické incidenty;

87. vyzýva všetky členské štáty, aby sa zapojili do Globálneho fóra o kybernetických odborných znalostiach (GFCE) s cieľom uľahčiť vytváranie partnerstiev zameraných na budovanie kapacít;

88. podporuje pomoc pri budovaní kapacít, ktorú EÚ poskytuje krajinám východného susedstva, keďže mnoho kybernetických útokov má pôvod v týchto krajinách;

o

o o

89. poveruje svojho predsedu, aby postúpil toto uznesenie Rade a Komisii.