Europa-Parlamentet
2014-2019

Mødedokument

A8-0272/2017

25.7.2017

BETÆNKNING

om bekæmpelse af it-kriminalitet
(2017/2068(INI))

Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender

Ordfører: Elissavet Vozemberg-Vrionidi

INDHOLD

Side

FORSLAG TIL EUROPA-PARLAMENTETS BESLUTNING

om bekæmpelse af it-kriminalitet
(2017/2068(INI))

Europa-Parlamentet,

– der henviser til artikel 2, 3 og 6 i traktaten om Den Europæiske Union (TEU),

– der henviser til artikel 16, 67, 70, 72, 73, 75, 82, 83, 84, 85, 87 og 88 i traktaten om Den Europæiske Unions funktionsmåde (TEUF),

– der henviser til artikel 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 og 52 i Den Europæiske Unions charter om grundlæggende rettigheder,

– der henviser til FN's konvention af 20. november 1989 om barnets rettigheder,

– der henviser til den valgfri protokol af 25. maj 2000 til FN-konventionen om barnets rettigheder vedrørende salg af børn, børneprostitution og børnepornografi,

– der henviser til Stockholm-erklæringen og handlingsplanen, som blev vedtaget på den 1. verdenskongres mod seksuel udnyttelse af børn i kommercielt øjemed, det globale tilsagn, som blev vedtaget i Yokohama på den 2. verdenskongres mod seksuel udnyttelse af børn i kommercielt øjemed, samt tilsagnet og handlingsplanen, der blev vedtaget i Budapest på den forberedende konference til den 2. verdenskongres mod seksuel udnyttelse af børn i kommercielt øjemed,

– der henviser til Europarådets konvention af 25. oktober 2007 om beskyttelse af børn mod seksuel udnyttelse og seksuelt misbrug,

– der henviser til sin beslutning af 20. november 2012 om beskyttelse af børn i den digitale verden[1],

– der henviser til sin beslutning af 11. marts 2015 om seksuelt misbrug af børn på internettet[2],

– der henviser til Rådets rammeafgørelse af 28. maj 2001 om bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter[3],

– der henviser til Budapest-konventionen om IT-kriminalitet af 23. november 20012[4] med den supplerende protokol,

– der henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed[5],

– der henviser til Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og

[1] EUT C 419 af 16.12.2015, s. 33.
[2] EUT C 316 af 30.8.2016, s. 109.
[3] EFT L 149 af 2.6.2001, s. 1.
[4] Europarådet, European Treaty Series nr. 185, 23.11.2001.
[5] EUT L 77 af 13.3.2004, s. 1.

udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre[1],

– der henviser til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor[2],

– der henviser til Europa-Parlamentets og Rådets direktiv 2011/92/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug af børn, seksuel udnyttelse af børn og børnepornografi og om ophævelse af rammeafgørelse 2004/68/RIA[3],

– der henviser til den fælles meddelelse af 7. februar 2013 til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget fra Kommissionen og næstformanden i Kommissionen/Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik med titlen "Den Europæiske Unions strategi for it-sikkerhed: "Et åbent, sikkert og beskyttet internet" (JOIN(2013)0001),

– der henviser til Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA[4],

– der henviser til Europa-Parlamentets og Rådets direktiv 2014/41/EU af 3. april 2014 om den europæiske efterforskningskendelse i straffesager[5],

– der henviser til fra Den Europæiske Unions Domstol dok af 8. april 2014, som ophævede EU-datalagringsdirektivet,

– der henviser til sin beslutning af 12. september 2013 om EU's strategi for it-sikkerhed: Et åbent, sikkert og beskyttet internet[6],

– der henviser til Kommissionens meddelelse af 6. maj 2015 med titlen "En strategi for et digitalt indre marked" (COM(2015)0192),

– der henviser til Kommissionens meddelelse af 28. april 2015 med titlen "Den europæiske dagsorden om sikkerhed" (COM(2015)0185) og de efterfølgende statusrapporter om indførelsen af en effektiv og ægte sikkerhedsunion",

– der henviser til rapporten fra konferencen om jurisdiktion på internettet, der blev afholdt i Amsterdam d. 7. og 8. marts 2016,

– der henviser til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af

[1] EUT L 345 af 23.12.2008, s. 75.
[2] EFT L 201 af 31.7.2002, s. 37.
[3] EUT L 335 af 17.12.2011, s. 1.
[4] EUT L 218 af 14.8 2013, s. 8.
[5] EUT L 130 af 1.5.2014, s. 1.
[6] EUT C 93 af 9.3 2016, s. 112.

direktiv 95/46/EF (generel forordning om databeskyttelse)[1],

– der henviser til Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA[2],

– der henviser til Europa-Parlamentets og Rådets forordning (EU) 2016/794 af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol)[3],

– der henviser til Kommissionens afgørelse af 5. juli 2016 om undertegnelse af en kontrakt om et offentlig-privat partnerskab for it-sikkerhed, industriel forskning og innovation mellem Den Europæiske Union, repræsenteret ved Kommissionen, og interessentorganisationen (C(2016)4400),

– der henviser til den fælles meddelelse af 6. april 2016 til Europa-Parlamentet og Rådet med titlen "Fælles ramme for imødegåelse af hybride trusler Den Europæiske Unions indsats" (JOIN(2016)0018),

– der henviser til Kommissionens meddelelse med titlen "Europæisk strategi for et bedre internet for børn " (COM(2012)0196) og til Kommissionens rapport af 6. juni 2016 med titlen "Endelig evaluering af det flerårige EU-program om beskyttelse af børn, der bruger internettet og andre kommunikationsteknologier (et sikrere internet)" (COM(2016)0364),

– der henviser til Europol og ENISA's fælles erklæring af 20. maj 2016 om lovmæssig strafferetlig efterforskning, som respekterer det 21. århundredes databeskyttelse;

– der henviser til Rådets konklusioner af 9. juni 2016 om oprettelse af Det Europæiske Retlige Netværk for It-kriminalitet;

– der henviser til Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen[4],

– der henviser til ENISA's skriftlige udtalelse af december 2016 om kryptering – Stærk kryptering beskytter vores digitale identitet,

– der henviser til den endelige rapport fra Europarådets T-CY Cloud Evidence Group med titlen "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY" af 16. september 2016,

– der henviser til arbejdet i den fælles taskforce om it-kriminalitet (J-CAT),

[1] EUT L 119 af 4.5.2016, s. 1.
[2] EUT L 119 af 4.5.2016, s. 89.
[3] EUT L 135 af 24.5 2016, s. 53.
[4] EUT L 194 af 19.7.2016, s. 1.

– der henviser til Europols SOCTA-rapport (trusselsvurdering af grov og organiseret kriminalitet) af 28. februar 2017 og IOCTA-rapporten (trusselsvurderingen af organiseret internetkriminalitet) af 28. september 2016,

– der henviser til EU-Domstolens dom i sag C-203/15 (Tele2-dommen) af 21. december 2016[1],

– der henviser til Europa-Parlamentets og Rådets direktiv 2017/541/EU af 15. marts 2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA[2],

– der henviser til forretningsordenens artikel 52,

– der henviser til betænkning fra Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender og til udtalelse fra Udvalget om det Indre Marked og Forbrugerbeskyttelse (A8-0272/2017),

A. der henviser til, at it-kriminalitet forårsager stadig større økonomiske og samfundsmæssige skader, der påvirker borgernes grundlæggende rettigheder, udgør en trussel mod retsstatsprincippet på internettet og truer stabiliteten i de demokratiske samfund;

B. der henviser til, at it-kriminalitet er et stigende problem i medlemsstaterne,

C. der henviser til, at IOCTA-rapporten fra 2016 viser, at it-kriminalitet er steget i intensitet, kompleksitet og omfang, at anmeldt it-kriminalitet overstiger traditionel kriminalitet i nogle EU-lande, at det udvikler sig til at omfatte andre kriminalitetsområder som f.eks. menneskehandel, at anvendelsen af krypterings- og anonymiseringsværktøjer til kriminelle formål er stigende, og at antallet af angreb med ransomware er større end traditionelle malwaretrusler som trojanske heste;

D. der henviser til, at der var 20 % flere angreb på Kommissionens servere i 2016 end i 2015;

E. der henviser til, at computeres sårbarheder skyldes den specifikke måde, som informationsteknologien har udviklet sig på gennem årene, den hastighed hvormed internethandlen vokser og den manglende indsats fra myndighedernes side;

F. der henviser til, at der er et stadigt voksende sort marked for digital pengeafpresning, anvendelse af lejede botnet og hacking samt tyveri af digitale varer;

G. der henviser til, at det centrale fokus for it-angreb fortsat er på malware som f.eks. banktrojanere, men at der er et stigende antal mere alvorlige angreb på industrielle styringssystemer og netværk, der sigter mod at ødelægge kritisk infrastruktur og økonomiske strukturer og destabilisere samfund, som det var tilfældet med hackerangrebet "WannaCry" for i maj 2017, hvilket udgør en alvorlig trussel mod sikkerheden, forsvaret og andre vigtige sektorer; der henviser til, at hovedparten af

[1] Domstolens dom af 21. december 2016, Tele2 Sverige AB mod Post- och telestyrelsen og statssekretæren i Indenrigsministeriet mod Tom Watson m.fl., C-203/15, ECLI:EU:C:2016:970.
[2] EUT L 88 af 31.3.2017, s. 6.

internationale anmodninger fra politiet vedrører oplysninger om svig og finansiel kriminalitet efterfulgt af voldskriminalitet og anden grov kriminalitet;

H. der henviser til, at den konstant voksende indbyrdes forbundethed mellem mennesker, steder og ting medfører mange fordele, men at det indebærer en stigende risiko for it-kriminalitet; der henviser til, at udstyr, der er tilknyttet tingenes internet (IoT) og omfatter intelligente net, køleskabe, biler, medicinsk udstyr eller hjælpemidler, ofte ikke er så godt beskyttet som traditionelt internetudstyr og derfor er et ideelt mål for it-kriminelle, i særdeleshed fordi systemet med sikkerhedsopdateringer til forbundne enheder ofte er utilstrækkelig eller til tider slet ikke forefindes; der henviser til, at hackede enheder fra tingenes internet, som indeholder eller kan styre fysiske aktuatorer, kan udgøre en konkret trussel for menneskers liv;

I. der henviser til, at en effektiv retlig ramme for databeskyttelse er afgørende for at opbygge tillid og tiltro i internetverdenen og dermed gøre det muligt for forbrugerne og virksomhederne at få det fulde udbytte af det digitale indre marked og samtidig gribe ind over for it-kriminalitet;

J. der henviser til, at virksomheder ikke kan tackle problemet med at gøre den forbundne verden mere sikker alene, og at statsmagten bør bidrage til at forbedre it-sikkerheden gennem lovgivning og ved at indføre incitamenter, der fremmer sikker adfærd blandt brugerne;

K. der henviser til, at linjerne mellem it-kriminalitet, it-spionage, it-sabotage, it-krigsførelse og it-terrorisme bliver stadigt mere uklare; der henviser til, at it-kriminalitet kan være rettet mod enkeltpersoner, offentlige eller private enheder og omfatte en lang række lovovertrædelser, herunder krænkelse af privatlivets fred, seksuelle overgreb på børn over internettet, offentlig tilskyndelse til vold eller had, sabotage, spionage, økonomisk kriminalitet og svig som f.eks. betalingssvig, tyveri og identitetstyveri samt ulovligt indgreb i informationssystemer;

L. der henviser til, at databedrageri og -tyveri er anført i den globale risikovurderingsrapport 2017 fra World Economic Forum som et af de fem største globale risici for så vidt angår sandsynligheden for, at de indtræffer;

M. der henviser til, at en betydelig mængde it-kriminalitet ikke er blevet retsforfulgt og straffet; der henviser til, at der fortsat er en betydelig underrapportering, lange sporingsperioder, der gør det muligt for it-kriminelle at udvikle flere forskellige indgange/udgange eller bagdøre, vanskelig adgang til elektronisk bevismateriale, problemer med at indhente dette og få det antaget i retten samt komplicerede procedurer og juridiske problemer, som skyldes it-kriminalitetens grænseoverskridende karakter;

N. der henviser til, at Rådet i sine konklusioner fra juni 2016 understregede, at et bedre samarbejde og en bedre informationsudveksling mellem politiet og de retlige myndigheder og eksperter i it-kriminalitet i betragtning af it-kriminalitetens grænseoverskridende karakter samt de fælles trusler mod it-sikkerheden, som EU står over for, er afgørende for en effektiv efterforskning på internettet og for sikring af elektronisk bevismateriale;

O. der henviser til, at EU-domstolens annullering af datalagringsdirektivet i dommen af 8.

april 2014 samt forbuddet mod generel, vilkårlig og ikke-målrettet datalagring, som bekræftet af EU-domstolens Tele2-dom af 21. december 2016 fastsætter snævre grænser for behandlingen af store mængder telekommunikationsdata samt for de kompetente myndigheders adgang til sådanne oplysninger

P. der henviser til, at EU-Domstolens Maximillian Schrems-dom understreger, at masseovervågning er en krænkelse af grundlæggende rettigheder;

Q. der henviser til, at bekæmpelse af it-kriminalitet skal sikre de samme proceduremæssige og substantielle garantier og grundlæggende rettigheder, navnlig vedrørende databeskyttelse og ytringsfrihed, som det er tilfældet i forbindelse med bekæmpelsen af alle andre former for kriminalitet;

R. der henviser til, at børn er særligt sårbare over for online grooming og andre former for seksuel udnyttelse på internettet (it-modning, seksuelle overgreb. seksuel tvang og seksuel afpresning), misbrug af personoplysninger og farlige kampagner, der har til formål at fremme forskellig former for selvbeskadigelse, som tilfældet med ”blue whale”, og derfor kræver særlig beskyttelse; der henviser til, at gerningsmænd på internettet kan finde og groome ofre hurtigere via chatrooms, e-mail, onlinespil og sociale netværk, og at skjulte peer-to-peer-netværk (P2P) stadig er de centrale platforme, som børnesexforbrydere anvender til at få adgang til, sprede, lagre og dele materiale, der viser seksuel udnyttelse af børn, og til at søge efter nye ofre uden at blive opdaget;.

S. der henviser til, at den stigende tendens til seksuel tvang og afpresning fortsat ikke anmeldes og undersøges i tilstrækkelig grad, hovedsageligt på grund af forbrydelsernes natur, som forårsager skam- og skyldfølelser hos ofrene;

T. der henviser til, at der er meldinger om direkte transmission af "fjernmisbrug" af børn som en stigende trussel. Der henviser til, at direkte transmission af fjernmisbrug af børn helt er det mest åbenlyse eksempel på kommerciel distribution af materiale med seksuel udnyttelse af børn.

U. der henviser til, at kriminalpolitiet i Det Forenede Kongeriges har konstateret, at unge, der deltager i hackingaktiviteter, i mindre grad er motiveret af penge og ofte angriber computernetværk for at imponere venner eller protestere mod et politisk system.

V. der henviser til, at bevidstheden om risiciene ved it-kriminalitet er stigende, men at forebyggende foranstaltninger for private brugere, offentlige institutioner og erhvervslivet fortsat er langt fra tilstrækkelige på grund af manglende viden og ressourcer;

W. der henviser til, at kampen mod it-kriminalitet og illegale aktiviteter på internettet ikke bør overskygge de positive aspekter af et frit og åbent internet, der skaber nye muligheder for udveksling af viden og for at fremme politisk og social inklusion verden over;

Generelle bemærkninger

1. understreger, at den kraftige stigning i ransomware, botnet og uautoriseret beskadigelse

af edb-systemer har konsekvenser for enkeltpersoners sikkerhed, for adgangen til og integriteten af personoplysninger, for beskyttelsen af privatlivets fred og de grundlæggende frihedsrettigheder og for integriteten af kritisk infrastruktur, herunder men ikke begrænset til, energi- og elforsyning og finansielle strukturer som f.eks. børser; minder i den forbindelse om, at bekæmpelsen af it-kriminalitet prioriteres i den europæiske dagsorden om sikkerhed af 28. april 2015;

2. understreger behovet for at strømline definitionerne af it-kriminalitet, it-krigsførelse, it-sikkerhed, it-chikane og it-angreb for at sikre, at EU-institutionerne og medlemsstaterne anvender de samme juridiske definitioner;

3. understreger, at bekæmpelsen af it-kriminalitet først og fremmest bør handle om at sikre og styrke kritisk infrastruktur og andre netværksbaserede enheder, og ikke udelukkende om at indføre repressive foranstaltninger;

4. bekræfter, hvor vigtigt det er, at der træffes retlige foranstaltninger på EU-plan for at harmonisere definitionen på strafbare handlinger i form af angreb på informationssystemer samt seksuelle overgreb og seksuel udnyttelse af børn på internettet, og at medlemsstaterne får pligt til at indføre et system for indsamling, behandling og offentliggørelse af statistiske oplysninger om disse overtrædelser for at gøre bekæmpelsen af disse former for kriminalitet mere effektiv;

5. opfordrer indtrængende de medlemsstater, som endnu ikke har gennemført direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug og seksuelt udnyttelse af børn og børnepornografi, til at gøre det hurtigt og korrekt; opfordrer Kommissionen til nøje at overvåge og sikre en fuldstændig og effektiv gennemførelse af direktivet, til i rette tid at aflægge rapport til Parlamentet og dets ansvarlige udvalg om resultaterne af overvågningen og til samtidig at erstatte rammeafgørelsen 2004/68/RIA ; understreger, at Eurojust og Europol skal have de nødvendige ressourcer til at forbedre identificeringen af ofre, bekæmpe organiserede netværk med udøvere af seksuelt misbrug og fremskynde efterforskning, analyse og sagsanlæg i forbindelse med sager med online og offline materiale med misbrug af børn;

6. beklager, at 80 % af alle virksomheder i Europa har oplevet mindst én it-sikkerhedshændelse, og at it-angreb mod virksomheder ofte ikke opdages eller anmeldes; henviser til, at en række undersøgelser anslår, at de årlige omkostninger ved it-angreb har væsentlige konsekvenser for verdensøkonomien; mener, at kravet om offentliggørelse af brud på sikkerheden og om udveksling af oplysninger om risici, der blev indført ved Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (den generelle forordning om databeskyttelse)[1] og Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (direktivet om net- og informationssikkerhed (NIS))[2], vil bidrage til at løse dette problem ved at yde støtte til erhvervslivet og navnlig små og mellemstore virksomheder;

[1] EUT L 119 af 4.5.2016, s. 1.
[2] EUT L 194 af 19.7.2016, s. 1.

7. understreger, at den konstant skiftende karakter af it-truslerne stiller alle interesserede parter over for alvorlige juridiske og teknologiske problemer; mener, at ny teknologi ikke bør betragtes som en trussel, og fremfører, at teknologiske fremskridt inden for kryptering vil forbedre sikkerheden generelt i vore it-systemer, bl.a. ved at give slutbrugerne mulighed for bedre at beskytte deres oplysninger og kommunikation; påpeger imidlertid, at der fortsat er store huller i sikringen af kommunikation, og at teknikker som onion routing og skjulte netværk kan anvendes af ondsindede brugere, herunder terrorister og børnesexforbrydere, hackere, der sponsoreres af fjendtlige fremmede stater, eller ekstremistiske politiske eller religiøse organisationer til kriminelle formål, navnlig til at sløre deres kriminelle virksomhed eller identitet, hvilket skaber alvorlige problemer for efterforskningen.

8. er dybt bekymret over det seneste ransomwareangreb, som tilsyneladende påvirkede titusindvis af computere i op mod 100 lande og talrige organisationer, blandt andet Det Forenede Kongeriges nationale sundhedstjeneste (NHS), der var det mest fremtrædende offer for det omfattende malwareangreb; anerkender i denne forbindelse den vigtige indsats, som "No More Ransom"-kampagnen har gjort ved at stille over 40 gratis krypteringsværktøjer til rådighed, som giver ofrene for ransomware verden over mulighed for at kryptere deres berørte enheder;

9. understreger, at de skjulte netværk og onion routing i visse lande også skaber et frirum for journalister, politiske aktivister og menneskerettighedsforkæmpere, hvor de kan undgå at blive opdaget af undertrykkende statslige myndigheder;

10. bemærker, at kriminelle og terroristiske netværks anvendelse af værktøjer og tjenester til it-kriminalitet stadig er begrænset; understreger dog, at det kan tænkes at ændre sig i lyset af de voksende forbindelser mellem terrorisme og organiseret kriminalitet og den brede tilgængelighed af skydevåben og eksplosivstoffer på de skjulte netværk;

11. fordømmer på det kraftigste ethvert indgreb, der udfører eller styres af en fremmed nation eller dennes agenter med henblik på at forstyrre den demokratiske proces i et andet land;

12. understreger, at anmodninger på tværs af grænser om konfiskation af domæner, fjernelse af indhold og adgang til brugerdata skaber alvorlige problemer, som kræver øjeblikkelig indgriben, da der står meget på spil; understreger i denne sammenhæng, at internationale menneskerettighedsrammer, som både gælder online og offline, udgør et afgørende benchmark på verdensplan;

13. opfordrer medlemsstaterne til at sikre, at ofre for it-angreb kan udnytte alle de rettigheder, der er fastsat i direktiv 2012/29/EU, og til at optrappe deres indsats i forhold til identificering af ofre og tjenester med ofrene i centrum, bl.a. gennem fortsat støtte til Europols taskforce Victim ID; opfordrer medlemsstaterne til i samarbejde med Europol hurtigt at oprette relaterede platforme for at sikre, at alle internetbrugere ved, hvordan de kan bede om hjælp, hvis de bliver ofre for illegale aktiviteter online; opfordrer Kommissionen til at gennemføre en undersøgelse af konsekvenserne af grænseoverskridende it-kriminalitet i henhold til direktiv 2012/29/EU;

14. understreger, at Europols IOCTA-rapport fra 2014 nævner behovet for mere effektive lovgivningsmæssige redskaber under hensyntagen til de eksisterende begrænsninger i

forbindelse med0 aftaler om gensidig retshjælp (MLAT), og går ligeledes i givet fald ind for en yderligere harmonisering af lovgivningen i hele EU;

15. understreger, at it-kriminalitet i alvorlig grad underminerer det digitale indre markeds funktion ved at mindske tilliden til udbydere af digitale tjenester, underminere grænseoverskridende transaktioner og alvorligt skade forbrugerne af digitale tjenesters interesser;

16. understreger, at it-sikkerhedsstrategier og -foranstaltninger kun er fornuftige og effektive, hvis de bygger på de grundlæggende rettigheder og frihedsrettighederne i Den Europæiske Unions charter om grundlæggende rettigheder og EU's centrale værdigrundlag.

17. understreger, at der er et legitimt og stærkt behov for at beskytte kommunikation mellem enkeltpersoner og mellem enkeltpersoner og offentlige og private organisationer for at forhindre it-kriminalitet; fremhæver, at en stærk kryptering kan bidrage til at opfylde dette behov; understreger endvidere, at en begrænsning af anvendelsen eller svækkelse af styrken af de kryptografiske redskaber vil medføre svagheder, der kan misbruges til kriminelle formål og svække tilliden til elektroniske tjenester, som igen vil være til skade for både civilsamfundet og erhvervslivet;

18. efterlyser en handlingsplan for beskyttelse af børns rettigheder online og offline på internettet og minder om, at de retshåndhævende myndigheder ved bekæmpelsen af it-kriminalitet bør være særligt opmærksomme på forbrydelser mod børn; understreger i den forbindelse behovet for at styrke det retlige og politimæssige samarbejde mellem medlemsstaterne og med Europol og dets europæiske center til bekæmpelse af it-kriminalitet (EC3) med henblik på at forebygge og bekæmpe it-kriminalitet, og navnlig seksuel udnyttelse af børn over internettet;

19. opfordrer Kommissionen og medlemsstaterne til at træffe alle relevante retslige foranstaltninger til at bekæmpe problemet med vold mod kvinder online; opfordrer navnlig EU og medlemsstaterne til at gå sammen om at få skabt en strafferetlig ramme, der forpligter internet-selskaber til at slette eller stoppe spredning af nedværdigende, anstødelige og ydmygende indhold; anmoder endvidere om, at der indføres psykologisk støtte til kvinder, der er ofre for vold online og piger, der udsættes for it-mobning;

20. understreger, at onlineindhold, der er kendt ulovligt på grundlag af en retlig procedure, straks skal slettes; fremhæver den rolle, som informations- og kommunikationsteknologien, internetudbyderne og internethostingudbyderne spiller i forbindelse med at sikre hurtig og effektiv fjernelse af illegalt internetindhold på anmodning fra den ansvarlige retshåndhævende myndighed;

Forebyggelse

21. opfordrer Kommissionen til i forbindelse med revisionen af den europæiske strategi til at fortsætte arbejdet med at identificere svagheder i netværks- og informationssikkerheden i den europæiske kritiske infrastruktur, tilskynde til udvikling af modstandsdygtige systemer og vurdere situationen med hensyn til bekæmpelse af it-kriminalitet i Den Europæiske Union og medlemsstaterne for at opnå en bedre forståelse af tendenserne og udviklingen i forbindelse med strafbare handlinger på internettet;

22. understreger, at it-modstandsdygtighed er nøglen til forebyggelse af it-kriminalitet og derfor bør gives højeste prioritet; opfordrer medlemsstaterne til at indføre proaktive politikker og foranstaltninger til beskyttelse af netværk og kritisk infrastruktur og opfordrer til en omfattende EU-strategi til bekæmpelse af it-kriminalitet, der er forenelig med de grundlæggende rettigheder, databeskyttelse, it-sikkerhed, forbrugerbeskyttelse og e-handel;

23. glæder sig i denne forbindelse over investeringen af EU-midler i forskningsprojekter som det offentlig-private partnerskab (OPP) om it-sikkerhed for at fremme europæisk it-modstandsdygtighed gennem innovation og kapacitetsopbygning; anerkender særligt den indsats, som det offentlig-private partnerskab om it-sikkerhed (OPP) har gjort for at udvikle hensigtsmæssige processer til håndtering af zero-day-sårbarhed;

24. understreger i den forbindelse betydningen af gratis og open source-software; opfordrer til, at der afsættes flere EU-midler til specifik forskning i it-sikkerhed på grundlag af gratis open source-software;

25. konstaterer med bekymring, at der er mangel på kvalificerede it-specialister, der arbejder med it-sikkerhed; opfordrer medlemsstaterne til at investere i uddannelse;

26. mener, at lovgivning bør spille en større rolle ved håndtering af it-sikkerhedsrisici gennem forbedrede produkt- og softwarestandarder for design og efterfølgende opdateringer samt gennem minimumsstandarder for standard brugernavne og adgangskoder;

27. opfordrer medlemsstaterne til at intensivere informationsudvekslingen gennem Eurojust, Europol and ENISA og udvekslingen af bedste praksis gennem det europæiske netværk af enheder, der håndterer It-sikkerhedshændelser (CSIRT Computer Security Incident Response) og it-beredskabsenheder (CERTs Computer Emergency Response Teams) om de udfordringer, de står overfor i forbindelse med bekæmpelse af it-kriminalitet, samt om konkrete juridiske og tekniske løsninger til at imødegå dem og styrke it-modstandsdygtigheden; opfordrer i den forbindelse Kommissionen til at fremme et effektivt samarbejde og lette udvekslingen af oplysninger med henblik på at forudskikke og fjerne potentielle risici i henhold til NIS-direktivet;

28. er bekymret over, at Europol har konstateret, at de fleste vellykkede angreb på enkeltpersoner kan tilskrives manglende digital hygiejne og bevidsthed hos brugerne samt manglende hensyntagen til tekniske sikkerhedsforanstaltninger som f.eks. sikkerhed i designet; understreger, at brugerne er de første ofre for dårligt sikret hardware og software;

29. opfordrer Kommissionen til at iværksætte en oplysningskampagne med inddragelse af alle relevante aktører og interesserede parter med henblik på at styrke børns færdigheder og bevidsthed og hjælpe forældre, omsorgspersoner, og lærere med at forstå og håndtere risici på internettet og beskytte børnenes sikkerhed på nettet, til at bistå medlemsstaterne med at udforme forebyggelsesprogrammer mod seksuelt misbrug på internettet, til at fremme bevidstgørelseskampagne for ansvarlig adfærd på de sociale medier og til at tilskynde større søgemaskiner og sociale medienetværk til at anvende en proaktiv tilgang til at beskytte børns sikkerhed på nettet;

30. opfordrer Kommissionen og medlemsstaterne til at iværksætte oplysnings-, bevidstgørelses- og forebyggelseskampagner og til at fremme god praksis for at sikre, at ikke blot borgere og navnlig børn og andre sårbare brugere, men også de centrale og regionale myndigheder, centrale aktører og aktørerne i den private sektor og navnlig små og mellemstore virksomheder bliver klar over de risici, som er forbundet med it-kriminalitet, og over, hvordan de kan beskytte sig selv og deres udstyr på internettet; opfordrer endvidere Kommissionen og medlemsstaterne til at fremme anvendelsen af praktiske sikkerhedsforanstaltninger såsom kryptering eller andre teknologier til forbedring af sikkerheden og privatlivets fred samt anonymiseringsredskaber;

31. understreger, at bevidstgørelseskampagner skal ledsages af uddannelsesprogrammer om "informeret brug" af informationsteknologisk udstyr; opfordrer medlemsstaterne til at indføre it-sikkerhed samt risiciene ved og konsekvenserne af anvendelse af persondata på internettet i skolernes it-undervisningsplaner; understreger i den forbindelse den indsats, der gøres inden for rammerne af den europæiske strategi for et bedre internet for børn (Better Internet for Kids (BIK)-strategien fra 2012);

32. understreger det akutte behov for i forbindelse med bekæmpelsen af it-kriminalitet at gøre en yderligere indsats med hensyn til undervisning i net- og informationssikkerhed (NIS) ved at indføre undervisning i NIS, i sikker softwareudvikling og i personlig databeskyttelse for it-studerende samt grundlæggende undervisning i NIS for medarbejdere i den offentlige forvaltning;

33. mener, at forsikring mod it-hacking kunne være et middel til at anspore til en større indsats på sikkerhedsområdet både i virksomheder, der gøres ansvarlige for softwaredesign, og for brugere, der tilskyndes til at anvende software korrekt;

34. understreger, at virksomheder bør identificere svagheder og risici gennem regelmæssige evalueringer, beskytte deres produkter og tjenester ved øjeblikkeligt at afhjælpe svagheder, bl.a. gennem patch-forvaltningsprocedurer og ajourføring af personoplysninger, afbøde konsekvenserne af ransomwareangreb såsom WannaCry gennem etablering af robuste backupordninger og konsekvent anmelde it-angreb;

35. opfordrer medlemsstaterne til at oprette it-beredskabsenheder (CERTs), hvor virksomheder og forbrugere kan indberette ondsindede e-mails og websider i overensstemmelse med NIS-direktivet, så medlemsstaterne regelmæssigt holdes underrettet om sikkerhedshændelser og foranstaltninger til bekæmpelse og mindskelse af risikoen for deres egne systemer; tilskynder medlemsstaterne til at overveje at etablere en database med oplysninger om alle former for it-kriminalitet og overvåge udviklingen af de pågældende fænomener;

36. opfordrer indtrængende medlemsstaterne til at investere i at gøre deres kritiske infrastruktur og tilhørende data mere sikre for at modstå it-angreb;

Øget ansvar hos tjenesteydere

37. anser et styrket samarbejde mellem de kompetente myndigheder og tjenesteudbydere for at være en nøglefaktor med hensyn til at fremskynde og strømline den gensidige juridiske bistand og de gensidige anerkendelsesprocedurer, der er hjemmel for i den europæiske rammelovgivning; opfordrer udbydere af elektroniske

kommunikationstjenester, der ikke er etableret i Unionen, til skriftligt at udpege repræsentanter i Unionen;

38. gentager, at producenterne er det vigtigste udgangspunkt for en stramning af ansvarsbestemmelserne med hensyn til tingenes internet, hvilket vil føre til produkter af højere kvalitet og et mere sikkert miljø både hvad angår ekstern adgang og en dokumenteret ajourføringsordning;

39. mener, at der på baggrund af udviklingen af nye innovative produkter og den voksende tilgængelighed af produkter til tingenes internet skal tages særligt hensyn til sikkerheden i alle disse produkter, selv i de mest simple; mener, at hardwareproducenter og udviklere af innovativ software har en interesse i at investere i løsninger, som forebygger it-kriminalitet, og i at udveksle oplysninger om trusler mod it-sikkerheden; opfordrer Kommissionen og medlemsstaterne til at fremme tilgangen med indbygget sikkerhed og opfordrer industrien til at inkludere indbyggede sikkerhedsløsninger i alle produkter; tilskynder i den forbindelse den private sektor til at indføre frivillige ordninger, der er udviklet på grundlag af den relevante EU-lovgivning som f.eks. NIS-direktivet og tilpasset internationalt anerkendte standarder, for at styrke tilliden til sikkerheden ved software og udstyr som f.eks. tillidsmærket for tingenes internet;

40. opfordrer tjenesteudbydere til at efterleve adfærdskodeksen mod ulovlige hadefulde udtalelser online og opfordrer Kommissionen og de deltagende virksomheder til at fortsætte samarbejdet om dette spørgsmål;

41. minder om, at Europa-Parlamentets og Rådets direktiv 2000/31/EF om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»direktivet om elektronisk handel«)[1] kun undtager formidlere for indholdsansvar, hvis de spiller en neutral og passiv rolle i forhold til det sendte og/eller hostede indhold, men kræver også en hurtig fjernelse eller deaktivering af adgang til indhold, når en formidler får faktisk kendskab til overtrædelse eller ulovlig aktivitet eller information;

42. understreger, at det er absolut nødvendigt at beskytte de retshåndhævende myndigheders databaser mod brud på sikkerheden og ulovlig adgang, da dette er et problem for den enkelte borger; er bekymret over de retshåndhævende myndigheders ekstraterritoriale muligheder for at tilgå data i forbindelse med strafferetlig efterforskning og understreger behovet for at indføre stramme regler på dette område.

43. mener, at problemer i forbindelse med ulovligt online-virksomhed skal løses på en hurtig og effektiv måde, bl.a. gennem nedlukning hvis der ikke længere er behov for indholdet til sporing, efterforskning og retsforfølgelse; minder om, at medlemsstaterne, hvis det ikke er muligt at fjerne indhold, kan træffe de fornødne forholdsmæssige foranstaltninger for at blokere for adgangen til indholdet på deres territorium; understreger, at sådanne indgreb skal være i overensstemmelse med eksisterende lovgivning og retslige procedurer samt med chartret, og også skal være underlagt passende kontrolforanstaltninger, herunder muligheden for domstolsprøvelse;

[1] EFT L 178 af 17.7.2000, s. 1.

44. fremhæver betydningen af den rolle, som tjenesteudbydere i det digitale informationssamfund spiller med hensyn til at sikre hurtig og effektiv fjernelse af ulovligt onlineindhold efter anmodning af den kompetente retshåndhævende myndighed, og glæder sig over de fremskridt, der er gjort i denne forbindelse, bl.a. gennem bidraget fra EU's internetforum; understreger, at der er behov for et stærkere engagement og et tættere samarbejde mellem de kompetente myndigheder og tjenesteudbydere i informationssamfundet for at sikre hurtig og effektiv nedtagning og dermed undgå blokering af ulovligt indhold gennem offentlige indgreb; opfordrer medlemsstaterne til at gøre strafferetligt ansvar gældende over for ikke-samarbejdsvillige platforme; gentager, at foranstaltninger med henblik på at fjerne illegalt onlineindhold, som fastsætter betingelser og vilkår, kun bør være tilladt, hvis de nationale procedureregler gør det muligt for brugerne at gøre deres rettigheder gældende ved en domstol efter at have fået meddelelse om sådanne foranstaltninger;

45. understreger, at begrænset formidleransvar, som det fremgår af Parlamentets beslutning af 19. januar 2016 "På vej mod en akt for det digitale indre marked"[1], er af afgørende betydning for beskyttelsen af internettets åbenhed, de grundlæggende rettigheder, retssikkerheden og innovation; glæder sig over, at Kommissionens har til hensigt at yde vejledning om procedurerne i forbindelse med advarsel og nedlukning og at bistå onlineplatforme med at opfylde deres ansvar og efterleve ansvarsbestemmelserne i direktivet om elektronisk handel (2000/31/EC) for at forbedre retssikkerheden og øge brugernes tillid; opfordrer Kommissionen til at fremsætte lovgivningsforslag på disse områder;

46. opfordrer til anvendelse af en "følg pengene"-tilgang, som beskrevet i Parlamentets beslutning af 9. juni 2015 "Mod en fornyet konsensus for så vidt angår håndhævelsen af intellektuelle ejendomsrettigheder: En EU-handlingsplan"[2] på grundlag af rammelovgivningen i direktivet om elektronisk handel og direktivet om håndhævelsen af intellektuelle ejendomsrettigheder;

47. understreger den afgørende betydning af at yde løbende og specifik træning og psykologisk støtte til indholdsmoderatorer i private og offentlige enheder, der har ansvaret for at vurderer upassende eller ulovligt onlineindhold, da de bør betragtes som de første til at reagere på dette område

48. opfordrer tjenesteyderne til at fastlægge klare anmeldelsesårsager og en nøje defineret backofficeinfrastruktur, som gør det muligt at reagere hurtigt og hensigtsmæssigt på anmeldelser;

49. opfordrer tjenesteyderne til at styrke deres indsats for at orientere og øge bevidstheden om farerne på internettet, især for børn, gennem udvikling af interaktive værktøjer og informationsmateriale;

Styrkelse af politisamarbejdet og det retlige samarbejde

50. er bekymret over, at en lang række it-forbrydelser forbliver ustraffede; beklager, at internetudbydernes anvendelse af teknologier som NAT CGN skader efterforskningen i

[1] Vedtagne tekster, P8_TA(2016)0009.
[2] Vedtagne tekster, P8_TA(2015)0220.

alvorlig grad ved at gøre det teknisk umuligt at identificere brugeren af en IP-adresse præcist og dermed de(n) ansvarlige for it-forbrydelser; understreger behovet for at tillade de retshåndhævende myndigheder lovlig adgang til relevante oplysninger under de begrænsede omstændigheder, hvor en sådan adgang er nødvendig og forholdsmæssig set i forhold til sikkerhed og retfærdighed; understreger, at retlige og retshåndhævende myndigheder skal have tilstrækkelig kapacitet til at foretage legitim efterforskning;

51. opfordrer medlemsstaterne til ikke at pålægge krypteringsleverandører nogen forpligtelse, der kunne svække eller true sikkerheden i deres netværk og tjenester som f.eks. installering eller muliggørelse af bagdøre; understreger at der skal findes mulige løsninger både gennem lovgivningen og gennem den fortsatte teknologiske udvikling, når det er nødvendigt af hensyn til retfærdighed og sikkerhed; opfordrer medlemsstaterne til i samråd med retsvæsenet og Eurojust at samarbejde om indbyrdes tilpasning af betingelserne for lovlig anvendelse af online efterforskningsredskaber;

52. understreger, at lovlig aflytning kan være en særdeles effektiv foranstaltning til bekæmpelse af ulovlig hacking på betingelse af, at den er nødvendig, forholdsmæssig, under retsvæsenets kontrol og fuldt ud overholder de grundlæggende rettigheder og EU's databeskyttelsesbestemmelser og retspraksis; opfordrer alle medlemsstaterne til at udnytte mulighederne ved lovlig aflytning af mistænkte enkeltpersoner, til at fastlægge klare regler for proceduren for indhentning af tilladelse til lovlige aflytningsaktiviteter, herunder begrænsninger i anvendelsen og varigheden af lovlige aflytningsredskaber, til at oprette en kontrolmekanisme og til at fastsætte effektive retsmidler for de personer, der er genstand for disse aflytningsaktiviteter;

53. opfordrer medlemsstaterne til at engagere sig i ikt-sikkerhedssamfundet og tilskynde det til at spille en mere aktiv rolle i "hvid hat-hacking" og anmeldelse af ulovligt indhold som f.eks. materiale om seksuelt misbrug af børn

54. opfordrer Europol til at etablere et anonymt anmeldelsessystem inde fra de skjulte net, som gør det muligt for personer at anmelde ulovligt indhold som f.eks. materiale med billeder af seksuel misbrug af børn til myndighederne ved at bruge de samme tekniske sikkerhedsforanstaltninger, som anvendes af mange nyhedsorganisationer, der bruger sådanne systemer til at lette udveksling af følsomme oplysninger med journalister på en måde, der tillader en større grad af anonymitet og sikkerhed, end det er tilfældet med konventionel e-mail;

55. understreger behovet for at minimere de risici for internetbrugernes privatliv, der opstår ved læk af exploits eller værktøjer, der anvendes af de retshåndhævende myndigheder som led i deres lovlige efterforskning;

56. understreger, at retlige og retshåndhævende myndigheder skal have tilstrækkelig kapacitet og tilstrækkelige midler til effektivt at kunne bekæmpe it-kriminalitet;

57. understreger, at de forskellige særskilte, territorialt afgrænsede nationale retssystemer skaber vanskeligheder ved fastlæggelsen af gældende ret i forbindelse med grænseoverskridende virksomhed og giver anledning til retlig usikkerhed og hindrer dermed samarbejdet på tværs af grænserne, hvilket er nødvendigt for at løse problemerne med it-kriminalitet;

58. understreger nødvendigheden af at udvikle det praktiske grundlag for en fælles europæisk tilgang til jurisdiktion på internettet, som det kom til udtryk under justits- og indenrigsministrenes uformelle møde den 26. januar 2016;

59. understreger i den forbindelse nødvendigheden af at udvikle fælles procedurenormer for fastlæggelse af de territoriale faktorer, der giver grundlag for gældende ret på internettet, og at definere efterforskningstiltag, der kan anvendes uanset geografiske grænser;

60. anerkender, at en sådan fælles europæisk tilgang, der skal respektere de grundlæggende rettigheder og privatlivets fred, vil skabe tillid blandt de interesserede parter, mindske forsinkelserne i behandlingen af grænseoverskridende anmodninger, etablere interoperabilitet blandt heterogene aktører og give mulighed for at indarbejde behørige proceskrav i de operationelle rammer;

61. mener også, at der bør udvikles fælles procedurenormer for jurisdiktion for retshåndhævelse på internettet på verdensplan: glæder sig i den forbindelse over det arbejde, der udføres af Europarådets Cloud Evidence Group;

Elektronisk bevismateriale

62. understreger, at en fælles europæisk tilgang til strafferetlige bestemmelser på internettet bør prioriteres, da det vil forbedre håndhævelsen af retsstatsprincippet på internettet, lette indhentning af elektronisk bevismateriale i straffesager og bidrage til en meget hurtigere opklaring af sager;

63. understreger nødvendigheden af at finde metoder til at sikre og indhente elektronisk bevismateriale hurtigere og betydningen af et tæt samarbejde mellem de retshåndhævende myndigheder, bl.a. gennem øget brug af fælles efterforskningshold og inddragelse af tredjelande og tjenesteudbydere, der er aktive på det europæiske område, i henhold til den generelle forordning om databeskyttelse (2016/679/EU), direktiv (EU) 2016/680 af 27. april 2016 (politidirektivet)[1] og eksisterende aftaler om gensidig retshjælp (MLA); understreger behovet for at oprette kvikskranker i medlemsstaterne og forbedre anvendelsen af de eksisterende kontaktpunkter mest muligt, da det vil lette adgangen til elektronisk bevismateriale og udveksling af oplysninger, forbedre samarbejdet med tjenesteudbyderne og fremskynde procedurerne i forbindelse med gensidig retshjælp;

64. erkender, at de forskellige lovgivningsrammer kan skabe problemer for tjenesteudbyderne, når de forsøger at imødekomme anmodninger fra de retshåndhævende myndigheder; opfordrer Kommissionen til at foreslå en europæisk juridisk ramme for elektronisk bevismateriale, herunder harmoniserede regler for fastlæggelsen af, hvorvidt en tjenesteyder er indenlandsk eller udenlandsk, og til at pålægge tjenesteudbydere at imødekomme anmodninger fra andre medlemsstater, der er behørigt juridisk begrundet og i overensstemmelse med den europæiske efterforskningskendelse, men samtidig tage hensyn til proportionalitetsprincippet for at undgå krænkelser af etableringsfriheden og den frie udveksling af tjenesteydelse, og sikre tilstrækkelige garantier for dermed at skabe retssikkerhed og forbedre

[1] EUT L 119 af 4.5.2016, s. 89.

tjenesteydernes og formidlernes muligheder for at reagere på anmodninger fra de retshåndhævende myndigheder;

65. understreger behovet for, at lovgivningsrammerne for elektronisk bevismateriale indeholder tilstrækkelige garantier for alle berørte parters rettigheder og friheder; fremhæver, at dette skal omfatte et krav om, at anmodninger om elektronisk bevismateriale i første række fremsættes over for ejeren af eller den, der styrer dataene, så der sikres respekt for deres rettigheder og rettighederne for dem, som dataene vedrører (for eksempel deres ret til at påberåbe sig tavshedspligt og søge retshjælp i tilfælde af uforholdsmæssig eller på anden måde ulovlig adgang); understreger ligeledes behovet for at sikre, at enhver lovgivningsmæssig ramme beskytter udbydere og alle andre parter mod krav, der kan skabe konflikter mellem jurisdiktioner eller på anden måde krænke andre staters suverænitet;

66. opfordrer medlemsstaterne til fuldt ud at gennemføre Europa-Parlamentets og Rådets direktiv 2014/41/EU af 3. april 2014 om den europæiske efterforskningskendelse[1] med henblik på en effektiv sikring og indhentning af elektronisk bevismateriale i EU, til at indføje specifikke bestemmelser om internettet i deres nationale strafferet med henblik på at lette anerkendelsen af elektronisk bevismateriale i retssager og til at udstede klarere retningslinjer til dommere for så vidt angår strafudmåling for it-kriminalitet;

67. glæder sig over Kommissionens igangværende arbejde med en samarbejdsplatform med sikre kommunikationskanaler til digital udveksling af europæiske efterforskningskendelser (EIO) og svar mellem EU's retsmyndigheder; opfordrer Kommissionen til i samarbejde med medlemsstaterne, Eurojust og tjenesteudbydere at undersøge og harmonisere formularer, redskaber og procedure for anmodning om sikring og indhentning af elektronisk bevismateriale for at lette legaliseringen af det, sikre en hurtig afvikling og øge gennemskueligheden og ansvarligheden under processen med at sikre og indhente elektronisk bevismateriale; opfordrer Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse (Cepol) til at udvikle undervisningsmoduler om en effektiv anvendelse af de nuværende rammer, der bruges til at sikre og indhente elektronisk bevismateriale; understreger i den forbindelse, at strømlining af tjenesteudbydernes politik vil bidrage til at mindske de forskellige tilgange, navnlig med hensyn til procedurer og betingelser for at give adgang til de ønskede oplysninger;

Kapacitetsopbygning på europæisk plan

68. påpeger, at nylige hændelser med al tydelighed viser den akutte sårbarhed i EU og navnlig i EU-institutionerne, i de nationale regeringer og parlamenter, i store europæiske virksomheder, i de europæisk it-infrastrukturer og -net over for avancerede angreb under anvendelse af kompliceret software og malware; opfordrer Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) til løbende at vurdere trusselsniveauet og Kommissionen om at investere i it-kapacitet og i forsvar af og modstandsdygtighed i EU-institutionernes kritiske it-infrastrukturer med henblik på at mindske EU's sårbarhed over for alvorlige it-angreb fra store kriminelle organisationer, statsstøttede hackere eller terrorgrupper;

[1] EUT L 130 af 1.5.2014, s. 1.

69. anerkender det vigtige bidrag, som Det Europæiske Center til Bekæmpelse af It-kriminalitet (EC3) under Europol og Eurojust samt Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) har ydet til bekæmpelsen af it-kriminalitet;

70. opfordrer Europol til at støtte de nationale retshåndhævende myndigheder i forbindelse med etableringen af sikre og hensigtsmæssige transmissionskanaler;

71. beklager, at der for øjeblikket ikke findes EU-standarder for uddannelse og certificering; erkender, at fremtidige udvikling inden for it-kriminalitet nødvendiggør mere ekspertise hos i virksomhederne; glæder sig over, at igangværende initiativer som Den Europæiske Uddannelsesgruppe vedrørende It-kriminalitet (ECTEG), projektet uddannelse af trænerne (TOT) og uddannelsesaktiviteterne inden for rammerne for EU's politikcyklus allerede er begyndt at rette op på manglen på ekspertviden på EU-plan;

72. opfordrer Cepol og Det Europæiske Netværk for Uddannelse af Dommere og Anklagere til at udvide deres tilbud om kurser om it-kriminalitet til kompetente retshåndhævende myndigheder og retslige myndigheder i Unionen;

73. understreger, at antallet af kriminelle it-handlinger, som henvises til Eurojust, er steget med 30 %; opfordrer til, at der afsættes tilstrækkelige bevillinger om nødvendigt med oprettelse af flere stillinger for at sætte Eurojust i stand til at klare den stigende arbejdsbyrde, der er forbundet med it-kriminalitet, samt til at udvikle og yderligere styrke sin støtte til nationale anklagere i grænseoverskridende it-kriminalitetssager, bl.a. gennem det nyligt oprettede Europæiske Retlige Netværk for It-kriminalitet;

74. opfordrer til en revision af ENISA-mandatet og en styrkelse af de nationale agenturer for it-sikkerhed; opfordrer til en styrkelse af ENISA's opgaver, personale og bevillinger; understreger, at det nye mandat også bør omfatte en styrkelse af forbindelserne mellem Europol og de interesserede parter fra erhvervet for at sætte agenturet i stand til bedre at støtte de kompetente myndigheder i kampen mod it-kriminalitet;

75. anmoder agenturet for grundlæggende rettigheder (FRA) om at udarbejde en praktisk og detaljeret håndbog med retningslinjer for medlemsstaternes tilsyns- og kontrolmuligheder;

Styrket samarbejde med tredjelande

76. understreger betydningen af et nært samarbejde med tredjelande i den verdensomspændende kamp mod it-kriminalitet, bl.a. gennem udveksling af bedste praksis, fælles efterforskning, kapacitetsopbygning og gensidig retshjælp;

77. opfordrer de medlemsstater, som endnu ikke har ratificeret og fuldt ud gennemført Europarådets konvention af 23. november 2001 om it-kriminalitet ("Budapest-konventionen") sammen med tillægsprotokollerne, til at gøre det og til i samarbejde med Europa-Kommissionen at tilskynde til anvendelsen af den i de relevante internationale fora;

78. understreger sin alvorlige bekymring over arbejdet i Europarådets komité om konventionen om it-kriminalitet omkring fortolkningen af artikel 32 i Budapest-

konventionen om grænseoverskridende adgang til lagrede computerdata ("cloud evidence") og modsætter sig enhver indgåelse af en tillægsprotokol eller retningslinjer, der har til formål at udvide anvendelsesområdet for denne bestemmelse ud over den nuværende ordning, der er indeholdt i konventionen, hvilket allerede indebærer en væsentlig fravigelse af territorialitetsprincippet, fordi den muligvis kan medføre ubegrænset fjernadgang fra de retshåndhævende myndigheders side til servere og computere, der findes i andre jurisdiktioner, uden anvendelse af ordningen om gensidig retshjælp (MLA) og andre juridiske samarbejdsinstrumenter, der er etableret for at sikre individets grundlæggende rettigheder, som f.eks. databeskyttelse og behørig proces, herunder navnlig Europarådets konvention nr. 108;

79. beklager, at der ikke findes nogen bindende internationale retsbestemmelser om it-kriminalitet, og opfordrer medlemsstaterne og EU-institutionerne til at arbejde for vedtagelsen af en sådan konvention;

80. opfordrer Kommissionen til at foreslå mulige initiativer til forbedring af effektiviteten og fremme anvendelsen af traktater om gensidig retshjælp (MLATS) for at modvirke, at tredjelande påberåber sig ekstraterritorial jurisdiktion;

81. opfordrer medlemsstaterne til at sikre tilstrækkelig kapacitet til at håndtere anmodninger om gensidig retshjælp vedrørende undersøgelser på internettet og at udvikle relevante uddannelsesprogrammer for det personale, der er ansvarligt for behandlingen af sådanne anmodninger;

82. understreger, at de strategiske og operative samarbejdsaftaler mellem Europol og tredjelande både letter udvekslingen af oplysninger og det praktiske samarbejde;

83. noterer sig, at det største antal anmodninger fra retshåndhævende myndigheder er sendt til USA og Canada; er bekymret over, at frigivelsen af oplysninger fra store amerikanske tjenesteudbydere efter anmodning fra de europæiske strafferetlige myndigheder ligger under 60 %, og minder om, at traktater om gensidig retshjælp og andre internationale aftaler i overensstemmelse med kapitel V i den generelle forordning om databeskyttelse er det foretrukne middel til at få adgang til personoplysninger, der opbevares i udlandet;

84. opfordrer Kommissionen til at foreslå konkrete foranstaltninger til beskyttelse af mistænkte eller anklagede personers grundlæggende rettigheder, når der finder udveksling af oplysninger sted mellem europæiske retshåndhævende myndigheder og tredjelande, navnlig garantier i forbindelse med hurtig indhentning efter en retsafgørelse af relevant bevismateriale, oplysninger om abonnenter samt detaljerede meta- og indholdsdata (hvis de ikke er krypteret) fra retshåndhævende myndigheder og/eller tjenesteydere med henblik på at forbedre den gensidige retshjælp;

85. opfordrer Kommissionen til i samarbejde med medlemsstaterne, de associerede europæiske organer og om nødvendigt tredjelande at overveje nye måder til effektivt at sikre og indhente elektronisk bevismateriale, der er hostet i tredjelande, i fuld overensstemmelse med grundlæggende rettigheder og EU's databeskyttelseslovgivning ved at fremskynde og effektivisere brugen af gensidig retshjælp og i givet fald gensidig anerkendelse;

86. fremhæver betydningen af NATO's Cyber Incidents Response Center;

87. opfordrer alle medlemsstater til at deltage i det globale forum for it-ekspertise (GFCE) for at lette etableringen af partnerskaber med henblik på kapacitetsopbygning;

88. støtter bistanden fra EU til kapacitetsopbygning til de østlige nabolande, da mange it-angreb udgår fra disse lande;

°

° °

89. pålægger sin formand at sende denne beslutning til Rådet og Kommissionen.

13.6.2017

UDTALELSE FRA UDVALGET OM DET INDRE MARKED OG FORBRUGERBESKYTTELSE

til Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender

om bekæmpelse af IT-kriminalitet
(2017/2068(INI))

Ordfører: Anneleen Van Bossuyt

ÆNDRINGSFORSLAG

Udvalget om det Indre Marked og Forbrugerbeskyttelse opfordrer Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender, som er korresponderende udvalg, til at tage hensyn til følgende ændringsforslag:

Ændringsforslag 1
Forslag til beslutning
Betragtning A a (ny)

Forslag til beslutning	*Ændringsforslag*
	Aa. der henviser til, at opbygning af tillid og tiltro i onlineverdenen er afgørende for skabelsen af et digitalt indre marked og for dets succes;

Ændringsforslag 2
Forslag til beslutning
Betragtning A b (ny)

Forslag til beslutning	*Ændringsforslag*
	Ab. der henviser til, at en effektiv retlig ramme for databeskyttelse vil gøre det muligt for forbrugerne og virksomhederne at drage fuld fordel af det

digitale indre marked og samtidig adressere IT-kriminalitet;

Ændringsforslag 3
Forslag til beslutning
Betragtning I

Forslag til beslutning	*Ændringsforslag*
I. der henviser til, at den konstant voksende indbyrdes forbundethed mellem mennesker, steder og ting ***gør*** tingenes internet ***til*** det ideelle mål for it-kriminelle;	I. der henviser til, at den konstant voksende indbyrdes forbundethed mellem mennesker, steder og ting ***giver en øget risiko for IT-kriminalitet, da*** tingenes internet ***ofte ikke er så godt beskyttet som traditionelt udstyr, der er tilsluttet internettet, og som sådant er*** det ideelle mål for IT-kriminelle;

Ændringsforslag 4
Forslag til beslutning
Punkt 7 a (nyt)

Forslag til beslutning	*Ændringsforslag*
	7a. understreger, at IT-kriminalitet i alvorlig grad underminerer det digitale indre markeds funktion ved at mindske tilliden til udbydere af digitale tjenester, underminere grænseoverskridende transaktioner og skade interesserne hos forbrugerne af digitale tjenester alvorligt;

Ændringsforslag 5
Forslag til beslutning
Punkt 11

Forslag til beslutning	*Ændringsforslag*
11. opfordrer indtrængende medlemsstaterne til at intensivere informationsudveksling om de udfordringer, de står overfor i forbindelse med bekæmpelse af cyberkriminalitet, samt forslag til løsning heraf;	11. opfordrer indtrængende medlemsstaterne til at intensivere informationsudveksling om de udfordringer, de står overfor i forbindelse med bekæmpelse af cyberkriminalitet, samt forslag til løsning heraf; ***opfordrer i denne forbindelse Kommissionen til at fremme et***

effektivt samarbejde og lette udvekslingen af oplysninger mellem de kompetente myndigheder med henblik på at forudse og forvalte potentielle risici, jf. direktivet om net- og informationssikkerhed;

Ændringsforslag 6
Forslag til beslutning
Punkt 13

Forslag til beslutning	*Ændringsforslag*
13. opfordrer Kommissionen og medlemsstaterne til at iværksætte oplysnings- og bevidstgørelseskampagner for at sikre, at borgerne, navnlig børn og andre sårbare brugere, og den private sektor er klar over de risici, der er forbundet med cyberkriminalitet, og for at fremme anvendelsen af sikkerhedsforanstaltninger såsom kryptering;	13. opfordrer Kommissionen og medlemsstaterne til at iværksætte oplysnings- og bevidstgørelseskampagner for at sikre, at borgerne, navnlig børn***,*** ***mindreårige*** og andre sårbare brugere, og den private sektor er klar over de risici, der er forbundet med cyberkriminalitet, og for at fremme anvendelsen af sikkerhedsforanstaltninger såsom kryptering;

Ændringsforslag 7
Forslag til beslutning
Punkt 16

Forslag til beslutning	*Ændringsforslag*
16. anser styrket samarbejde ***med*** tjenesteudbydere for at være en nøglefaktor med hensyn til at fremskynde og strømline gensidig retshjælp og gensidige anerkendelsesprocedurer;	16. anser styrket samarbejde ***mellem de kompetente myndigheder og*** tjenesteudbydere for at være en nøglefaktor med hensyn til at fremskynde og strømline gensidig retshjælp og gensidige anerkendelsesprocedurer;

Ændringsforslag 8
Forslag til beslutning
Punkt 16 a (nyt)

Forslag til beslutning	*Ændringsforslag*
	16a. mener, at EU og de nationale myndigheder bør have beføjelse til at vedtage foreløbige foranstaltninger til

	forebyggelse af alvorlig og uoprettelig skade for forbrugerne, navnlig midlertidig lukning af et websted, et domæne eller en tilsvarende digital lokalitet, tjeneste eller konto, forudsat at EU-borgeres grundlæggende rettigheder, databeskyttelsesreglerne og national lovgivning overholdes;

Ændringsforslag 9
Forslag til beslutning
Punkt 17

Forslag til beslutning	*Ændringsforslag*
17. mener, at ***innovation ikke bør hæmmes af unødigt bureaukrati for softwareudviklere*** og hardwarefabrikanter; opfordrer den private sektor til at indføre frivillige foranstaltninger, der tager sigte på at styrke tilliden til sikkerheden ved software og udstyr, såsom tillidsmærket for tingenes internet;	17. mener, at ***udviklere af innovativ software*** og hardwarefabrikanter ***har en interesse i at investere i løsninger til forebyggelse af IT-kriminalitet***; opfordrer ***i denne forbindelse*** den private sektor til at indføre frivillige foranstaltninger, ***som f.eks. standarder,*** der tager sigte på at styrke tilliden til sikkerheden ved software og udstyr, såsom tillidsmærket for tingenes internet***, udviklet på grundlag af den relevante EU-lovgivning som f.eks. direktivet om net- og informationssikkerhed***;

Ændringsforslag 10
Forslag til beslutning
Punkt 18

Forslag til beslutning	*Ændringsforslag*
18. ***opfordrer Kommissionen til at foreslå lovgivningsmæssige foranstaltninger, som indeholder klare definitioner og minimumsstraffe for formidling af falske nyheder og tilskyndelse til had på internettet, de dermed forbundne forpligtelser, der påhviler udbydere af internettjenester, og sanktioner i tilfælde af manglende overholdelse;***	***udgår***

Ændringsforslag 11
Forslag til beslutning
Punkt 19

Forslag til beslutning	*Ændringsforslag*
19. opfordrer Kommissionen til at undersøge ***de juridiske muligheder*** for at forbedre tjenesteyderes ansvarlighed og for at indføre en forpligtelse til at besvare udenlandske anmodninger om håndhævelse af EU-lovgivningen;	19. opfordrer Kommissionen til at undersøge ***mulighederne*** for at forbedre tjenesteyderes ***og formidleres*** ansvarlighed og ***de juridiske muligheder*** for at indføre en forpligtelse til at besvare udenlandske anmodninger om håndhævelse af EU-lovgivningen***, under hensyntagen til proportionalitetsprincippet, for at forhindre, at der indføres foranstaltninger, der kan gøre det vanskeligere eller mindre attraktivt at udøve etableringsfriheden og den frie udveksling af tjenesteydelser***;

Ændringsforslag 12
Forslag til beslutning
Punkt 19 a (nyt)

Forslag til beslutning	*Ændringsforslag*
	19a. mener, at der er brug for vejledning fra Kommissionens side om gennemførelsen af rammen for formidleransvar, således at onlineplatforme kan opfylde deres ansvar og reglerne om ansvar, forbedre retssikkerheden og øge brugernes tillid; opfordrer Kommissionen til at udvikle yderligere skridt med henblik herpå og erindrer om, at direktivet om elektronisk handel kun fritager formidlere for ansvar for indhold, hvis de spiller en neutral og passiv rolle i forhold til det indhold, der formidles og/eller lagres, men samtidig kræver, at de handler hurtigt for fjerne eller hindre adgang til indhold, så snart de får konkret kendskab til en overtrædelse eller til ulovlige aktiviteter eller data;

Ændringsforslag 13
Forslag til beslutning
Punkt 20

Forslag til beslutning	*Ændringsforslag*
20. ***opfordrer medlemsstaterne til at indføre de samme krypteringsforpligtelser for udbydere af onlinetjenester som dem, der gælder for udbydere af traditionelle telekommunikationstjenester;***	***udgår***

Ændringsforslag 14
Forslag til beslutning
Punkt 21

Forslag til beslutning	*Ændringsforslag*
21. ***understreger***, at ulovligt onlineindhold ***straks skal slettes***; glæder sig i denne forbindelse over de fremskridt, der er gjort med hensyn til blokering og fjernelse af ulovligt indhold på internettet, men understreger behovet for et stærkere engagement fra ***platformudbydere*** at reagere hurtigt og effektivt;	21. ***mener***, at ***spørgsmål vedrørende*** ulovligt onlineindhold ***skal tackles på en effektiv måde, herunder ved at begrænse adgangen til onlineindhold eller gennem procedurer for fjernelse***; glæder sig i denne forbindelse over de fremskridt, der er gjort med hensyn til blokering og fjernelse af ulovligt indhold på internettet, men understreger behovet for et stærkere engagement fra ***de kompetente myndigheder og udbydere af digitale tjenester i*** at reagere hurtigt og effektivt;

Ændringsforslag 15
Forslag til beslutning
Punkt 21 a (nyt)

Forslag til beslutning	*Ændringsforslag*
	21a. opfordrer til, at der anvendes en "følg pengene"-tilgang, som beskrevet i dets beslutning af 9. juni 2015 om "Mod en fornyet konsensus for så vidt angår håndhævelsen af intellektuelle ejendomsrettigheder: En EU-handlingsplan"[1], baseret på lovrammen for direktivet om elektronisk handel og direktivet om håndhævelsen af

intellektuelle ejendomsrettigheder;

1 EUT C 407 af 4.11.2016, s. 25.

Ændringsforslag 16
Forslag til beslutning
Punkt 21 b (nyt)

Forslag til beslutning	*Ændringsforslag*
	21b. understreger, at begrænset formidleransvar – som anført i dets beslutning af 19. januar 2016 om "På vej mod en akt for det digitale indre marked"[1] – er af afgørende betydning for beskyttelsen af internettets åbenhed, grundlæggende rettigheder, retssikkerhed og innovation; glæder sig over, at Kommissionen agter at vejlede onlineplatforme for at hjælpe dem med at overholde direktivet om elektronisk handel; opfordrer Kommissionen til at tage yderligere skridt med henblik herpå under henvisning til, at platforme, der ikke spiller en neutral rolle som defineret i direktivet om elektronisk handel, ikke er omfattet af ansvarsfritagelsen;

[1] Vedtagne tekster, P8_TA(2016)0009.

OPLYSNINGER OM VEDTAGELSE I RÅDGIVENDE UDVALG

Dato for vedtagelse	8.6.2017
Resultat af den endelige afstemning	+: 0 –: 0 0: 0

OPLYSNINGER OM VEDTAGELSE I KORRESPONDERENDE UDVALG

Dato for vedtagelse	11.7.2017
Resultat af den endelige afstemning	+: 50 –: 4 0: 2
Til stede ved den endelige afstemning - medlemmer	Jan Philipp Albrecht, Gerard Batten, Malin Björk, Michał Boni, Caterina Chinnici, Agustín Díaz de Mera García Consuegra, Frank Engel, Tanja Fajon, Raymond Finch, Monika Flašíková Beňová, Kinga Gál, Ana Gomes, Nathalie Griesbeck, Sylvie Guillaume, Jussi Halla-aho, Sophia in ‘t Veld, Dietmar Köster, Barbara Kudrycka, Cécile Kashetu Kyenge, Marju Lauristin, Juan Fernando López Aguilar, Monica Macovei, Roberta Metsola, Claude Moraes, Soraya Post, Judith Sargentini, Birgit Sippel, Branislav Škripek, Csaba Sógor, Traian Ungureanu, Bodil Valero, Kristina Winberg, Tomáš Zdechovský, Auke Zijlstra
Til stede ved den endelige afstemning – stedfortrædere	Kostas Chrysogonos, Carlos Coelho, Pál Csáky, Anna Hedh, Marek Jurek, Miltiadis Kyrkos, Jean Lambert, Jeroen Lenaers, Morten Helveg Petersen, John Procter, Christine Revault D’Allonnes Bonnefoy, Petri Sarvamaa, Barbara Spinelli, Jaromír Štětina, Axel Voss, Elissavet Vozemberg-Vrionidi
Til stede ved den endelige afstemning – stedfortrædere (forretningsordenens art. 200, stk. 2)	Beatriz Becerra Basterrechea, Izaskun Bilbao Barandica, André Elissen, Arne Gericke, Josu Juaristi Abaunz, Georg Mayer

ENDELIG AFSTEMNING VED NAVNEOPRÅB
I KORRESPONDERENDE UDVALG

50	+
ALDE	Beatriz Becerra Basterrechea, Izaskun Bilbao Barandica, Nathalie Griesbeck, Morten Helveg Petersen, Sophia in 't Veld
ECR	Arne Gericke, Jussi Halla-aho, Marek Jurek, Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Malin Björk, Kostas Chrysogonos, Josu Juaristi Abaunz, Barbara Spinelli
PPE	Michał Boni, Carlos Coelho, Pál Csáky, Agustín Díaz de Mera García Consuegra, Frank Engel, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Roberta Metsola, Petri Sarvamaa, Jaromír Štětina, Csaba Sógor, Traian Ungureanu, Axel Voss, Elissavet Vozemberg-Vrionidi, Tomáš Zdechovský
S&D	Caterina Chinnici, Tanja Fajon, Monika Flašíková Beňová, Ana Gomes, Sylvie Guillaume, Anna Hedh, Cécile Kashetu Kyenge, Miltiadis Kyrkos, Dietmar Köster, Marju Lauristin, Juan Fernando López Aguilar, Claude Moraes, Soraya Post, Christine Revault D'Allonnes Bonnefoy, Birgit Sippel
VERTS/ALE	Jan Philipp Albrecht, Jean Lambert, Judith Sargentini, Bodil Valero

4	-
EFDD	Gerard Batten, Raymond Finch
ENF	André Elissen, Auke Zijlstra

2	0
EFDD	Kristina Winberg
ENF	Georg Mayer

Tegnforklaring:
+ : for
- : imod
0 : hverken/eller