Torek, 3. oktober 2017

P8_TA(2017)0366

Boj proti kibernetski kriminaliteti

Resolucija Evropskega parlamenta z dne 3. oktobra 2017 o boju proti kibernetski kriminaliteti (2017/2068(INI))

(2018/C 346/04)

Evropski parlament,

— ob upoštevanju členov 2, 3 in 6 Pogodbe o Evropski uniji (PEU),

— ob upoštevanju členov 16, 67, 70, 72, 73, 75, 82, 83, 84, 85. 87 in 88 Pogodbe o delovanju Evropske unije (PDEU),

— ob upoštevanju členov 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 in 52 Listine Evropske unije o temeljnih pravicah,

— ob upoštevanju Konvencije ZN o otrokovih pravicah z dne 20. novembra 1989,

— ob upoštevanju Izbirnega protokola h Konvenciji ZN o otrokovih pravicah glede prodaje otrok, otroške prostitucije in otroške pornografije z dne 25. maja 2000,

— ob upoštevanju stockholmske deklaracije in agende za ukrepanje, ki sta bili sprejeti na prvem svetovnem kongresu proti komercialnemu spolnemu izkoriščanju otrok, svetovne zaveze iz Jokohame, ki je bila sprejeta na drugem svetovnem kongresu proti komercialnemu spolnemu izkoriščanju otrok, ter zaveze in akcijskega načrta iz Budimpešte, ki sta bila sprejeta na pripravljalni konferenci za drugi svetovni kongres proti komercialnemu spolnemu izkoriščanju otrok;

— ob upoštevanju konvencije Sveta Evrope z dne 25. oktobra 2007 o zaščiti otrok pred spolnim izkoriščanjem in zlorabo,

— ob upoštevanju svoje resolucije z dne 20. novembra 2012 o zaščiti otrok v digitalnem svetu ([1]),

— ob upoštevanju svoje resolucije z dne 11. marca 2015 o spolni zlorabi otrok na internetu ([2]),

— ob upoštevanju Okvirnega sklepa Sveta 2001/413/JAI z dne 28. maja 2001 o boju proti goljufijam in ponarejanju v zvezi z negotovinskimi plačilnimi sredstvi ([3]),

— ob upoštevanju konvencije o kibernetski kriminaliteti iz Budimpešte z dne 23. novembra 2001 ([4]) in njenega dodatnega protokola,

— ob upoštevanju Uredbe (ES) št. 460/2004 Evropskega parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij ([5]),

([1]) UL C 419, 16.12.2015, str. 33.
([2]) UL C 316, 30.8.2016, str. 109.
([3]) UL L 149, 2.6.2001, str. 1.
([4]) Svet Evrope, Serija Evropskih pogodb, št. 185, 23.11.2001.
([5]) UL L 77, 13.3.2004, str. 1.

— ob upoštevanju Direktive Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanju njene zaščite ([1]),

— ob upoštevanju Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij ([2]),

— ob upoštevanju Direktive 2011/93/EU Evropskega parlamenta in Sveta z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ ([3]),

— ob upoštevanju skupnega sporočila z dne 7. februarja 2013 Komisije in podpredsednice Komisije/visoke predstavnice Unije za zunanje zadeve in varnostno politiko Evropskemu parlamentu, Svetu, Evropskemu ekonomskemu in socialnemu odboru in Odboru regij z naslovom Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor (JOIN(2003)0001),

— ob upoštevanju Direktive 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ ([4]),

— ob upoštevanju Direktive 2014/41/EU Evropskega parlamenta in Sveta z dne 3. aprila 2014 o evropskem preiskovalnem nalogu v kazenskih zadevah ([5]) (direktiva o EPN),

— ob upoštevanju sodbe Sodišča Evropske unije (SEU) z dne 8. aprila 2014 ([6]), s katero je razveljavilo direktivo EU o hrambi podatkov,

— ob upoštevanju svoje resolucije z dne 12. septembra 2013 o strategiji Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor ([7]),

— ob upoštevanju sporočila Komisije z dne 6. maja 2015 z naslovom Strategija za enotni digitalni trg za Evropo (COM(2015)0192),

— ob upoštevanju sporočila Komisije z dne 28. aprila 2015 z naslovom Evropska agenda za varnost (COM(2015)0185) in kasnejših poročil o spremljanju napredka pri vzpostavljanju učinkovite in prave varnostne unije,

— ob upoštevanju poročila konference o pristojnosti v kibernetskem prostoru, ki je potekala 7. in 8. marca 2016 v Amsterdamu,

— ob upoštevanju Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (splošna uredba o varstvu podatkov) ([8]),

---

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

— ob upoštevanju Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ ([1]),

— ob upoštevanju Uredbe (EU) 2016/794 Evropskega parlamenta in Sveta z dne 11. maja 2016 o Agenciji Evropske unije za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Europol) ([2]),

— ob upoštevanju sklepa Komisije z dne 5. julija 2016 o podpisu pogodbenega sporazuma o javno-zasebnem partnerstvu za industrijske raziskave in inovacije na področju kibernetske varnosti med Evropsko unijo, ki jo predstavlja Komisija, in partnerskimi organizacijami (C(2016)4400),

— ob upoštevanju skupnega sporočila Komisije in podpredsednice Komisije/visoke predstavnice Unije za zunanje zadeve in varnostno politiko Evropskemu parlamentu in Svetu z dne 6. aprila 2016 z naslovom Skupni okvir o preprečevanju hibridnih groženj: odziv Evropske unije (JOIN(2016)0018),

— ob upoštevanju sporočila Komisije z naslovom Evropska strategija za boljši internet za otroke (COM(2012)0196) ter poročila Komisije z dne 6. junija 2016 z naslovom Končna ocena večletnega programa EU za zaščito otrok, ki uporabljajo internet in druge komunikacijske tehnologije (Varnejši internet) (COM(2016)0364),

— ob upoštevanju skupne izjave Europola in Agencije Evropske unije za varnost omrežij in informacij (ENISA) z dne 20. maja 2016 o zakonitem kazenskem preiskovanju, ki spoštuje varstvo podatkov v 21. stoletju;

— ob upoštevanju sklepov Sveta z dne 9. junija 2016 o Evropski pravosodni mreži za kibernetsko kriminaliteto,

— ob upoštevanju Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji ([3]),

— ob upoštevanju stališča agencije ENISA o šifriranju iz decembra 2016 – močno šifriranje ščiti našo digitalno identiteto,

— ob upoštevanju končnega poročila skupine za dokazno gradivo v oblaku Sveta Evrope (T-CY) z naslovom Dostop do elektronskega dokaznega gradiva v oblaku za namene kazenskega pravosodja: priporočila za obravnavo v skupini T-CY z dne 16. septembra 2016,

— ob upoštevanju dela Projektne skupine za skupno ukrepanje na področju kibernetske kriminalitete (J-CAT),

— ob upoštevanju Europolove ocene ogroženosti zaradi nevarnosti organiziranega kriminala (EU SOCTA) z dne 28. februarja 2017 in ocene nevarnosti internetnega organiziranega kriminala (IOCTA) z dne 28. septembra 2016,

— ob upoštevanju sodbe Sodišča Evropske unije v zadevi C-203/15 (sodba TELE2) z dne 21. decembra 2016 ([4]),

([1]) UL L 119, 4.5.2016, str. 89.
([2]) UL L 135, 24.5.2016, str. 53.
([3]) UL L 194, 19.7.2016, str. 1.
([4]) Sodba Sodišča z dne 21. decembra 2016, Tele2 Sverige AB proti Post-och telestyrelsen in Secretary of State for the Home Department proti Tomu Watsonu in drugim, C-203/15, ECLI:EU:C:2016:970.

Torek, 3. oktober 2017

— ob upoštevanju Direktive (EU) 2017/541 Evropskega parlamenta in Sveta z dne 15. marca 2017 o boju proti terorizmu in nadomestitvi Okvirnega sklepa Sveta 2002/475/PNZ ter o spremembi Sklepa Sveta 2005/671/PNZ ([1]),

— ob upoštevanju člena 52 Poslovnika,

— ob upoštevanju poročila Odbora za državljanske svoboščine, pravosodje in notranje zadeve in mnenja Odbora za notranji trg in varstvo potrošnikov (A8-0272/2017),

A. ker kibernetska kriminaliteta povzroča družbi in gospodarstvu vse večjo škodo, vpliva na temeljne pravice posameznikov, ogroža pravni red kibernetskega prostora in spravlja v nevarnost stabilnost demokratičnih družb;

B. ker je kibernetska kriminaliteta vse večja težava v državah članicah;

C. ker se je pri oceni IOCTA 2016 pokazalo, da postaja kibernetski kriminal vse bolj intenziven, celovit in razsežen, da je število prijavljenih primerov kibernetske kriminalitete v nekaterih državah EU večje od tradicionalnega kriminala, da se širi na druga področja kriminalitete, na primer trgovine z ljudmi, da zloraba orodij za šifriranje in anonimizacijo za kriminalne namene narašča ter da je napadov z izsiljevalskim programjem več kot tradicionalnih groženj z zlonamerno programsko opremo;

D. ker je bilo leta 2016 za 20 % več napadov na strežnike Komisije kot leta 2015;

E. ker je ranljivost računalnikov za napade posledica specifičnega načina, kako se je informacijska tehnologija z leti razvijala, hitrosti, s katero raste spletno poslovanje, in pomanjkanja vladnih ukrepov;

F. ker se črni trg na področju računalniškega izsiljevanja, uporabe najetih botnetov in hekanja ter ukradenega digitalnega blaga širi;

G. ker je glavni poudarek kibernetskih napadov še naprej zlonamerna programska oprema, kot so trojanski konji v bančništvu, vendar pa se povečuje tudi število in učinek napadov na industrijske nadzorne sisteme in omrežja, katerih namen je uničiti kritično infrastrukturo, gospodarske strukture in destabilizirati družbo, kot je to bilo v primeru napada z izsiljevalskim programjem „WannaCry“ maja 2017, in tako predstavljajo naraščajočo grožnjo za varnost, obrambo in druge pomembne sektorje; ker je večina mednarodnih zaprosil organov kazenskega pregona za podatke povezanih z utajo in finančnim kriminalom, ki jima sledijo nasilna in huda kazniva dejanja;

H. ker vedno večja medsebojna povezanost ljudi, krajev in stvari prinaša številne koristi, povečuje pa tveganje za kibernetsko kriminaliteto; ker naprave, povezane z internetom stvari, vključno s pametnimi omrežji, povezanimi hladilniki, avtomobili, medicinsko opremo in pripomočki, pogosto niso tako dobro zaščitene kot tradicionalne internetne naprave, zato so idealna tarča kibernetskih kriminalcev, zlasti ker je režim varnostnih posodobitev povezanih naprav pogosto nepopoln, včasih pa sploh ne obstaja; ker naprave interneta stvari, ki nadzorujejo fizična sprožila, v katere vdrejo hekerji, dejansko ogrožajo življenja ljudi;

I. ker je uspešen pravni okvir za varstvo podatkov nujen za krepitev zaupanja v spletno okolje, saj bo potrošnikom in podjetjem omogočil, da v celoti izkoristijo prednosti enotnega digitalnega trga in se zoperstavijo kibernetski kriminaliteti;

J. ker se podjetja sama ne morejo spopasti z izzivom, da bi povečali varnost digitalnega sveta, vlade pa bi morale s predpisi in spodbudami za varnejše vedenje uporabnikov prispevati h kibernetski varnosti;

([1]) UL L 88, 31.3.2017, str. 6.

K. ker se meje med kibernetsko kriminaliteto, vohunstvom, vojskovanjem, sabotažo in terorizmom vse bolj zabrisujejo; ker lahko kibernetski kriminal meri na posameznike, javnost ali zasebne subjekte ter pokriva vrsto kaznivih dejanj, kot so kršitve zasebnosti, spolna zloraba otrok na spletu, javno spodbujanje k nasilju in sovraštvu, sabotaža, vohunstvo, finančni kriminal in goljufije, na primer plačilne goljufije, kraje in kraje identitete ter nezakonito poseganje v sistem;

L. ker je Svetovni gospodarski forum v svojem Poročilu o globalnih tveganjih 2017 navedel, da je obsežen incident na področju goljufije s podatki in kraje podatkov eno izmed petih najverjetnejših in najpomembnejših svetovnih tveganj;

M. ker se veliko število primerov kibernetskega kriminala ne preganja ali kaznuje; ker so prijave še vedno redke, obdobja odkrivanja dolga (kar storilcem teh kaznivih dejanj omogoča, da razvijejo večkratni vstop/izstop ali stranska vrata), dostop do elektronskih dokazov je težaven, prihaja do težav s pridobivanjem dokazov in dopustnostjo na sodišču, postopki in pravosodni izzivi pa so tudi obsežni, kar je posledica čezmejne narave kibernetskega kriminala;

N. ker je Svet v svojih sklepih iz junija 2016 poudaril, da je glede na čezmejno naravo kibernetskega kriminala ter skupno ogroženost kibernetske varnosti, s katero se sooča EU, okrepljeno sodelovanje in izmenjava informacij med policijskimi in pravosodnimi organi ter strokovnjaki za kibernetsko kriminaliteto bistvenega pomena za izvajanje učinkovitih preiskav v kibernetskem prostoru in pridobitev elektronskih dokazov;

O. ker razveljavitev direktive o hrambi podatkov, ki izhaja iz sodbe Sodišča Evropske unije z dne 8. aprila 2014, pa tudi prepoved splošne, neselektivne in neciljne hrambe podatkov, ki jo potrjuje sodba Sodišča Evropske unije v zadevi TELE2 z dne 21. decembra 2016, predpisujeta strogo omejevanje obdelave množičnih telekomunikacijskih podatkov in dostopa pristojnih organov do njih;

P. ker sodba Sodišča Evropske unije v zadevi Maximillian Schrems ([1]) poudarja, da je množični nadzor kršitev temeljnih pravic;

Q. ker mora boj proti kibernetski kriminaliteti spoštovati ista procesna in materialna jamstva in temeljne pravice, zlasti glede varstva podatkov in svobode govora, kot boj na področju vseh drugih kaznivih dejanj;

R. ker otroci uporabljajo internet vse mlajši in ker so še posebej izpostavljeni temu, da postanejo žrtve pridobivanja za spolne namene in drugih oblik spolnega izkoriščanja na spletu (kibernetskega nadlegovanja ter spolne zlorabe, prisile in izsiljevanja), zlorabe osebnih podatkov, pa tudi nevarnih kampanj za spodbujanje različnih vrst samopoškodb, kot v primeru „sinji kit“, in zato potrebujejo posebno zaščito; ker lahko spletni storilci s pomočjo klepetalnic, elektronske pošte, spletnih iger in družabnih omrežij hitreje najdejo žrtve, da bi jih pridobili za spolne namene, ter ker skrita omrežja enakovrednih računalnikov (P2P) ostajajo osrednje platforme za storilce kaznivih dejanj zoper spolno nedotakljivost otrok za dostop do, posredovanje, shranjevanje in izmenjavo gradiva spolnega izkoriščanja otrok in za neopazno iskanje novih žrtev;

S. ker je naraščajoči trend spolne prisile in izsiljevanja še vedno premalo raziskan in premalokrat prijavljen, zlasti zaradi narave kaznivega dejanja, ki ga spremljata sram in krivda, ki ju občuti žrtev;

T. ker je po poročanjih zloraba otrok v živo in na daljavo naraščajoča grožnja; ker ima zloraba otrok v živo in na daljavo najočitnejšo povezavo s komercialnim razširjanjem gradiva spolnega izkoriščanja otrok;

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

U. ker je nacionalna kriminalistična agencija v Združenem kraljestvu v nedavni študiji ugotovila, da je za mlade, ki se ukvarjajo s hekanjem, denar manj pomemben kot navduševanje prijateljev ali zoperstavljanje političnemu sistemu z napadi na računalniška omrežja;

V. ker se je ozaveščenost o tveganjih kibernetskega kriminala povečala, vendar posamezniki, javne ustanove in podjetja še vedno neustrezno uporabljajo preventivne ukrepe, predvsem zaradi pomanjkanja znanja in virov;

W. ker boj proti kibernetski kriminaliteti in nezakonitim spletnim dejavnostim ne bi smel prikrivati pozitivnih vidikov, ki jih nudi brezplačno in odprto kibernetsko okolje z novimi možnostmi za širitev znanja in spodbujanjem političnega in družbenega vključevanja po vsem svetu;

Splošne ugotovitve

1. poudarja, da nagel porast izsiljevalskega programja, botnetov in nedovoljenega povzročanja škode v računalniških sistemih vpliva na varnost posameznikov, razpoložljivost in celovitost njihovih osebnih podatkov, varstvo zasebnosti in temeljnih svoboščin ter celovitost kritične infrastrukture, kar vključuje, ni pa omejeno na, oskrbo z energijo in elektriko ter finančne strukture, kot so borze; v zvezi s tem želi opomniti, da je boj proti kibernetski kriminaliteti v evropski agendi za varnost z dne 28. aprila 2015 opredeljen kot prednostna naloga;

2. poudarja, da je treba uskladiti skupne opredelitve kibernetskega kriminala, kibernetskega vojskovanja, kibernetske varnosti, kibernetskega nadlegovanja in kibernetskih napadov, da bi zagotovili skupno pravno opredelitev v institucijah EU in državah članicah EU;

3. poudarja, da bi se morali v boju proti kibernetski kriminaliteti osredotočiti na zaščito in utrditev kritične infrastrukture in drugih omreženih naprav, ne le na izvajanje represivnih ukrepov;

4. poudarja pomen pravnih ukrepov, sprejetih na evropski ravni, za uskladitev opredelitve kaznivih dejanj, povezanih z napadi na informacijske sisteme ter spolnim izkoriščanjem otrok na spletu, ter za uvedbo obveznosti za države članice, da vzpostavijo sistem za beleženje, izdelavo in zagotavljanje statističnih podatkov o teh kaznivih dejanjih, za učinkovito ukrepanje proti njim;

5. odločno poziva tiste države članice, ki še niso prenesle Direktive 2011/93/EU o boju proti spolni zlorabi in spolnemu izkoriščanju otrok ter otroški pornografiji in je še ne izvajajo, naj to ustrezno in brez odlašanja storijo; poziva Komisijo, naj budno spremlja in zagotavlja celovito in učinkovito izvajanje te direktive ter naj o svojih ugotovitvah pravočasno poroča Parlamentu in pristojnemu parlamentarnemu odboru, hkrati pa naj nadomesti Okvirni sklep Sveta 2004/68/PNZ; poudarja, da je treba Eurojustu in Europolu dodeliti ustrezna sredstva, potrebna za boljšo identifikacijo žrtev, boj proti organiziranim mrežam storilcev kaznivih dejanj spolne zlorabe ter hitrejše odkrivanje, pregledovanje in prijavljanje materiala o zlorabi otrok na spletu in zunaj njega;

6. obžaluje dejstvo, da je 80 % podjetij v Evropi že doživelo vsaj en kibernetski incident in da kibernetskih napadov zoper podjetja pogosto ni mogoče odkriti ali niso prijavljeni; opozarja, da različne študije ocenjujejo, da so letni stroški kibernetskih napadov za svetovno gospodarstvo precejšnji; meni, da bosta obvezno razkritje kršitev varnosti ter izmenjava informacij o tveganjih, uvedena z Uredbo (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (Splošna uredba o varstvu podatkov) in Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (direktiva o varnosti omrežij in informacij), pripomogla k reševanju tega problema z zagotavljanjem podpore za podjetja, zlasti za mala in srednja;

7. poudarja, da stalno spreminjanje značilnosti krajine kibernetskih groženj prinaša za vse deležnike hude pravne in tehnološke izzive; meni, da na nove tehnologije ne bi smeli gledati kot na grožnjo, in priznava, da se bo s tehnološkim napredkom pri šifriranju izboljšala splošna varnost naših informacijskih sistemov, kar bo končnim uporabnikom omogočalo boljšo zaščito podatkov in komunikacij; vendar poudarja, da še vedno obstajajo pomembne vrzeli pri varstvu komunikacij in da lahko tehnike, kot so anonimna komunikacija (onion routing) in skrita omrežja, uporabljajo zlonamerni

uporabniki, vključno s teroristi in storilci kaznivih dejanj zoper spolno nedotakljivost otrok, hekerji, ki jih sponzorirajo tuje države, ki niso prijateljske, ali ekstremistične politične ali verske organizacije za prikrivanje kriminalne namene, zlasti za prikrivanje svojih kriminalnih dejavnosti ali identitete, kar povzroča resne izzive za preiskave;

8. je globoko zaskrbljen zaradi nedavnega svetovnega napada z izsiljevalskim programjem, ki naj bi napadel na desetine tisočev računalnikov v skoraj 100 državah ter številne organizacije, med drugim nacionalni zdravstveni sistem v Združenem kraljestvu, ki je bil najodmevnejša žrtev tega obsežnega napada z zlonamerno programsko opremo; je v zvezi s tem seznanjen s pomembnim delom pobude No More Ransom, ki ponuja več kot 40 brezplačnih orodij za dešifriranje, ki žrtvam izsiljevalskega programja po vsem svetu omogočajo dešifriranje napadenih naprav;

9. poudarja, da skrita omrežja in anonimna komunikacija (onion routing) omogočajo tudi svobodno okolje za novinarje, politične aktiviste in zagovornike človekovih pravic v določenih državah, s čimer se izognejo, da bi jih odkrili represivni državni organi;

10. ugotavlja, da kriminalne in teroristične mreže še vedno v omejenem obsegu uporabljajo orodja in sredstva kibernetskega kriminala; vendar poudarja, da se utegne to spremeniti zaradi vse tesnejših povezav med terorizmom in organiziranim kriminalom ter široko razpoložljivostjo orožja in sestavin za eksplozive na skritih omrežjih;

11. ostro obsoja vsako poseganje v sistem, ki ga izvedejo ali naročijo tuje države ali njihovi agenti, da bi ovirali demokratični proces v drugi državi;

12. poudarja, da čezmejne zahteve za zaseg domene, odstranitev vsebine in dostop do podatkov uporabnika ustvarjajo resne izzive, ki zahtevajo takojšnje ukrepanje, saj se nanašajo na pomembne zadeve; v zvezi s tem poudarja, da so mednarodni okviri na področju človekovih pravic, ki veljajo tako na spletu kot zunaj njega, pomemben standard na svetovni ravni;

13. poziva države članice, naj zagotovijo, da bodo žrtve kibernetskih napadov v celoti upravičene do vseh pravic, opredeljenih v Direktivi 2012/29/EU, ter naj povečajo prizadevanja na področju identifikacije žrtev in namenskih storitev zanje, tudi z nadaljnjo podporo projektni skupini Europola za identificiranje žrtev; poziva države članice, naj čim prej v sodelovanju z Europolom vzpostavijo s tem povezane platforme s ciljem zagotoviti, da bi vsi uporabniki interneta znali zaprositi za pomoč, če so tarča nezakonitega spletnega napada; poziva Komisijo, naj pripravi študijo o posledicah čezmejne kibernetske kriminalitete na podlagi Direktive 2012/29/EU;

14. poudarja, da Europolova ocena IOCTA za leto 2014 navaja potrebo po učinkovitejših in uspešnejših pravnih orodjih, ob upoštevanju sedanjih omejitev postopka iz sporazuma o medsebojni pravni pomoči, in zagovarja nadaljnjo harmonizacijo zakonodaje v EU, kadar je ustrezna;

15. poudarja, da kibernetska kriminaliteta resno ogroža delovanje enotnega digitalnega trga, saj zmanjšuje zaupanje v ponudnike digitalnih storitev, ogroža čezmejne transakcije in resno škoduje interesom potrošnikov digitalnih storitev;

16. poudarja, da so lahko strategije in ukrepi za kibernetsko varnost dobri in učinkoviti le, če so osnovani na temeljnih pravicah in svoboščinah, določenih v Listini Evropske unije o temeljnih pravicah, in temeljnih vrednotah EU;

17. poudarja, da obstaja legitimna in močna potreba po varstvu komunikacije med posamezniki ter med posamezniki in javnimi ter zasebnimi organizacijami za preprečevanje kibernetske kriminalitete; poudarja, da lahko z močno kriptografijo zadostimo tej potrebi; nadalje poudarja, da bo omejevanje uporabe ali slabitev moči kriptografskih orodij ustvarilo ranljivosti, ki se lahko izkoristijo za kriminalne namene in zmanjšajo zaupanje v elektronske storitve, kar bo posledično škodilo tako civilni družbi kot industriji;

18. poziva k oblikovanju akcijskega načrta za zaščito otrokovih pravic na spletu in drugje v kibernetskem prostoru in opominja, da morajo organi kazenskega pregona v boju proti kibernetski kriminaliteti posebno pozornost posvetiti kaznivim dejanjem zoper otroke; v zvezi s tem poudarja, da je treba okrepiti pravosodno in policijsko sodelovanje med

državami članicami in z Europolom in Evropskim centrom za boj proti kibernetski kriminaliteti (EC3) z namenom preprečevanja kibernetske kriminalitete in boja proti njej, zlasti spolnega izkoriščanja otrok na spletu;

19. poziva Komisijo in države članice, naj uvedejo vse pravosodne ukrepe za boj proti pojavu nasilja nad ženskami na spletu in kibernetskega nadlegovanja; zlasti poziva EU in države članice, naj združijo moči in vzpostavijo kazenskopravni okvir, ki bo spletne korporacije obvezal k izbrisu ali prenehanju širjenja ponižujoče in žaljive vsebine; poziva tudi k uvedbi psihološke podpore za ženske žrtve spletnega nasilja in deklice, ki so bile izpostavljene kibernetskemu nadlegovanju;

20. poudarja, da bi bilo treba nezakonite spletne vsebine z ustreznim pravnim postopkom takoj odstraniti; poudarja vlogo industrije informacijskih in komunikacijskih tehnologij ter ponudnikov internetnih storitev in ponudnikov spletnega gostovanja pri zagotavljanju hitre in učinkovite odstranitve nezakonitih spletnih vsebin na zahtevo pristojnega organa kazenskega pregona;

Preprečevanje

21. poziva Komisijo, naj v okviru pregleda evropske strategije za kibernetsko varnost še naprej išče ranljivosti v varnosti omrežij in informacij evropske kritične infrastrukture, spodbudi razvoj odpornih sistemov ter oceni stanje glede boja proti kibernetski kriminaliteti v EU in državah članicah, da se doseže boljše razumevanje trendov in razvoja dogodkov glede kaznivih dejanj v kibernetskem prostoru;

22. poudarja, da je kibernetska odpornost bistvena za preprečevanje kibernetske kriminalitete in bi ji morali zato pripisati kar največji pomen; poziva države članice, naj sprejmejo proaktivne politike in ukrepe za zaščito omrežij in kritične infrastrukture ter poziva k celovitemu evropskemu pristopu k boju proti kibernetski kriminaliteti, ki bi bil združljiv s temeljnimi pravicami, varstvom podatkov, kibernetsko varnostjo, varstvom potrošnikov in elektronskim trgovanjem;

23. pri tem pozdravlja vlaganje sredstev EU v raziskovalne projekte, kot je javno-zasebno partnerstvo na področju kibernetske varnosti, da bi se evropska kibernetska odpornost povečala z inovacijami in izgradnjo zmogljivosti; priznava zlasti prizadevanja javno-zasebnega partnerstva za kibernetsko varnost, da bi razvili ustrezne načine odzivanja za ranljivosti ničtega dne (zero-day vulnerability);

24. v zvezi s tem poudarja velik pomen proste in odprtokodne programske opreme; poziva, naj se da na voljo več finančnih sredstev EU specifično za raziskave na področju varnosti informacijske tehnologije, ki bodo temeljile na prosti in odprtokodni programski opremi;

25. z zaskrbljenostjo ugotavlja, da vlada pomanjkanje kvalificiranih strokovnjakov za IT, ki delajo na področju kibernetske varnosti; poziva države članice, naj vlagajo v izobraževanje;

26. meni, da bi morala uredba igrati večjo vlogo pri upravljanju tveganj za kibernetsko varnost prek izboljšanih proizvodnih standardov in standardov programske opreme za oblikovanje in poznejše posodobitve, kot tudi minimalnih standardov glede uporabniških imen in gesel;

27. poziva države članice, naj okrepijo izmenjavo informacij prek Eurojusta, Europola in agencije ENISA, pa tudi izmenjavo dobre prakse prek evropske mreže skupin za odzivanje na incidente na področju računalniške varnosti ter skupin za odzivanje na računalniške grožnje, o izzivih, s katerimi se soočajo na področju boja proti kibernetski kriminaliteti, ter konkretnih pravnih in tehničnih rešitvah za njihovo obravnavo in povečanje kibernetske odpornosti; v zvezi s tem poziva Komisijo, naj spodbuja učinkovito sodelovanje in lažjo izmenjavo informacij, da bi se predvidela in obvladala možna tveganja, kot je določeno v direktivi o varnosti omrežij in informacij;

28. je zaskrbljen zaradi ugotovitve Europola, da je večina napadov na posameznike uspešnih zaradi pomanjkljive digitalne higiene in ozaveščenosti uporabnikov ter nezadostnega namenjanja pozornosti tehničnim varnostnim ukrepom, na primer vgrajeni varnosti; poudarja, da so uporabniki prve žrtve slabo varovane strojne in programske opreme;

29. poziva Komisijo in države članice, naj začnejo uravnoteženo kampanjo ozaveščanja, v kateri bodo sodelovali vsi pomembni akterji in deležniki, da bodo otroci bolje ozaveščeni o tveganjih na internetu in tem, kako se lahko pred njimi zaščitijo, starši, skrbniki in učitelji pa bodo imeli podporo pri razumevanju teh tveganj in zaščiti varnosti otrok, naj podprejo države članice pri oblikovanju programov za preprečevanje spolne zlorabe na spletu, podprejo kampanje ozaveščanja o odgovornem ravnanju v družabnih medijih in spodbudijo glavne ponudnike spletnih iskalnikov in družabnih omrežij k proaktivnemu pristopu k zaščiti varnosti otrok na spletu;

30. poziva Komisijo in države članice, naj uvedejo kampanje za ozaveščanje in preprečevanje ter spodbujajo dobre prakse, da bi se državljani, predvsem otroci in drugi ranljivi uporabniki, pa tudi centralni in lokalni organi oblasti, ključni operaterji in zasebni sektor, zlasti mala in srednja podjetja, zavedali tveganj, povezanih s kibernetsko kriminaliteto, in vedeli, kako biti varen na spletu in kako zaščititi svoje naprave; nadalje poziva Komisijo in države članice, naj spodbujajo praktične varnostne ukrepe, kot so šifriranje ali druge tehnologije, ki omogočajo večjo varnost in zasebnost, in orodja za anonimizacijo;

31. poudarja, da morajo kampanje ozaveščanja spremljati izobraževalni programi „ozaveščeni uporabi“ instrumentov informacijske tehnologije; spodbuja države članice, naj v šolske učne načrte računalništva vključijo kibernetsko varnost ter nevarnosti in posledice uporabe osebnih podatkov na spletu; v zvezi s tem opozarja na prizadevanja v okviru evropska strategije za boljši internet za otroke;

32. poudarja, da je v boju proti kibernetski kriminaliteti nujno potrebnih več prizadevanj na področju izobraževanja in usposabljanja o varnosti omrežij in informacij, z uvedbo usposabljanja na področju varnosti omrežij in informacij, razvoja varne programske opreme in varstva osebnih podatkov za študente računalništva, pa tudi osnovnega usposabljanja na področju varnosti omrežij in informacij za osebje v javni upravi;

33. meni, da bi lahko bilo zavarovanje proti kibernetskemu vdiranju v informacijske sisteme eno od orodij za spodbujanje ukrepov na področju varnosti tako s strani podjetij, ki so odgovorna za zasnovo programske opreme, kot uporabnikov, ki se jih poziva k pravilni uporabi programske opreme;

34. poudarja, da bi morala podjetja z rednimi ocenami opredeliti ranljivosti in tveganja, zaščititi svoje proizvode in storitve s takojšnjo odpravo ranljivosti, vključno z ukrepi za upravljanje programskih popravkov in posodobitvami varstva podatkov, ublažiti učinek napadov z izsiljevalskim programjem z vzpostavitvijo zanesljive rezervne ureditve in doslednim poročanjem o kibernetskih napadih;

35. poziva države članice, naj vzpostavijo skupine za odzivanje na računalniške grožnje, predvidene v direktivi o varnosti omrežij in informacij, ki bi jim podjetja in potrošniki poročali o zlonamernih elektronskih sporočilih in spletnih mestih, da bi bile države članice redno obveščene o varnostnih incidentih ter ukrepih za boj proti njim in za zmanjšanje tveganja za lastne sisteme; spodbuja države članice, naj razmislijo o vzpostavitvi podatkovne zbirke za evidentiranje vseh vrst kibernetske kriminalitete ter za spremljanje razvoja teh pojavov;

36. poziva države članice, naj vlagajo v večjo varnost kritične infrastrukture in z njo povezanih podatkov, da bi se ubranile kibernetskih napadov;

Torek, 3. oktober 2017

Povečanje odgovornosti in obveznosti ponudnikov storitev

37. meni, da je boljše sodelovanje med pristojnimi organi in ponudniki storitev bistveni dejavnik za pospešitev in racionalizacijo medsebojne pravne pomoči in postopkov vzajemnega priznavanja znotraj evropskega pravnega okvira; poziva ponudnike elektronskih komunikacijskih storitev, ki nimajo sedeža v Uniji, naj pisno določijo predstavnika v Uniji;

38. znova poudarja, da so, kar zadeva internet stvari, proizvajalci ključno izhodišče za poostritev ureditve odgovornosti, ki bo omogočila boljšo kakovost izdelkov ter varnejše okolje v smislu zunanjega dostopa in dokumentiranih posodobitev;

39. meni, da je treba glede na trende na področju inovacij in vse večjo dostopnost naprav interneta stvari posebno pozornost posvetiti varnosti vseh, celo najbolj enostavnih naprav; meni, da je v interesu proizvajalcev strojne opreme in inovativnih razvijalcev programske opreme, da vlagajo v rešitve za preprečevanje kibernetske kriminalitete in si izmenjujejo informacije o ogroženosti kibernetske varnosti; odločno poziva Komisijo in države članice, naj spodbujajo pristop vgrajene varnosti, ter odločno poziva industrijo, naj v vse te naprave vključi vgrajene varnostne rešitve; v zvezi s tem spodbuja zasebni sektor, naj izvaja prostovoljne ukrepe, razvite na podlagi ustrezne zakonodaje EU, kot je direktiva o varnosti omrežij in informacij, in usklajene z mednarodno priznanimi standardi, da bi se povečalo zaupanje v varnost programske opreme in naprav, kot je oznaka zaupanja interneta stvari;

40. spodbuja ponudnike storitev, naj sledijo kodeksu ravnanja na področju boja proti nezakonitemu sovražnemu govoru na spletu, Komisijo in udeležena podjetja pa, naj nadaljujejo sodelovanje v zvezi s tem vprašanjem;

41. opozarja, da so v skladu z Direktivo 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu ([1]) (direktiva o elektronskem poslovanju), posredniki izvzeti iz odgovornosti za vsebino samo, če imajo nevtralno in pasivno vlogo pri poslanih vsebinah in/ali vsebinah, ki jih gostijo, vendar pa zahteva takojšnjo odstranitev ali onemogočitev dostopa do vsebine, če posrednik dejansko ve za kršitev ali nezakonito dejavnost ali informacijo;

42. poudarja, da je nujno treba podatkovne zbirke organov kazenskega pregona zaščititi pred varnostnimi incidenti in nezakonitim dostopanjem, saj je to pomembno za posameznike; izraža zaskrbljenost zaradi dostopa, ki ga imajo organi kazenskega pregona do podatkov zunaj svojega ozemlja v okviru preiskav kaznivih dejanj in poudarja, da so na tem področju potrebna stroga pravila;

43. meni, da je treba vprašanja v zvezi z nezakonitimi spletnimi dejavnostmi hitro in učinkovito reševati, tudi s postopki odstranitve vsebine, če ta ni (oziroma ni več) potrebna za odkrivanje, preiskovanje in kazenski pregon; opozarja, da lahko države članice, kadar odstranitev ni izvedljiva, sprejmejo potrebne in sorazmerne ukrepe za preprečevanje dostopa z ozemlja Unije do take vsebine; poudarja, da morajo biti ti ukrepi skladni z obstoječimi zakonodajnimi in sodnimi postopki ter Listino, prav tako pa morajo zanje veljati ustrezni zaščitni ukrepi, vključno z možnostjo sodnega varstva;

44. poudarja vlogo digitalnih ponudnikov storitev informacijske družbe pri zagotavljanju hitre in učinkovite odstranitve nezakonitih spletnih vsebin na zahtevo pristojnega organa kazenskega pregona, in pozdravlja doseženi napredek, tudi zaradi prispevka spletnega foruma EU; poudarja, da sta nujna močnejša zavezanost in sodelovanje pristojnih organov in ponudnikov storitev informacijske družbe, da bi sektor hitro in učinkovito odstranjeval vsebino in da se nezakonite vsebine ne bi blokirale z vladnimi ukrepi; poziva države članice, naj platformam, ki se tega ne držijo, naložijo pravno odgovornost; znova poudarja, da so lahko ukrepi za odstranitev nezakonitih spletnih vsebin na podlagi pogojev dovoljeni samo, če nacionalni postopkovni predpisi uporabnikom omogočajo, da svoje pravice uveljavljajo pred sodiščem, potem ko so se seznanili takšnimi ukrepi;

45. poudarja, da je v skladu z resolucijo Parlamenta z dne 19. januarja 2016 z naslovom Aktu za enotni digitalni trg naproti ([2]) omejitev odgovornosti posrednikov bistvena za zaščito odprtosti interneta, temeljnih pravic, pravne gotovosti in inovacij; pozdravlja namero Komisije, da zagotovi smernice o postopkih obveščanja in odstranitve, ki bodo spletnim platformam omogočile, da izpolnijo svoje obveznosti in spoštujejo pravila o odgovornosti, opredeljene v direktivi

([1]) UL L 178, 17.7.2000, str. 1.
([2]) Sprejeta besedila, P8_TA(2016)0009.

o elektronskem poslovanju (2000/31/ES), okrepile pravno varnost in povečale zaupanje uporabnikov; poziva Komisijo, naj pripravi zakonodajni predlog na teh področjih;

46. poziva k uporabi pristopa sledenja denarju iz resolucije Evropskega parlamenta z dne 9. junija 2015 o napredku v smeri prenovljenega soglasja glede uveljavljanja pravic intelektualne lastnine: akcijski načrt EU ([1]), na podlagi regulativnega okvira iz direktive o elektronskem poslovanju in direktive o uveljavljanju pravic intelektualne lastnine;

47. poudarja, da je bistvenega pomena zagotoviti stalno in posebno usposabljanje in psihološko podporo za moderatorje vsebin v zasebnih in javnih subjektih, ki so pristojni za presojanje spornih ali nezakonitih spletnih vsebin, saj jih treba šteti za tiste, ki se prvi odzovejo na tem področju;

48. poziva ponudnike storitev, naj zagotovijo jasne oblike prijav ter ustrezno opredelijo podporno infrastrukturo, ki bo zmožna zagotavljati hitro in ustrezno reševanje prijav;

49. poziva ponudnike storitev, naj pospešijo prizadevanja za ozaveščanje o tveganjih, povezanih z uporabo interneta, zlasti za otroke, tako da oblikujejo interaktivna orodja in zagotovijo informacijski material;

Okrepitev policijskega in pravosodnega sodelovanja

50. je zaskrbljen, ker se veliko število kibernetskih kaznivih dejanj ne kaznuje; obžaluje, da ponudniki storitev z uporabo tehnologij, kot je NAT CGN, resno ogrožajo preiskave, saj je tehnično nemogoče ugotoviti, kdo točno uporablja IP-naslov in torej kdo je odgovoren za spletni kriminal; poudarja, da je treba v omejenih primerih omogočiti zakonit dostop organov kazenskega pregona do ustreznih informacij, če je ta dostop nujen in sorazmeren zaradi varnosti in pravice; poudarja, da morajo imeti pravosodni organi in organi kazenskega pregona zadostne zmogljivosti za vodenje zakonitih preiskav;

51. poziva države članice, naj ponudnikom šifriranja ne predpisujejo obveznosti, ki bi oslabile ali ogrozile varnost njihovih omrežij in storitev, kot je ustvarjanje ali omogočanje stranskih vrat; poudarja, da morata zakonodaja in stalni tehnološki razvoj zagotavljati izvedljive rešitve, kadar so te potrebne za pravosodje in varnost; poziva države članice, naj v posvetovanju s sodstvom in Eurojustom sodelujejo pri usklajevanju pogojev za zakonito uporabo preiskovalnih orodij na spletu;

52. poudarja, da je lahko zakonito prestrezanje izjemno učinkovito za boj proti nezakonitem hekanju, pod pogojem, da je nujno, sorazmerno, na podlagi dolžnega pravnega postopanja in v celoti skladno s temeljnimi pravicami, pravom o varstvu podatkov in sodno prakso EU; poziva vse države članice, naj izkoristijo možnosti, ki jih ponuja zakonito prestrezanje, usmerjeno proti posameznim osumljencem, določijo jasna pravila za postopek predhodne sodne odobritve zakonitih dejavnosti prestrezanja, vključno z omejitvami uporabe in trajanja zakonitih orodij hekanja, vzpostavijo nadzorni mehanizem in zagotovijo učinkovita pravna sredstva za tarče teh dejavnosti hekanja;

53. spodbuja države članice, naj se povežejo s skupnostjo, ki skrbi za varnost informacijske in komunikacijske tehnologije, in jo spodbudijo k prevzemanju dejavnejše vloge pri etičnem hekanju in poročanju o nezakonitih vsebinah, kot je gradivo o spolni zlorabi otrok;

54. poziva Europol, naj vzpostavi sistem anonimnega obveščanja s skritih omrežij, ki bo posameznikom omogočal, da pristojnim organom prijavijo nezakonite vsebine, kot so upodobitve spolne zlorabe otrok, in bo uporabljal podobno tehnično zaščito, kot jo imajo številne tiskovne organizacije, ki uporabljajo take sisteme za izmenjavo občutljivih podatkov z novinarji na način, ki omogoča večjo stopnjo anonimnosti in varnosti kot pa običajna elektronska pošta;

([1]) UL C 407, 4.11.2016, str. 25.

Torek, 3. oktober 2017

55. poudarja, da je treba zmanjšati tveganja za zasebnost internetnih uporabnikov zaradi razkritij prijemov ali orodij, ki jih pri svojih zakonitih preiskavah uporabljajo organi kazenskega pregona;

56. poudarja, da morajo biti organi kazenskega pregona opremljeni z zadostnimi zmogljivostmi in sredstvi, da se lahko učinkovito odzivajo na kibernetsko kriminaliteto;

57. poudarja, da mozaik različnih, teritorialno opredeljenih nacionalnih jurisdikcij povzroča težave pri opredelitvi prava, ki se uporablja v nadnacionalnih interakcijah, in pravno negotovost, s tem pa preprečuje čezmejno sodelovanje, ki je nujno za učinkovito obravnavo kibernetske kriminalitete;

58. poudarja, da je treba razviti praktično podlago za skupen pristop EU na področju jurisdikcije v kibernetskem prostoru, kot je bilo poudarjeno na neformalnem srečanju ministrov za pravosodje in notranje zadeve 26. januarja 2016;

59. v zvezi s tem poudarja, da je treba prednost nameniti razvoju skupnih postopkovnih standardov, ki bodo določali ozemeljske dejavnike, ki so podlaga za določitev prava, ki se uporablja v kibernetskem prostoru, in opredelitvi preiskovalnih ukrepov, ki se lahko uporabljajo ne glede na geografske meje;

60. priznava, da bi se s takšnim skupnim evropskim pristopom, ki naj spoštuje temeljne pravice in zasebnost, vzpostavilo zaupanje med deležniki, zmanjšale zamude pri obravnavi čezmejnih zaprosil, vzpostavila interoperabilnost heterogenih akterjev in ustvarila priložnost za vključitev dolžnega pravnega postopanja v operativne okvire;

61. meni, da bi bilo treba dolgoročno razviti tudi skupne svetovne postopkovne standarde na področju izvrševanja pristojnosti v kibernetskem prostoru; v zvezi s tem pozdravlja delo skupine za dokazno gradivo v oblaku Sveta Evrope;

Elektronski dokazi

62. poudarja, da je skupen evropski pristop h kazenskemu pravosodju v kibernetskem prostoru prednostnega pomena, saj bo prispeval k boljšemu izvajanju pravne države na tem področju, lažjemu pridobivanju elektronskih dokazov v kazenskih postopkih in hitremu reševanju primerov;

63. poudarja, da je treba najti načine za hitrejše zavarovanje in pridobivanje elektronskih dokazov in da je potrebno tesno sodelovanje med organi kazenskega pregona (vključno z večjo uporabo skupnih preiskovalnih ekip), tretjimi državami in ponudniki storitev, delujočimi na evropskem ozemlju, v skladu s Splošno uredbo o varstvu podatkov (EU) 2016/679, Direktivo (EU) 2016/680 (policijska direktiva) in obstoječimi sporazumi o medsebojni pravni pomoči; poudarja, da je treba vzpostaviti enotne kontaktne točke v vseh državah članicah in optimizirati uporabo obstoječih kontaktnih točk, kar bo olajšalo dostop do elektronskih dokazov ter izmenjavo informacij, izboljšalo sodelovanje s ponudniki storitev in pospešilo postopke medsebojne pravne pomoči;

64. se zaveda, da je lahko sedanji razdrobljen pravni okvir izziv za ponudnike storitev, ki si prizadevajo upoštevati zahteve organov kazenskega pregona; poziva Komisijo, naj predlaga evropski pravni okvir za elektronske dokaze, vključno z usklajenimi pravili za določanje statusa ponudnika kot domačega ali tujega, in uvede obveznost za ponudnike storitev, da odgovorijo na zaprosila iz drugih držav članic na podlagi dolžnega pravnega postopanja in v skladu z evropskim preiskovalnim nalogom, pri čemer naj upošteva načelo sorazmernosti in prepreči negativne vplive na uresničevanje svobode ustanavljanja in svobode opravljanja storitev ter zagotovi ustrezne zaščitne ukrepe za vzpostavitev pravne varnosti in izboljšanje zmožnosti ponudnikov storitev in posrednikov za odzivanje na zaprosila organov kazenskega pregona;

65. poudarja, da je potreben okvir za elektronske dokaze, ki bo vključeval zadostne zaščitne ukrepe za pravice in svoboščine vseh, ki jih to zadeva; poudarja, da bi to moralo vključevati zahtevo, da se zaprosila za elektronske dokaze na prvi stopnji naslovijo na upravljavce ali lastnike podatkov, da bi se zagotovilo varstvo njihovih pravic in pravic oseb, na katere se podatki nanašajo (na primer njihova pravica uveljavljati varovanje poklicne skrivnosti in uporabo pravnih sredstev v primeru nesorazmernega ali drugače nepooblaščenega dostopa); poudarja, da je treba zagotoviti tudi pravni okvir, ki ščiti

vse ponudnike in vse druge strani pred zaprosili, ki bi lahko povzročila kolizijo zakonov ali kako drugače posegala v suverenost drugih držav;

66. poziva države članice, naj za namene učinkovitega varovanja in pridobivanja elektronskih dokazov v EU v celoti izvajajo Direktivo 2014/41/EU o evropskem preiskovalnem nalogu v kazenskih zadevah (direktiva o EPN) ter v svoje nacionalne kazenske zakonike vključijo posebne določbe v zvezi s kibernetskim prostorom, da omogočijo dostopnost elektronskih dokazov na sodišču in izdajo jasnih smernic za sodnike glede kaznovanja kibernetskega kriminala;

67. pozdravlja delo, ki ga Komisija posveča oblikovanju platforme za sodelovanje z varnim komunikacijskim kanalom za digitalno izmenjavo evropskih preiskovalnih nalogov za elektronske dokaze in odgovorov med pravosodnimi organi EU; poziva Komisijo, naj v sodelovanju z državami članicami, Eurojustom in ponudniki storitev preuči in uskladi obrazce, orodja in postopke za zahtevke za zavarovanje in pridobivanje elektronskih dokazov z namenom lažje avtentikacije, da bi zagotovili hitre postopke in povečali preglednost in odgovornost v procesu zavarovanja in pridobivanja elektronskih dokazov; poziva Agencijo Evropske unije za usposabljanje na področju odkrivanja in pregona kaznivih dejanj, naj razvije module usposabljanja o učinkoviti uporabi obstoječih okvirov za zavarovanje in pridobivanje elektronskih dokazov; pri tem poudarja, da bo uskladitev politike ponudnikov storitev pripomogla k manjši raznolikost pristopov, zlasti glede postopkov in pogojev za odobritev dostopa do zahtevanih podatkov;

Krepitev zmogljivosti na evropski ravni

68. poudarja, da nedavni dogodki jasno kažejo veliko izpostavljenost EU, še zlasti institucij EU, nacionalnih vlad in parlamentov, velikih evropskih podjetij, evropske infrastrukture in omrežij IT, kompleksnim oblikam napadov z zapleteno programsko opremo, tudi zlonamerno; poziva agencijo ENISA, naj redno ocenjuje stopnjo ogroženosti, Komisijo pa, naj vlaga v zmogljivosti informacijskih tehnologij ter v zaščito in odpornost kritične infrastrukture institucij EU, da bi zmanjšali ranljivost EU za resne kibernetske napade, za katere so odgovorne velike hudodelske združbe, ter napade, ki jih sponzorirajo države ali teroristične skupine;

69. priznava pomen prispevkov Europolovega in Eurojustovega Evropskega centra za kibernetsko kriminaliteto (EC3) ter agencije ENISA, v boju proti kibernetskemu kriminalu;

70. poziva Europol, naj nacionalne organe kazenskega pregona podpre pri vzpostavitvi varnih in primernih kanalov prenosa;

71. obžaluje, da trenutno ni standardov EU na področju usposabljanja in certificiranja; priznava, da bodo prihodnji trendi v kibernetski kriminaliteti od strokovnjakov zahtevali vse višje strokovno znanje; pozdravlja dejstvo, da obstoječe pobude, kot so evropska skupina za usposabljanje in izobraževanje na področju kibernetske kriminalitete, projekt usposabljanja izvajalcev izobraževanja in dejavnosti usposabljanja v okviru cikla EU politike že začenjajo obravnavati vrzeli v strokovnem znanju na ravni EU;

72. poziva Agencijo Evropske unije za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in Evropsko mrežo institucij za izobraževanje v pravosodju, naj ponudbo izobraževanj o temah, povezanih s kibernetskim kriminalom, razširijo na pristojne organe kazenskega pregona in pravosodne organe v vsej Uniji;

73. poudarja, da se je število kibernetskih kaznivih dejanj, o katerih je bil obveščen Eurojust, povečalo za 30 %; poziva, naj se Eurojustu dodelijo zadostna sredstva in po potrebi več delovnih mest, da bi bil kos vse večjemu obsegu dela, povezanemu s kibernetsko kriminaliteto, ter tudi naj se prek nedavno ustanovljene Evropske pravosodne mreže za kibernetsko kriminaliteto razvije in nadalje okrepi podpora nacionalnim tožilstvom za kibernetski kriminal v čezmejnih primerih;

74. poziva k reviziji mandata agencije ENISA ter okrepitvi nacionalnih agencij za kibernetsko varnost; poziva k okrepitvi agencije ENISA z vidika delovnih nalog, osebja in sredstev; poudarja, da bi moral njen novi mandat obsegati tudi tesnejše povezave z Europolom in zainteresiranimi stranmi v industriji, da bo bolje podpirala pristojne organe v boju proti kibernetski kriminaliteti;

75. poziva Agencijo Evropske unije za temeljne pravice, naj pripravi praktičen in podroben priročnik za države članice s smernicami za nadzor in kontrolo;

Izboljšano sodelovanje s tretjimi državami

76. poudarja pomen tesnega sodelovanja s tretjimi državami v svetovnem boju proti kibernetskemu kriminalu, tudi z izmenjavo dobre prakse, skupnimi preiskavami, krepitvijo zmogljivosti in medsebojno pravno pomočjo;

77. poziva države članice, ki tega še niso storile, naj ratificirajo in v celoti izvajajo konvencijo Sveta Evrope o kibernetski kriminaliteti z dne 23. novembra 2001 (Budimpeška konvencija) in njene dodatne protokole ter v sodelovanju z Evropsko komisijo v ustreznih mednarodnih forumih spodbujajo njeno uporabo;

78. opozarja na svoje resne pomisleke glede dela Odbora Sveta Evrope za konvencijo o kibernetski kriminaliteti v zvezi s tolmačenjem člena 32 Budimpeške konvencije o čezmejnem dostopu do shranjenih računalniških podatkov (dokazno gradivo v oblaku) in nasprotuje sklenitvi kakršnega koli dodatnega protokola ali smernic z namenom, da bi razširili področje uporabe te določbe in presegli veljavno ureditev, ki jo določa ta konvencija in ki že tako uvaja veliko izjemo od načela teritorialnosti, saj bi to lahko pripeljalo do neoviranega dostopa organov kazenskega pregona na daljavo do strežnikov in računalnikov v drugih jurisdikcijah, ne da bi pri tem spoštovali sporazume o medsebojni pravni pomoči in druge instrumente pravosodnega sodelovanja, ki obstajajo z namenom zagotavljanja temeljnih pravic posameznikov, vključno z varstvom podatkov in dolžnim pravnim postopanjem, zlasti s Konvencijo Sveta Evrope št. 108;

79. obžaluje, da ni zavezujočega mednarodnega prava s področja kibernetske kriminalitete, in poziva države članice in evropske institucije, naj si prizadevajo za sklenitev konvencije na tem področju;

80. poziva Komisijo, naj predlaga možne pobude za izboljšanje učinkovitosti in spodbujanje uporabe sporazumov o medsebojni pravni pomoči za preprečitev domnevne ekstrateritorialne pristojnosti tretjih držav;

81. poziva države članice, naj zagotovijo zadostne zmogljivosti za obdelavo zaprosil za medsebojno pravno pomoč v zvezi s preiskavami v kibernetskem prostoru in razvijejo ustrezne programe za usposabljanje osebja, ki je pristojno za obravnavo teh zaprosil;

82. poudarja, da sporazumi o strateškem in operativnem sodelovanju med Europolom in tretjimi državami omogočajo izmenjavo informacij in praktično sodelovanje;

83. ugotavlja, da se največje število zaprosil organov kazenskega pregona pošlje v Združene države in Kanado; je zaskrbljen, ker je stopnja razkritja velikih ponudnikov storitev ZDA v odgovor na zaprosila evropskih kazenskih sodnih organov nekaj manj kot 60 %, in opozarja, da so v skladu s Poglavjem V Splošne uredbe o varstvu podatkov sporazumi medsebojni pravni pomoči in drugi mednarodni sporazumi prednostni mehanizem za omogočanje dostopa do osebnih podatkov, shranjenih v tujini;

84. poziva Komisijo, naj predlaga konkretne ukrepe za zaščito temeljnih pravic osumljenih ali obtoženih oseb pri izmenjavi informacij med evropskimi organi kazenskega pregona in tretjimi državami, zlasti zaščitne ukrepe pri postopkih, ko se na podlagi sodnega sklepa od organov kazenskega pregona in/ali ponudnikov storitev hitro pridobijo pomembni dokazi, informacije o naročniku ter podrobni metapodatki in vsebinski podatki (če niso šifrirani), da bi se izboljšala medsebojna pravna pomoč;

85. poziva Komisijo, naj v sodelovanju z državami članicami, ustreznimi evropskimi organi in po potrebi tretjimi državami preuči nove načine za učinkovito zavarovanje in pridobivanje e-dokazov, ki jih gostujejo v tretjih državah, v popolni skladnosti s temeljnimi pravicami in zakonodajo EU o varstvu podatkov, s pospešitvijo in poenostavitvijo postopkov medsebojne pravne pomoči in, kjer je to primerno, vzajemnim priznavanjem;

86. poudarja pomembnost centra za odzivanje na kibernetske incidente pri zvezi Nato;

87. poziva vse države članice, naj sodelujejo v svetovnem forumu o kibernetskem strokovnem znanju, da bi omogočile vzpostavitev partnerstev za izgradnjo zmogljivosti;

88. podpira pomoč pri krepitvi zmogljivosti, ki jo EU nudi državam vzhodnega sosedstva, saj iz njih prihaja mnogo kibernetskih napadov;

o

o o

89. naroči svojemu predsedniku, naj to resolucijo posreduje Svetu in Komisiji.