4. traži od Komisije da podrži države članice u smanjivanju razlika u plaćama među spolovima za najmanje pet postotnih bodova godišnje u cilju uklanjanja razlika u plaćama među spolovima do 2020.;

5. prepoznaje da višeslojan, višedimenzionalan pristup traži od Komisije da podrži države članice u promicanju dobrih praksi i provođenju politika za rješavanje razlika u plaćama među spolovima;

6. poziva Komisiju da bez odlaganja revidira Direktivu 2006/54/EZ te da predloži njezine izmjene u skladu s člankom 32. Direktive i na temelju članka 157. UFEU-a, na osnovi detaljnih preporuka iz priloga Rezoluciji Parlamenta od 24. svibnja 2012.;

7. nalaže svojem predsjedniku da ovu Rezoluciju proslijedi Vijeću, Komisiji te vladama država članica.

P7_TA(2013)0376

Strategija za kibernetičku sigurnost u EU-u: otvoren i siguran kibernetički prostor

Rezolucija Europskog parlamenta od 12. rujna 2013. o Strategiji Europske unije za kibernetičku sigurnost: otvoren, siguran i zaštićen kibernetički prostor (2013/2606(RSP))

(2016/C 093/16)

Europski parlament,

— uzimajući u obzir zajedničku komunikaciju Europske komisije i Visoke predstavnice Europske unije za vanjske poslove i sigurnosnu politiku od 7. veljače 2013. naslovljenu „Strategija Europske unije za kibernetičku sigurnost: otvoren, siguran i zaštićen kibernetički prostor” (JOIN(2013)0001),

— uzimajući u obzir prijedlog direktive Komisije od 7. veljače 2013. o mjerama za osiguravanje visoke zajedničke razine mrežne i informacijske sigurnosti u cijeloj Uniji (COM(2013)0048),

— uzimajući u obzir Komunikaciju Komisije od 19. svibnja 2010. naslovljenu „Digitalni program za Europu” (COM(2010) 0245) i Komunikaciju Komisije od 18. prosinca 2012. naslovljenu „Digitalni program za Europu – digitalni poticaji za europski rast” (COM(2012)0784),

— uzimajući u obzir Komunikaciju Komisije od 27. rujna 2012. naslovljenu „Ostvarivanje potencijala računalstva u oblaku u Europi” (COM(2012)0529),

— uzimajući u obzir Komunikaciju Komisije od 28. ožujka 2012. naslovljenu „Suočavanje s kriminalom u našem digitalnom dobu: uspostavljanje Europskog centra za kibernetički kriminal” (COM(2012)0140) i Zaključke Vijeća od 7. lipnja 2012. o tome,

— uzimajući u obzir Direktivu 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i kojom se zamjenjuje Okvirna odluka Vijeća 2005/222/PUP ([1]),

— uzimajući u obzir Direktivu Vijeća 2008/114/EZ od 8. prosinca 2008 o utvrđivanju i označivanju europske kritične infrastrukture i procjeni potrebe poboljšanja njezine zaštite ([2]),

---

([1]) SL L 218, 14.8.2013., str. 8.
([2]) SL L 345, 23.12.2008., str. 75.

— uzimajući u obzir Direktivu 2011/92/EU Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece te dječje pornografije, kojom se zamjenjuje Okvirna odluka Vijeća 2004/68/PUP ([1]),

— uzimajući u obzir Štokholmski program ([2]), Komunikaciju Komisije „Ostvarivanje područja slobode, sigurnosti i pravde za građane Europe – akcijski plan za provedbu Štokholmskog programa" (COM(2010)0171) i Komunikaciju Komisije „Strategija unutarnje sigurnosti EU-a u akciji: pet koraka prema sigurnijoj Europi" (COM(2010)0673) te svoju Rezoluciju od 22. svibnja 2012. o strategiji unutarnje sigurnosti Europske unije ([3]),

— uzimajući u obzir Zajednički prijedlog Komisije i Visoke predstavnice za odluku Vijeća o mjerama Unije za provedbu klauzule o solidarnosti (JOIN(2012)039),

— uzimajući u obzir Okvirnu odluku Vijeća 2001/413/PUP od 28. svibnja 2001. o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja ([4]),

— uzimajući u obzir svoju Rezoluciju od 12. lipnja 2012. o zaštiti kritične informacijske infrastrukture – postignuća i sljedeći koraci: prema globalnoj kibernetičkoj sigurnosti ([5]) i Zaključke Vijeća od 27. svibnja 2011. o Komunikaciji Komisije naslovljenoj „Zaštita kritične informacijske infrastrukture – postignuća i sljedeći koraci: prema globalnoj kibernetičkoj sigurnosti" (COM(2011)0163),

— uzimajući u obzir svoju Rezoluciju od 11. prosinca 2012. o ostvarenju jedinstvenog digitalnog tržišta ([6]),

— uzimajući u obzir svoju Rezoluciju od 22. studenog 2012. o kibernetičkoj sigurnosti i obrani ([7]),

— uzimajući u obzir svoje stajalište u prvom čitanju od 16. travnja 2013. o prijedlogu uredbe Europskog parlamenta i Vijeća o Europskoj agenciji za sigurnost mreža i podataka (ENISA) (COM(2010)0521) ([8]),

— uzimajući u obzir svoju Rezoluciju od 11. prosinca 2012. o strategiji digitalne slobode u vanjskoj politici EU-a ([9]),

— uzimajući u obzir Konvenciju Vijeća Europe o kibernetičkom kriminalu od 23. studenog 2001.,

— uzimajući u obzir međunarodne obveze Unije, posebno one u sklopu Općeg sporazuma o trgovini uslugama (GATS),

— uzimajući u obzir članak 16. Ugovora o funkcioniranju Europske unije (UFEU) i Povelju Europske unije o temeljnim pravima, posebno njezine članke 6., 8. i 11.,

— uzimajući u obzir aktualne pregovore o partnerstvu za transatlantsku trgovinu i ulaganja između Europske unije i Sjedinjenih Američkih Država,

— uzimajući u obzir članak 110. stavak 2. Poslovnika,

A. budući da sve veći izazovi u kibernetičkom prostoru u obliku sve složenijih prijetnji i napada predstavljaju veliku opasnost sigurnosti, stabilnosti i gospodarskom blagostanju država članica te privatnom sektoru i široj zajednici; budući da će zaštita našega društva i gospodarstva stoga biti izazov koji se stalno mijenja;

([1]) SL L 335, 17.12.2011., str. 1.
([2]) SL C 115, 4.5.2010., str. 1.
([3]) Usvojeni tekstovi, P7_TA(2012)0207.
([4]) SL L 149, 2.6.2001., str. 1.
([5]) Usvojeni tekstovi, P7_TA(2012)0237.
([6]) Usvojeni tekstovi, P7_TA(2012)0468.
([7]) Usvojeni tekstovi, P7_TA(2012)0457.
([8]) Usvojeni tekstovi, P7_TA(2013)0103.
([9]) Usvojeni tekstovi, P7_TA(2012)0470.

B. budući da kibernetički prostor i kibernetička sigurnost trebaju biti jedan od strateških stupova sigurnosne i obrambene politike EU-a i svake države članice; budući da je od presudne važnosti jamčiti da kibernetički prostor ostane otvoren za slobodan protok ideja i informacija i za slobodno izražavanje;

C. budući da su elektronička trgovina i internetske usluge vitalna snaga interneta i da su ključne za ciljeve strategije Europa 2020., pri čemu će koristi imati i građani i privatni sektor; budući da Unija mora u potpunosti ostvariti potencijal i prilike koje internet predstavlja za daljnji razvoj jedinstvenog tržišta, uključujući jedinstveno digitalno tržište;

D. budući da strateški prioriteti izneseni u zajedničkoj komunikaciji o strategiji Europske unije za kibernetičku sigurnost obuhvaćaju postizanje kibernetičke otpornosti, smanjenje stope kibernetičkog kriminala, razvijanje politike za kibernetičku obranu i kibernetičkih mogućnosti povezanih sa zajedničkom sigurnosnom i obrambenom politikom (ZSOP) i uspostavljanje usklađene međunarodne politike kibernetičkog prostora u EU-u;

E. budući da su mrežni i informacijski sustavi diljem Unije iznimno međusobno povezani; budući da, s obzirom na globalnu narav interneta, mnogi izgredi u mrežnoj i informacijskoj sigurnosti nadilaze nacionalne granice i imaju potencijal da dovedu u pitanje funkcioniranje unutarnjeg tržišta i povjerenje potrošača u jedinstveno digitalno tržište;

F. budući da je kibernetička sigurnost diljem Unije, kao i u ostatku svijeta, snažna samo onoliko koliko i njezina najslabija karika i da poremećaji u jednom sektoru ili jednoj državi članici utječu na drugi sektor ili državu članicu, čime se stvaraju učinci prelijevanja s posljedicama za gospodarstvo Unije u cjelini;

G. budući da je do travnja 2013. samo 13 država članica službeno usvojilo nacionalne strategije za kibernetičku sigurnost; budući da i dalje postoje temeljne razlike među državama članicama kad je riječ o njihovoj pripremljenosti, sigurnosti, strateškoj kulturi i sposobnosti da razvijaju i provode nacionalne strategije za kibernetičku sigurnost te budući da treba izvršiti procjenu tih razlika;

H. budući da različite sigurnosne kulture i nedostatak pravnog okvira dovode do fragmentacije te da su od primarne važnosti na jedinstvenom digitalnom tržištu; budući da nedostatak usklađenog pristupa kibernetičkoj sigurnosti za sobom povlači ozbiljne rizike za gospodarsko blagostanje i sigurnost transakcija te budući da su zajednički napori i uža suradnja stoga nužni među vladama, u privatnom sektoru, među tijelima koja provode zakone i obavještajnim službama;

I. budući da je kibernetički kriminal sve skuplji međunarodni problem koji, prema Uredu UN-a za drogu i kriminal, globalnu ekonomiju trenutačno stoji 295 milijardi EUR godišnje;

J. budući da međunarodni organizirani kriminal, iskorištavajući tehnološke prednosti, nastavlja prebacivati svoj operativni teren u kibernetički prostor, pri čemu kibernetički kriminal radikalno mijenja tradicionalni ustroj skupina organiziranog kriminala; budući da je to dovelo do činjenice da je organizirani kriminal manje lokaliziran i veća je vjerojatnost da će se on koristiti teritorijalnošću i različitošću nacionalnih pravnih nadležnosti na globalnoj razini;

K. budući da brojne prepreke nadležnim tijelima još uvijek otežavaju istraživanje kibernetičkog kriminala, među njima uporaba „virtualnih valuta”, koje se mogu upotrebljavati za pranje novca, u transakcijama na kibernetičkom prostoru, pitanja teritorijalnosti i granica nadležnosti, nedovoljne mogućnosti razmjene obavještajnih podataka, manjak izobraženog osoblja i nedosljedna suradnja s drugim zainteresiranim stranama;

L. budući da je tehnologija temelj za razvoj kibernetičkog prostora i da je neprekidna prilagodba tehnološkim promjenama presudna ako se želi unaprijediti otpornost i sigurnost kibernetičkog prostora EU-a; budući da se moraju poduzeti mjere kako bi se zajamčilo da zakonodavstvo bude usklađeno s novim tehnološkim događanjima, čime se omogućuju djelotvorna identifikacija i kazneni progon kibernetičkih kriminalaca te zaštita žrtava kibernetičkog kriminala; budući

da strategija za kibernetičku sigurnost EU-a mora uključivati mjere usmjerene na osviještenost, obrazovanje, razvoj interventnih timova za kibernetičke krize, razvoj unutarnjeg tržišta proizvoda i usluga na području kibernetičke sigurnosti te promicanje ulaganja u istraživanje, razvoj i inovacije;

1. pozdravlja zajedničku komunikaciju o strategiji Europske unije za kibernetičku sigurnost i prijedlog direktive o mjerama kojima se jamči visoka razina sigurnosti mreža i podataka diljem Unije;

2. ističe iznimnu i sve veću važnost koju internet i kibernetički prostor imaju za političke, gospodarske i društvene transakcije, ne samo u Uniji već i u odnosu na druge aktere u svijetu;

3. ističe da je potrebno razviti stratešku komunikacijsku politiku o kibernetičkoj sigurnosti u EU-u, kriznim kibernetičkim situacijama, revizijama strategije, javno-privatnoj suradnji i upozorenjima te preporukama javnosti;

4. podsjeća da je visoka razina sigurnosti mreža i podataka potrebna ne samo radi održavanja usluga koje su nužne za neometano funkcioniranje društva i gospodarstva, već i radi očuvanja fizičkog integriteta građana povećanjem učinkovitosti, djelotvornosti i sigurnog funkcioniranja kritične infrastrukture; ističe da je, uz sigurnost mreža i podataka, čemu se mora posvetiti pozornost, važno pitanje i unapređenje fizičke sigurnosti; naglašava da infrastruktura treba biti otporna i na namjerne i na nenamjerne poremećaje; ističe da se, u tom smislu, u sklopu strategije za kibernetičku sigurnost veći naglasak treba staviti na uobičajene uzroke nenamjernih kvarova u sustavima;

5. ponavlja svoj poziv državama članicama da usvoje nacionalne strategije za kibernetičku sigurnost kojima se obuhvaćaju tehnički, koordinacijski i kadrovski aspekti te aspekti financijske dodjele i koje uključuju jasna pravila o koristima za privatni sektor i njegovim odgovornostima kako bi se jamčilo njihovo sudjelovanje, bez neopravdane odgode, i kako bi se osigurali sveobuhvatni postupci upravljanja rizikom te kako bi se očuvalo regulatorno okruženje;

6. primjećuje da će se samo kombiniranim vodstvom i političkim vlasništvom institucija Unije i država članica omogućiti visoka razina sigurnosti mreža i podataka diljem Unije i tako doprinijeti sigurnom i neometanom funkcioniranju jedinstvenog tržišta;

7. ističe da se u sklopu politike Unije o kibernetičkoj sigurnosti treba omogućiti sigurno i pouzdano digitalno okruženje zasnovano na zaštiti i očuvanju sloboda i poštovanju temeljnih internetskih prava, i oblikovano tako da ih jamči, kako su utvrđena u Povelji EU-a i članku 16. UFEU-a, posebno prava na privatnost i zaštitu podataka; vjeruje da posebnu pozornost treba posvetiti zaštiti djece na internetu;

8. poziva države članice i Komisiju da poduzmu sve potrebne mjere da organiziraju programe izobrazbe namijenjene promicanju i povećanju razine osviještenosti, vještina i odgoja među europskim građanima, posebno s obzirom na osobnu sigurnost kao dio nastavnog plana digitalne pismenosti od rane dobi; pozdravlja inicijativu da se organizira Europski mjesec kibernetičke sigurnosti uz podršku ENISA-e i u suradnji s tijelima javne vlasti i privatnim sektorom kako bi se podigla razina osviještenosti o izazovima obuhvaćenima zaštitom sustava mreža i podataka;

9. smatra da obrazovanje o kibernetičkoj sigurnosti povećava razinu osviještenosti europskog društva o kibernetičkim prijetnjama, čime se potiče odgovorna uporaba kibernetičkog prostora i pomaže povećanje riznice objedinjenih kibernetičkih vještina; prepoznaje glavnu ulogu Europola i njegova novog Europskog centra za kibernetički kriminal (EC3) kao i ENISA-e i Eurojust-a u pružanju aktivnosti izobrazbe na razini EU-a o uporabi međunarodnih instrumenata za pravosudnu suradnju i provedbi zakona povezanima s različitim aspektima kibernetičkog kriminala;

10. ponavlja potrebu da se pružaju tehnički savjeti i pravne informacije te da se uspostave programi o sprečavanju i suzbijanju kibernetičkog kriminala; potiče izobrazbu inženjera kibernetičke tehnologije specijaliziranih za zaštitu kritične infrastrukture i sustava podataka kao i operatera sustava za nadzor prijenosa i centara za upravljanje prometom; ističe krajnju potrebu za uvođenjem redovnih programa izobrazbe o kibernetičkoj sigurnosti za osoblje na svim razinama u javnom sektoru;

11. ponavlja svoj poziv na oprez pri primjeni ograničenja na sposobnost građana da se koriste instrumentima komunikacijske i informacijske tehnologije te ističe da države članice trebaju nastojati da nikad ne ugroze prava i slobode građana pri osmišljanju odgovora na kibernetičke prijetnje i napade i da trebaju imati odgovarajuća zakonodavna sredstva za razlikovanje kibernetičkih izgreda na civilnoj od onih na vojnoj razini;

12. smatra da regulatorno uključivanje u područje kibernetičke sigurnosti treba biti upućeno na rizike i usmjereno na kritičnu infrastrukturu čije je ispravno funkcioniranje od velikog javnog interesa te da se treba oslanjati na postojeće napore industrije utemeljene na tržištu kako bi se osigurala otpornost mreža; naglašava presudnu ulogu suradnje na operativnoj razini pri poticanju učinkovitije razmjene informacija o kibernetičkim prijetnjama između tijela javnih vlasti i privatnog sektora, na razini Unije i na nacionalnoj razini te sa strateškim partnerima Unije, s ciljem jamčenja sigurnosti mreža i podataka stvaranjem uzajamnog povjerenja, vrijednosti i predanosti i razmjenom stručnog znanja; smatra da se javno-privatna partnerstva trebaju zasnivati na mrežnoj i tehnološkoj neutralnosti i da trebaju biti usmjerena na napore za rješavanje problema koji imaju velik učinak na javnost; poziva Komisiju da potiče sve uključene tržišne subjekte da budu oprezniji i spremniji za suradnju kako bi druge subjekte zaštitili od štete njihovim uslugama;

13. priznaje da je otkrivanje izgreda u kibernetičkoj sigurnosti i obavještavanje o njima iznimno važno za promicanje kibernetičke otpornosti u Uniji; vjeruje da treba uvesti zahtjeve za razmjerno i nužno razotkrivanje kako bi se dopustilo obavještavanje nadležnih nacionalnih tijela o izgredima u kojima dolazi do znatnih povreda sigurnosti i time omogućilo poboljšano praćenje izgreda kibernetičkog kriminala i olakšali napori za podizanje razine osviještenosti na svim razinama;

14. potiče Komisiju i druge aktere da uvedu politiku o kibernetičkoj sigurnosti i kibernetičkoj otpornosti koja obuhvaća gospodarske poticaje za promicanje visokih razina kibernetičke sigurnosti i kibernetičke otpornosti;

Kibernetička otpornost

15. primjećuje da različiti sektori i države članice posjeduju različite razine sposobnosti i vještina te da to sprečava razvoj pouzdane suradnje i potkopava funkcioniranje jedinstvenog tržišta;

16. smatra da bi se zahtjevi za mala i srednja poduzeća trebali temeljiti na proporcionalnom pristupu utemeljenom na riziku;

17. inzistira na razvoju kibernetičke otpornosti kritične infrastrukture te podsjeća na to da bi u okviru predstojećih mehanizama primjene klauzule o solidarnosti (članak 222. UFEU-a) trebalo uzeti u obzir rizik od kibernetičkih napada na države članice; poziva Komisiju i visoku predstavnicu da taj rizik uzmu u obzir u svojim zajedničkim izvješćima o cjelovitoj procjeni prijetnji i rizika koja će se objavljivati od 2015.;

18. naglašava da za potrebe jamčenja cjelovitosti, dostupnosti i povjerljivosti posebno važnih usluga utvrđivanje i kategorizacija kritične infrastrukture moraju biti ažurirani te moraju biti utvrđeni nužni minimalni sigurnosni uvjeti za njihove sustave mreža i podataka;

19. priznaje da se prijedlogom direktive o mjerama za jamčenje zajedničke visoke razine sigurnosti mreža i podataka diljem Unije predviđaju ti minimalni sigurnosni uvjeti za pružatelje usluga informacijskog društva i voditelje kritične infrastrukture;

20. poziva države članice i Uniju da uspostave odgovarajuće okvire za sustave brze, dvosmjerne razmjene informacija kojima će se osigurati anonimnost privatnog sektora i stalno ažurirati javni sektor te da po potrebi pružaju pomoć privatnom sektoru;

21. pozdravlja zamisao Komisije o stvaranju kulture upravljanja rizikom u pogledu kibernetičke sigurnosti te poziva države članice i institucije Unije da u svoje planove upravljanja kriznim situacijama i analize rizika brzo uvrste upravljanje kibernetičkim krizama; nadalje poziva vlade država članica i Komisiju da potiču sudionike u privatnom sektoru da u svoje planove upravljanja i analize rizika uključe upravljanje kibernetičkim krizama te da obuče svoje osoblje za kibernetičku sigurnost;

22. poziva sve države članice i institucije Unije da uspostave mrežu funkcionalnih interventnih timova za informatičke krize koji će raditi 24 sata dnevno sedam dana u tjednu; naglašava da bi nacionalni interventni timovi za informatičke krize trebali biti dio učinkovite mreže u kojoj se razmjenjuju relevantne informacije u skladu s potrebnim standardima povjerenja i povjerljivosti; primjećuje da okvirne inicijative, u okviru kojih se ti timovi i druga relevantna sigurnosna tijela spajaju, predstavljaju korisno sredstvo u razvoju povjerenja u prekograničnom i međusektorskom kontekstu; prepoznaje važnost učinkovite i djelotvorne suradnje između tih interventnih timova i policijskih i pravosudnih tijela u borbi protiv kibernetičkog kriminala;

23. podržava ENISA-u u obavljanju njezinih dužnosti na području sigurnosti mreža i podataka, a posebno pružanjem smjernica i savjetovanjem država članica te podržavanjem razmjene najboljih praksi i razvoja okružja u kojemu vlada povjerenje;

24. naglašava potrebu da se u toj gospodarskoj grani primijene odgovarajući uvjeti kibernetičke sigurnosti u cijelom lancu vrijednosti proizvoda IKT-a koji se koriste u prometnim mrežama i informacijskim sustavima, da se primjenjuje odgovarajuće upravljanje rizicima, da se usvoje sigurnosni standardi i rješenja te da se razviju najbolje prakse i razmjena informacija kako bi se osigurali kibernetički sigurni prometni sustavi;

Industrijski i tehnološki resursi

25. smatra da osiguravanje visoke razine sigurnosti mreža i podataka ima središnju ulogu u jačanju konkurentnosti i dobavljača i korisnika sigurnosnih rješenja u Uniji; smatra da su, dok grana informacijsko-tehnološke sigurnosti u Uniji ima važan neiskorišten potencijal, privatni, javni i poslovni korisnici često neinformirani o troškovima i koristima ulaganja u kibernetičku sigurnost te da stoga ostaju ranjivi u slučaju štetnih kibernetičkih prijetnji; naglašava da je u tom pogledu primjena interventnih timova za informatičke krize relevantan čimbenik;

26. vjeruje da bogata ponuda rješenja na području kibernetičke sigurnosti i potražnja za njima zahtijeva od nacionalnih tijela uključenih u pitanja IKT-a odgovarajuća ulaganja u akademske resurse, istraživanje i razvoj te razvijanje znanja i izgradnju kapaciteta kako bi se potaknule inovacije i razvila dostatna svijest o rizicima za sigurnost mreža i podataka, što vodi stvaranju usklađene europske grane sigurnosti;

27. poziva institucije Unije i države članice da poduzmu potrebne mjere za uspostavu „jedinstvenog tržišta za kibernetičku sigurnost" na kojemu korisnici i dobavljači mogu najbolje iskoristiti inovacije, sinergije i kombinirano stručno znanje o ponudi te koje omogućuje sudjelovanje malih i srednjih poduzeća;

28. potiče države članice da razmotre zajednička ulaganja u europsku gospodarsku granu kibernetičke sigurnosti na vrlo sličan način na koji je to učinjeno u drugim gospodarskim granama, kao što je zrakoplovni sektor;

Kibernetički kriminal

29. smatra da kriminalne aktivnosti u kibernetičkom prostoru mogu biti jednako štetne za društva kao i prekršaji u fizičkom svijetu te da se ti oblici kriminala često uzajamno jačaju, kao što se, na primjer, može uočiti na području seksualnog iskorištavanja djece te organiziranog kriminala i pranja novca;

30. primjećuje da u nekim slučajevima postoji veza između zakonitih i nezakonitih poslovnih aktivnosti; naglašava važnost veze između financiranja terorizma i ozbiljnog organiziranog kriminala, koju olakšava internet; naglašava da javnost mora postati svjesna ozbiljnosti uplitanja u kibernetički kriminal te mogućnosti da ono što se na prvi pogled može učiniti „društveno prihvatljivim" kriminalom, kao što je nezakonito preuzimanje filmova, često donosi velike količine novca međunarodnim kriminalnim udrugama;

31. slaže se s Komisijom da se iste norme i načela primjenjuju izvan mreže i na mreži te da zbog toga borbu protiv kibernetičkog kriminala treba intenzivirati suvremenim zakonodavstvom i operativnim sposobnostima;

32. zauzima stajalište da su, s obzirom na prekograničnu prirodu kibernetičkog kriminala, zajednički napori i stručno znanje koji se nude na razini Unije, iznad razine pojedinačnih država članica, posebno važni i da se zbog toga Eurojustu, Europolovom Europskom centru za kibernetički kriminal, interventnim timovima za informatičke krize te sveučilištima i istraživačkim centrima moraju osigurati odgovarajuća sredstva i mogućnosti da valjano funkcioniraju kao središta stručnog znanja, suradnje i razmjene informacija;

33. snažno pozdravlja uspostavu Europskog centra za kibernetički kriminal te podržava budući razvoj te agencije i njezine vitalne uloge u koordiniranju pravovremene i učinkovite prekogranične razmjene informacija i stručnog znanja radi potpore sprečavanju, otkrivanju i istrazi kibernetičkog kriminala;

34. poziva države članice da građanima osiguraju jednostavan pristup informacijama o kibernetičkim prijetnjama i načinima borbe protiv njih; vjeruje da bi takve smjernice trebale sadržavati informacije o tome kako korisnici mogu zaštiti svoju privatnost na internetu, otkrivati i prijavljivati slučajeve navođenja djece na seksualne aktivnosti, instalirati programe i vatrozid, upravljati lozinkama te otkrivati slučajeve lažnog predstavljanja („phishing”) i mamljenja („pharming”) te druge napade;

35. ustraje u tome da bi države članice koje još nisu ratificirale budimpeštansku Konvenciju Vijeća Europe o kibernetičkom kriminalu trebale to učiniti bez nepotrebnog odgađanja; pozdravlja razmišljanja Vijeća Europe o potrebi ažuriranja te Konvencije u svjetlu tehnološkog razvoja kako bi se i dalje osigurala njezina učinkovitost u rješavanju pitanja kibernetičkog kriminala te poziva Komisiju i države članice da sudjeluju u toj debati; potiče napore na promicanju ratifikacije Konvencije među drugim zemljama i poziva Komisiju na njezino aktivno promicanje izvan Unije;

Kibernetička obrana

36. naglašava da kibernetički izazovi, prijetnje i napadi ugrožavaju interese država članica na područjima obrane i nacionalne sigurnosti te da bi civilni i vojni pristup zaštiti kritične infrastrukture, naporima na stvaranju sinergija, trebao maksimalno povećati korist za oba navedena područja;

37. zbog toga poziva države članice da pojačaju suradnju s Europskom obrambenom agencijom u cilju izrade prijedloga i inicijativa za mogućnosti kibernetičke obrane, oslanjajući se na novije inicijative i projekte; naglašava potrebu jačanja istraživanja i razvoja, između ostalog udruživanjem i razmjenom resursa;

38. ponovno naglašava da bi se u okviru sveobuhvatne strategije za kibernetičku sigurnost EU-a trebala uzeti u obzir dodana vrijednost postojećih agencija i tijela, kao i dobre prakse prikupljene od onih država članica koje su već uvele vlastite nacionalne strategije za kibernetičku sigurnost;

39. poziva potpredsjednicu/visoku predstavnicu da uvrsti upravljanje kibernetičkim krizama u planiranje kriznog upravljanja te naglašava potrebu da države članice u suradnji s Europskom obrambenom agencijom razviju planove zaštite misija i operacija ZSOP-a od kibernetičkih napada; poziva ih da uspostave zajedničke europske snage za kibernetičku obranu;

40. naglašava dobru praktičnu suradnju s NATO-om na području kibernetičke sigurnosti i potrebu poboljšanja te suradnje, posebno užom suradnjom na područjima planiranja, tehnologije, obuke i opreme;

41. poziva Uniju da uloži napore za uspostavljanje razmjene s međunarodnim partnerima, uključujući NATO, utvrđivanje područja suradnje te kad god je moguće izbjegavanje udvostručavanja aktivnosti i njihovo dopunjavanje;

Međunarodna politika

42. vjeruje da međunarodna suradnja i dijalog imaju važnu ulogu u stvaranju povjerenja i transparentnosti te promicanju visoke razine umrežavanja i razmjene informacija na svjetskoj razini; zbog toga poziva Komisiju i Europsku službu za vanjsko djelovanje da osnuju ekipu za kibernetičku diplomaciju čije bi odgovornosti obuhvaćale promicanje dijaloga sa zemljama i organizacijama istomišljenicama; poziva na aktivnije sudjelovanje EU-a u nizu međunarodnih konferencija na visokoj razini o kibernetičkoj sigurnosti;

43. smatra da je potrebno uspostaviti ravnotežu između konkurentnih ciljeva prekograničnog prijenosa podataka, zaštite podataka i kibernetičke sigurnosti u skladu s međunarodnim obvezama Unije, posebno u okviru GATS-a;

44. poziva potpredsjednicu/visoku predstavnicu da uvrsti pitanje kibernetičke sigurnosti u vanjsko djelovanje EU-a, posebno u odnosu na treće zemlje, kako bi se pojačala suradnja i razmjena iskustava i informacija o načinima rješavanja pitanja kibernetičke sigurnosti;

45. poziva Uniju da uloži napore kako bi se uključila u razmjenu s međunarodnim partnerima radi utvrđivanja područja suradnje, izbjegavajući udvostručavanje aktivnosti i osiguravajući njihovo dopunjavanje kad je to moguće; poziva potpredsjednicu/visoku predstavnicu i Komisiju da budu proaktivni u međunarodnim organizacijama te da koordiniraju stajališta država članica o načinima učinkovitog promicanja rješenja i politika na području kibernetike;

46. smatra da bi trebalo nastojati osigurati primjenu postojećih međunarodnih pravnih instrumenata u kibernetičkom prostoru, a posebno Konvencije Vijeća Europe o kibernetičkom kriminalu; zbog toga smatra da trenutno ne postoji potreba za novim pravnim instrumentima na međunarodnoj razini; međutim pozdravlja međunarodnu suradnju u razvijanju normi ponašanja u kibernetičkom prostoru, podržavajući vladavinu prava u kibernetičkom prostoru; smatra da bi trebalo razmotriti ažuriranje postojećih pravnih instrumenata kako bi se njima odrazio tehnološki napredak; smatra da pitanja nadležnosti zahtijevaju temeljitu raspravu o pravosudnoj suradnji i kaznenom gonjenju u slučaju transnacionalnih kaznenih djela;

47. smatra da bi posebno radna skupina EU-a i SAD-a za kibernetičku sigurnost i kibernetički kriminal mogla služiti kao sredstvo EU-a i SAD-a za razmjenu najboljih praksi na području politika kibernetičke sigurnosti kad god je to prikladno; u tom kontekstu primjećuje da će područja povezana s kibernetičkom sigurnošću, kao što su usluge koje ovise o sigurnom funkcioniranju mrežnih i informacijskih sustava, biti uključena u predstojeće pregovore o partnerstvu za transatlantsku trgovinu i ulaganja, koji trebaju biti zaključeni tako da štite suverenost EU-a i neovisnost njegovih institucija;

48. primjećuje da vještine na području kibernetičke sigurnosti i sposobnost sprečavanja, otkrivanja i učinkovitog suzbijanja prijetnji i zlonamjernih napada nisu jednako razvijeni u cijelom svijetu; naglašava da se napori za jačanje kibernetičke otpornosti i borbu protiv kibernetičkih prijetnji ne smiju ograničiti na partnere istomišljenike, nego bi trebali obuhvatiti i regije sa slabije razvijenim kapacitetima, tehničkom infrastrukturom i pravnim okvirima; vjeruje da koordinacija interventnih timova za informatičke krize ima presudan značaj na tom području; poziva Komisiju da, koristeći odgovarajuća sredstva, olakša nastojanja trećih strana da razviju vlastite sposobnosti na području kibernetičke sigurnosti te da im po potrebi u tome pomogne;

Provedba

49. poziva na redovita ocjenjivanja učinkovitosti nacionalnih strategija za kibernetičku sigurnost na najvišoj političkoj razini kako bi se osigurala prilagodba novim globalnim prijetnjama te zajamčila jednaka razina kibernetičke sigurnosti u različitim državama članicama;

50. traži od Komisije da izradi jasan plan kojim se utvrđuju rokovi za ostvarivanje ciljeva na razini Unije u okviru strategije za kibernetičku sigurnost te za njihovu prosudbu; poziva države članice da se dogovore o sličnom planu provedbe nacionalnih aktivnosti u okviru te strategije;

51. traži redovita izvješća Komisije, država članica, Europola, novoosnovanog Europskog centra za kibernetički kriminal, Eurojusta i ENISA-e u kojima će se ocjenjivati napredak u ostvarivanju ciljeva utvrđenih strategijom za kibernetičku sigurnost, uključujući ključne pokazatelje uspješnosti kojima se mjeri napredak provedbe;

o

o o

52. nalaže svojem predsjedniku da ovu Rezoluciju proslijedi Vijeću, Komisiji, vladama i parlamentima država članica, Europolu, Eurojustu i Vijeću Europe.

P7_TA(2013)0377

Digitalni program za rast, mobilnost i zapošljavanje

Rezolucija Europskog parlamenta od 12. rujna 2013. o Digitalnom programu za rast, mobilnost i zapošljavanje: vrijeme je za prelazak u višu brzinu (2013/2593(RSP))

(2016/C 093/17)

Europski parlament,

— uzimajući u obzir Komunikaciju Komisije od 18. prosinca 2012. naslovljenu „Digitalni program za Europu – digitalno poticanje europskog rasta” (COM(2012)0784),

— uzimajući u obzir pitanja Komisiji i Vijeću o Digitalnom programu za rast, mobilnost i zapošljavanje: vrijeme je za prelazak u višu brzinu (O-000085 – B7-0219/2013 i O-000086 – B7-0220/2013),

— uzimajući u obzir Uredbu (EU) br. 531/2012 Europskog parlamenta i Vijeća od 13. lipnja 2012. o roamingu u javnim pokretnim komunikacijskim mrežama u Uniji ([1]),

— uzimajući u obzir Odluku br. 243/2012/EU Europskog parlamenta i Vijeća od 14. ožujka 2012. o uspostavljanju višegodišnjeg programa za politiku radiofrekvencijskog spektra ([2]),

— uzimajući u obzir pregovore o instrumentu za povezivanje Europe koji su u tijeku, a naročito izmijenjeni prijedlog Uredbe Europskog parlamenta i Vijeća o smjernicama za transeuropske telekomunikacijske mreže i stavljanju izvan snage Odluke br. 1336/97/EZ (COM(2013)0329),

— uzimajući u obzir svoju rezoluciju od 5. svibnja 2010. o „novom Digitalnom programu za Europu: 2015.eu” ([3]),

— uzimajući u obzir Komunikaciju Komisije od 27. rujna 2012. naslovljenu „Ostvarivanje potencijala računalstva u oblaku u Europi” (COM(2012)0529),

— uzimajući u obzir prijedlog Uredbe Europskog parlamenta i Vijeća od 25. siječnja 2012. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka (Opća uredba o zaštiti podataka) (COM(2012) 0011),

---

([1]) SL L 172, 30.6.2012., str. 10.
([2]) SL L 81, 21.3.2012., str. 7.
([3]) SL C 81 E, 15.3.2011., str. 45.