P7_TA(2013)0376

Strategija za kibernetsko varnost EU: odprt in varen kibernetski prostor

Resolucija Evropskega parlamenta z dne 12. septembra 2013 o strategiji Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor (2013/2606(RSP))

Evropski parlament,

– ob upoštevanju skupnega sporočila Evropske komisije in visoke predstavnice Evropske unije za zunanje zadeve in varnostno politiko z dne 7. februarja 2013 z naslovom "Strategija Evropske unije za kibernetsko varnost: odprt, varen in zanesljiv kibernetski prostor" (JOIN(2013)1),

– ob upoštevanju predloga Komisije z dne 7. februarja 2013 glede direktive o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji (COM(2013)0048),

– ob upoštevanju sporočil Komisije z dne 19. maja 2010 z naslovom "Evropska digitalna agenda" (COM(2010)0245) in z dne 18. decembra 2012 z naslovom "Evropska digitalna agenda – digitalne spodbude za evropsko rast" (COM(2012)0784),

– ob upoštevanju sporočila Komisije z dne 27. septembra 2012 z naslovom "Sprostitev potenciala računalništva v oblaku v Evropi" (COM(2012)0529),

– ob upoštevanju sporočila Komisije z dne 28. marca 2012 z naslovom "Boj proti kriminalu v digitalni dobi: ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti" (COM(2012)0140) in sklepov Sveta o tem sporočilu z dne 7. junija 2012,

– ob upoštevanju Direktive Evropskega parlamenta in Sveta 2013/40/EU z dne 12. avgusta 2013 o napadih na informacijske sisteme in razveljavitvi Okvirnega sklepa Sveta 2005/222/PNZ[1],

– ob upoštevanju Direktive Sveta 2008/114/ES z dne 8. decembra 2008 o ugotavljanju in določanju evropske ključne infrastrukture ter o oceni potrebe po izboljšanju njene zaščite[2],

– ob upoštevanju Direktive Evropskega parlamenta in Sveta 2011/92/EU z dne 13. decembra 2011 o boju proti spolni zlorabi in spolnemu izkoriščanju otrok in ter otroški pornografiji in nadomestitvi Okvirnega sklepa Sveta 2004/68/PNZ[3],

– ob upoštevanju stockholmskega programa za območje svobode, varnosti in pravice[4], sporočil Komisije z naslovom "Zagotavljanje območja svobode, varnosti in pravice za državljane Evrope – akcijski načrt izvajanja stockholmskega programa" (COM(2010)0171) in "Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi" (COM(2010)0673) ter svoje resolucije z dne 22. maja 2012 o strategiji notranje

---

1 UL L 218, 14.8.2013, str. 8.
2 UL L 345, 23.12.2008, str. 75.
3 UL L 335, 17.12.2011, str. 1.
4 UL C 115, 4.5.2010, str. 1.

varnosti Evropske unije[1],

– ob upoštevanju skupnega predloga Komisije in visoke predstavnice za sklep Sveta o načinu izvajanja solidarnostne klavzule s strani Unije (JOIN/2012/0039),

– ob upoštevanju Okvirnega sklepa Sveta 2001/413/PNZ z dne 28. maja 2001 o boju proti goljufijam in ponarejanju v zvezi z negotovinskimi plačilnimi sredstvi[2],

– ob upoštevanju svoje resolucije z dne 12. junija 2012 o zaščiti kritične informacijske infrastrukture – dosežki in naslednji koraki: h globalni kibernetski varnosti[3] in sklepov Sveta z dne 27. maja 2011 o sporočilu Komisije z naslovom "Zaščita kritične informacijske infrastrukture – dosežki in naslednji koraki: h globalni kibernetski varnosti" (COM(2011)0163),

– ob upoštevanju svoje resolucije z dne 11. decembra 2012 o dokončanju enotnega digitalnega trga[4],

– ob upoštevanju svoje resolucije z dne 22. novembra 2012 o kibernetski varnosti in obrambi[5],

– ob upoštevanju svoje zakonodajne resolucije z dne 16. aprila 2013 o predlogu uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA) (COM(2010)0521), pri čemer je zavzel stališče v prvi obravnavi[6],

– ob upoštevanju svoje resolucije z dne 11. decembra 2012 o strategiji digitalne svobode v zunanji politiki EU[7],

– ob upoštevanju Konvencije Sveta Evrope o kibernetski kriminaliteti z dne 23. novembra 2001,

– ob upoštevanju mednarodnih obveznosti Unije, zlasti v okviru Splošnega sporazuma o trgovini s storitvami (GATS),

– ob upoštevanju člena 16 Pogodbe o delovanju Evropske unije (PDEU) in Listine Evropske unije o temeljnih pravicah, zlasti členov 6, 8 in 11,

– ob upoštevanju pogajanj o čezatlantskem trgovinskem in naložbenem partnerstvu, ki potekajo med Evropsko unijo in Združenimi državami Amerike,

– ob upoštevanju člena 110(2) Poslovnika,

A. ker vse večji kibernetski izzivi v obliki čedalje naprednejših groženj in napadov v veliki meri ogrožajo varnost, stabilnost in gospodarsko blaginjo držav članic, pa tudi zasebnega sektorja in širše skupnosti; ker bo zaradi tega varovanje naše družbe in gospodarstva

---

1 Sprejeta besedila, P7_TA(2012)0207.
2 UL L 149, 2.6.2001, str. 1.
3 Sprejeta besedila, P7_TA(2012)0237.
4 Sprejeta besedila, P7_TA(2012)0468.
5 Sprejeta besedila, P7_TA(2012)0457.
6 Sprejeta besedila, P7_TA(2013)0103.
7 Sprejeta besedila, P7_TA(2012)0470.

nenehno razvijajoč se izziv;

B. ker bi morala kibernetski prostor in kibernetska varnost tvoriti enega strateških temeljev varnostne in obrambne politike EU in posameznih držav članic; ker je izjemno pomembno zagotoviti, da bo ostal kibernetski prostor odprt prostemu pretoku zamisli in informacij ter svobodnemu izražanju;

C. ker so elektronsko poslovanje in spletne storitve gonilna sila interneta in so izjemnega pomena za dosego ciljev strategije Evropa 2020, od njih pa imajo koristi tako državljani kot zasebni sektor; ker se mora Unija začeti v celoti zavedati potenciala in priložnosti, ki jih ponuja internet pri nadaljnjem razvoju enotnega trga, tudi digitalnega;

D. ker strateške prednostne naloge, navedene v skupnem sporočilu o strategiji kibernetske varnosti za Evropsko unijo, zajemajo doseganje kibernetske odpornosti, zmanjševanje kibernetske kriminalitete, oblikovanje politike za varovanje pred kibernetsko kriminaliteto in kibernetske zmogljivosti, povezane s skupno varnostno in obrambno politiko, pa tudi oblikovanje usklajene mednarodne kibernetske politike EU;

E. ker so omrežni in informacijski sistemi po vsej Uniji zelo prepleteni; ker zaradi svetovne narave interneta številni incidenti na področju varnosti omrežja in informacij presegajo nacionalne meje, sposobni pa so tudi spodkopati delovanje notranjega trga in zaupanje potrošnikov v enotni digitalni trg;

F. ker je kibernetska varnost v Uniji, enako kot povsod po svetu, le tako močna kot njen najšibkejši člen in ker motnje v enem sektorju ali državi članici vplivajo na druge sektorje oziroma države članice, ustvarjajo učinek prelitja in prinašajo posledice za gospodarstvo celotne Unije;

G. ker je do aprila 2013 le trinajst držav članic uradno sprejelo nacionalne strategije kibernetske varnosti; ker so med državami članicami še zmeraj velike razlike, ko gre za pripravljenost, varnost, strateško kulturo ter sposobnost razvoja in uvedbe nacionalnih strategij za kibernetsko varnost, in ker bi bilo te razlike oceniti;

H. ker so razlike v kulturi na področju varnosti in pomanjkanje pravnega okvira povzročili razdrobljenost enotnega digitalnega trga in jih je treba prednostno obravnavati; ker odsotnost usklajenega pristopa h kibernetski varnosti vključuje resno tveganje za gospodarsko blaginjo in varnost transakcij in ker so zaradi tega potrebna usklajena prizadevanja in tesnejše sodelovanje med vladami, zasebnim sektorjem, organi kazenskega pregona in obveščevalnimi agencijami;

I. ker postaja kibernetska kriminaliteta čedalje dražji mednarodni problem, ki po podatkih Urada Združenih narodov za droge in kriminal svetovno gospodarsko trenutno stane skoraj 295 milijard EUR letno;

J. ker mednarodni organizirani kriminal izkorišča tehnološke prednosti in svoje področje delovanja še naprej usmerja v kibernetski prostor, kibernetski kriminal pa korenito spreminja tradicionalno strukturo organiziranih zločinskih združb; ker je zaradi tega postal organizirani kriminal manj lokaliziran in se povečuje verjetnost, da bo izkoristil ozemeljsko omejenost in razlike v nacionalnih jurisdikcijah na svetovni ravni;

K. ker delo pristojnih organov pri preiskovanju kibernetske kriminalitete še zmeraj otežuje

več ovir, med drugim uporaba navideznih valut pri transakcijah v kibernetskem prostoru, s čimer je mogoče prati denar, vprašanje ozemeljskih meja in omejitev sodnih pristojnosti, nezadostna zmogljivost za izmenjavo podatkov obveščevalnih služb, pomanjkanje usposobljenega osebja in nedosledno sodelovanje z drugimi deležniki;

L. ker je tehnologija temelj razvoja kibernetskega prostora in je nenehno prilagajanje tehnoloških spremembam nujno, če želimo izboljšati odpornost in varnost kibernetskega prostora EU; ker je treba sprejeti ukrepe, s katerimi bi zagotovili, da bo zakonodaja ohranila korak s tehnološkim razvojem, ter omogočili učinkovito identifikacijo in pregon kibernetskih kriminalcev in zaščito žrtev kibernetske kriminalitete; ker mora strategija EU za kibernetsko varnost vključevati ukrepe, ki se osredotočajo na ozaveščanje, izobraževanje, oblikovanje skupin za odzivanje na računalniške grožnje (CERT), vzpostavitev notranjega trga za proizvode in storitve s področja kibernetske varnosti ter spodbujanje naložb v raziskave, razvoj in inovacije;

1. pozdravlja skupno sporočilo o strategiji Evropske unije za kibernetsko varnost in predlog direktive o ukrepih, s katerimi bi zagotovili visoko raven varnosti omrežij in informacij po vsej Uniji;

2. poudarja izjemno in čedalje večjo pomembnost interneta in kibernetskega prostora za politične, gospodarske in družbene transakcije, ne le v Uniji, temveč tudi v zvezi z drugimi akterji po vsem svetu;

3. poudarja, da je treba oblikovati strateško komunikacijsko politiko o kibernetski varnosti EU, kibernetskih kriznih dogodkih, strateških pregledih, sodelovanju med javnim in zasebnim sektorjem ter opozorilih in priporočilih za javnost;

4. spominja, da visoka raven varnosti omrežja in informacij ni potrebna le za vzdrževanje storitev, nujnih za nemoteno delovanje družbe in gospodarstva, pač pa tudi za varovanje fizične integritete državljanov z izboljševanjem učinkovitosti, uspešnosti in varnega delovanja kritične infrastrukture; poudarja, da je sicer treba obravnavati varnost omrežja in informacij, a je pomembno vprašanje tudi izboljševanje fizične varnosti; poudarja, da mora biti infrastruktura odporna na namerne in nenamerne motnje; v zvezi s tem meni, da bi morala strategija za kibernetsko varnost večji poudarek nameniti splošnim vzrokom nenamernih sistemskih izpadov;

5. ponovno poziva države članice, naj sprejmejo nacionalne strategije za kibernetsko varnost, ki bodo zajemale tehnične in koordinacijske vidike ter vidike kadrovskih virov in dodeljevanja sredstev, vsebovale pa tudi jasna pravila o prednostih za zasebni sektor in njegovih odgovornostih, da bi brez nepotrebnega odlašanja zagotovili njegovo sodelovanje, omogočili celovite postopke za upravljanje tveganja ter zaščitili regulativno okolje;

6. ugotavlja, da bosta le skupno vodstvo in politična predanost institucij Unije in držav članic omogočila visoko raven varnosti omrežja in informacij po vsej Uniji, s tem pa prispevala k varnemu in nemotenemu delovanju enotnega trga;

7. poudarja, da mora politika kibernetske varnosti Unije zagotoviti varno in zanesljivo digitalno okolje, ki bi bilo osnovano in oblikovano tako, da bi zagotavljalo varstvo in ohranjanje svoboščin ter spoštovanje temeljnih pravic v spletu, kakor je opredeljeno v Listini EU o temeljnih pravicah in členu 16 PDEU, zlasti ko gre za pravice do zasebnosti

in varstva podatkov; meni, da bi bilo treba posebno pozornost nameniti varstvu otrok v spletu;

8. poziva države članice in Komisijo, naj storijo vse, kar je potrebno, da bi pripravili programe usposabljanja, s katerimi bi v okviru programa digitalne pismenosti že od zgornje starosti ozaveščali, usposabljali in izobraževali evropske državljane, zlasti na področju osebne varnosti; pozdravlja pobudo o organizaciji evropskega mesca kibernetske varnosti, pri čemer bi s podporo agencije ENISA in v sodelovanju z javnimi organi in zasebnim sektorjem javnost seznanjali z izzivi pri varovanju omrežnih in informacijskih sistemov;

9. meni, da izobraževanje o kibernetski varnosti ozavešča evropsko družbo o kibernetskih grožnjah, s čimer se spodbuja odgovorna uporaba kibernetskega prostora, prav tako pa pomaga pri povečevanju nabora kibernetskih veščin; priznava osrednjo vlogo agencije EUROPOL in njenega novega Evropskega centra za boj proti kibernetski kriminaliteti (EC3) ter agencij ENISA in EUROJUST pri zagotavljanju dejavnosti usposabljanja na ravni EU o uporabi orodij za mednarodno pravosodno sodelovanje in kazenski pregon v zvezi z različnimi vidiki kibernetske kriminalitete;

10. ponovno poudarja, da je treba zagotoviti tehnične nasvete in pravne informacije, prav tako pa oblikovati programe o preprečevanju kibernetske kriminalitete in boju proti njej; spodbuja usposabljanje računalniških inženirjev, specializiranih na varovanje kritične infrastrukture in informacijskih sistemov, pa tudi operaterjev sistemov za nadzor prometa in centrov za upravljanje prometa; poudarja, da je za zaposlene v javnem sektorju na vseh ravneh nujno treba uvesti programe rednega usposabljanja o kibernetski varnosti;

11. ponovno poziva k previdnosti pri omejevanju državljanov pri uporabi orodij komunikacijske in informacijske tehnologije in poudarja, da si morajo države članice pri pripravi odzivov na kibernetske grožnje in napade prizadevati, da v nobenem primeru ne bi ogrozile pravic in svoboščin državljanov, razpolagati pa morajo tudi z ustreznimi pravnimi sredstvi, ki razlikujejo med civilnimi in vojaškimi kibernetskimi incidenti;

12. meni, da bi moralo biti regulativno poseganje v kibernetsko varnost usmerjeno k tveganjem, osredotočeno na kritično infrastrukturo, katere neovirano delovanje je v interesu širše javnosti, in temeljiti na obstoječih tržnih poskusih industrije za zagotavljanje odpornosti omrežij; poudarja bistveno vlogo sodelovanja na operativni ravni pri spodbujanju učinkovitejše izmenjave informacij o kibernetskih grožnjah med javnimi organi in zasebnim sektorjem, tako na ravni Unije kot na nacionalni ravni, pa tudi s strateškimi partnerji Unije, da bi z vzpostavljanjem vzajemnega zaupanja, vrednot in predanosti ter izmenjavo strokovnega znanja zagotovili varnost omrežij in informacij; meni, da bi morala javno-zasebna partnerstva temeljiti na omrežni in tehnološki nevtralnosti ter se osredotočati na poskuse reševanja težav, ki občutno vplivajo na javnost; poziva Komisijo, naj vse sodelujoče tržne operaterje spodbuja k večji previdnosti in pripravljenosti k sodelovanju, da bi druge operaterje obvarovali pred motnjami v njihovih storitvah;

13. priznava, da je odkrivanje in sporočanje incidentov s področja kibernetske varnosti bistvenega pomena pri spodbujanju kibernetske odpornosti v Uniji; meni, da bi morale veljati sorazmerne in potrebne zahteve po razkritju, ki bi omogočale, da se incidenti, pri katerih prihaja do resnih kršitev varnosti, sporočijo pristojnim nacionalnim organom, prav tako pa bi izboljšale nadzor nad incidenti kibernetske kriminalitete in poenostavile

prizadevanje za ozaveščanje na vseh ravneh;

14. spodbuja Komisijo in druge akterje, naj na področju kibernetske varnosti in odpornosti uvedejo politiko, pri kateri bi se z ekonomskimi spodbudami zavzemali za visoko raven kibernetske varnosti in odpornosti;

Kibernetska odpornost

15. ugotavlja, da imajo različni sektorji in države članice različne ravni sposobnosti in veščin, to pa ovira razvoj zanesljivega sodelovanja in spodkopava delovanje enotnega trga;

16. meni, da bi morale zahteve za mala in srednja podjetja upoštevati sorazmeren in na tveganjih temelječ pristop;

17. vztraja pri razvoju kibernetske odpornosti za kritično infrastrukturo in opozarja, da bi bilo treba pri pripravah na izvajanje solidarnostne klavzule (člen 222 PDEU) upoštevati tveganje kibernetskega napada na posamezno državo članico; poziva Komisijo in visoko predstavnico, naj to tveganje upoštevata tudi v skupnih poročilih o celoviti oceni groženj in tveganj, ki jih bosta začela izdajati leta 2015;

18. poudarja, da mora biti, če želimo zagotoviti celovitost, razpoložljivost in zaupnost zlasti kritičnih storitev, identifikacija in kategorizacija kritične infrastrukture vselej posodobljena, izpolnjene pa morajo biti tudi potrebne minimalne varnostne zahteve za omrežja in informacijske sisteme;

19. priznava, da predlog direktive o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij po vsej Uniji predvideva minimalne varnostne zahteve za ponudnike storitev informacijske družbe in operaterje kritične infrastrukture;

20. poziva države članice in Unijo, naj oblikujejo ustrezne okvire za hitre, dvosmerne sisteme za izmenjavo informacij, s katerimi bodo zagotovili anonimnost zasebnega sektorja, javnemu sektorju pa redno posredovali najnovejše informacije, po potrebi pa naj zasebnemu sektorju zagotovijo tudi pomoč;

21. pozdravlja zamisel Komisije o vzpostavitvi kulture tveganja v zvezi s kibernetsko varnostjo in poziva države članice in institucije Unije, naj hitro vključijo krizno upravljanje na področju kibernetske varnosti v načrte kriznega upravljanja in analize tveganja; vlade držav članic in Komisijo prav tako poziva, naj spodbujajo akterje iz zasebnega sektorja, da bi krizno upravljanje na področju kibernetske varnosti vključili v svoje načrte kriznega upravljanja in analize tveganja ter usposabljali zaposlene o kibernetski varnosti;

22. poziva vse države članice in institucije Unije, naj vzpostavijo mrežo dobro delujočih skupin za odzivanje na računalniške grožnje (CERT), ki bi bile stalno dosegljive; poudarja, da bi bile nacionalne skupine CERT del učinkovite mreže, v kateri bi se izmenjevale ustrezne informacije ter upoštevali potrebni standardi zaupanja in zaupnosti; ugotavlja, da se utegnile krovne pobude, pri katerih bi sodelovale skupine CERT in drugi ustrezni varnostni organi, izkazati kot koristno orodje pri vzpostavljanju zaupanja v čezmejnem in medsektorskem okviru; priznava, kako pomembno je učinkovito in uspešno sodelovanje med skupinami CERT in organi kazenskega pregona pri boju proti kibernetski kriminaliteti;

23. podpira agencijo ENISA pri izvajanju dolžnosti na področju varnosti omrežja in informacij, zlasti s svetovanjem državam članicam in njihovem usmerjanju, pa tudi s podpiranjem izmenjave primerov najboljše prakse in vzpostavljanja okolja, v katerem vlada zaupanje;

24. poudarja, da mora industrija za proizvode IKT, ki se uporabljajo v prometnih omrežjih in informacijskih sistemih, po vsej verigi vrednot uvesti ustrezne zahteve glede zmogljivosti na področju kibernetske varnosti, vpeljati ustrezno upravljanje tveganj, sprejeti varnostne standarde in rešitve ter oblikovati primere najboljše prakse in vzpostaviti izmenjavo informacij, s čimer bi zagotovila, da bodo prometni sistemi varni;

Industrijski in tehnološki viri

25. meni, da ima zagotavljanje visoke ravni varnosti omrežij in informacij osrednjo vlogo pri povečevanju konkurenčnosti dobaviteljev in uporabnikov varnostnih rešitev v Uniji; meni, da se sicer v industriji informacijske varnosti v Uniji skriva še neizkoriščen potencial, a zasebni, javni in poslovni uporabniki pogosto niso seznanjeni s stroški in prednostmi naložb v kibernetsko varnost, zato ostajajo izpostavljeni škodljivim kibernetskim grožnjam; poudarja, da je pomemben dejavnik pri tem uvedba skupin CERT;

26. meni, da pestra ponudba rešitev kibernetske varnosti in povpraševanje po njih od nacionalnih organov, dejavnih na področju IKT, zahtevata ustrezne naložbe v akademske vire, raziskave in razvoj ter vzpostavljanje znanja in zmogljivosti, da bi spodbujali inovacije in dosegli zadostno ozaveščenost o tveganjih za varnost omrežij in informacij, posledično pa uskladili evropsko varnostno industrijo;

27. poziva institucije Unije in države članice, naj sprejmejo potrebne ukrepe za vzpostavitev "enotnega trga kibernetske varnosti", na katerem bodo lahko uporabniki in dobavitelji kar najbolje izkoristili razpoložljive inovacije, sinergije in skupno znanje, omogočil pa bo tudi vstop malih in srednjih podjetij;

28. spodbuja države članice, naj razmislijo o skupnih naložbah v evropsko industrijo kibernetske varnosti, podobno kot so storile pri drugih industrijah, na primer v letalskem sektorju;

Kibernetska kriminaliteta

29. meni, da so lahko kriminalne dejavnosti v kibernetskem prostoru enako škodljive za dobro delovanje družbe kot kazniva dejanja v realnem svetu in da se obe obliki kriminala pogosto medsebojno krepita, kakor je denimo mogoče videti na primerih spolnega izkoriščanja otrok ter organiziranega kriminala in pranja denarja;

30. ugotavlja, da v nekaterih primerih obstaja povezava med zakonitimi in nezakonitimi poslovnimi dejavnostmi; poudarja, kako pomembna je povezava med financiranjem terorizma in resnim organiziranim kriminalom, ki je po zaslugi interneta še enostavnejša; poudarja, da je treba javnost seznaniti z resnostjo vpletenosti v kibernetski kriminal in z dejstvom, da dejanja, ki utegnejo biti na prvi pogled videti kot družbeno sprejemljiv zločin, na primer nezakonito prenašanje filmov, mednarodnim kriminalnim združbam pogosto prinašajo velike količine denarja;

31. se strinja s Komisijo, da tudi v spletu veljajo enake norme in načela kot v običajnem svetu, zato meni, da je treba s posodobitvijo zakonodaje in operativnih zmogljivostmi okrepiti boj proti kibernetski kriminaliteti;

32. meni, da so glede na to, da kibernetska kriminaliteta ne pozna državnih meja, še posebej pomembna skupna prizadevanja in strokovno znanje na ravni Unije, torej nad ravnjo posameznih držav članic, in da je zato treba Eurojustu, EC3 Europola, skupinam CERT, univerzam in raziskovalnim centrom zagotoviti zadostna sredstva in možnosti, da bodo lahko neovirano delovali kot središča strokovnega znanja, sodelovanja in izmenjave informacij;

33. toplo pozdravlja ustanovitev agencije EC3 in spodbuja njen nadaljnji razvoj, spominja pa tudi na njeno pomembno vlogo pri usklajevanju pravočasne in učinkovite čezmejne izmenjave informacij in strokovnega znanja v podporo prizadevanjem za preprečevanje, odkrivanje in preiskovanje kibernetske kriminalitete;

34. poziva države članice, naj zagotovijo, da bodo lahko državljani zlahka dostopali do informacij o kibernetskih grožnjah in napotkov za spopadanje z njimi; meni, da bi napotki morali vključevati informacije o tem, kako lahko uporabniki varujejo zasebnost v internetu, odkrivajo in sporočajo primere navezovanja stikov z otroki v spolne namene, nameščajo programsko opremo in požarne zidove, upravljajo gesla in odkrivajo primere lažnega predstavljanja (phishing), zvabljanja (pharming) in druge napade;

35. vztraja pri tem, da morajo države članice, ki še niso ratificirale konvencije Sveta Evrope o kibernetski kriminaliteti iz Budimpešte, to nemudoma storiti; pozdravlja mnenje Sveta Evrope o potrebi po posodobitvi konvencije zaradi tehnološkega razvoja, da bi še naprej zagotavljali njeno učinkovitost pri obravnavi kibernetske kriminalitete, in poziva Komisijo in države članice, naj sodelujejo v tej razpravi; podpira prizadevanja za spodbujanje ratifikacije konvencije v drugih državah in poziva Komisijo, naj jo dejavno zagovarja tudi zunaj Unije;

Kibernetska zaščita

36. poudarja, da kibernetski izzivi, grožnje in napadi ogrožajo obrambne interese in interese nacionalne varnosti v državah članicah in da bi morali civilni in vojaški pristopi k varovanju kritične infrastrukture s prizadevanji za vzpostavitev sinergije prinesti koristi na obeh področjih;

37. zato poziva države članice, naj poglobijo sodelovanje z Evropsko obrambno agencijo, da bi pripravili predloge in pobude za zmogljivosti kibernetske zaščite, pri tem pa se opirali na nedavne pobude in projekte; poudarja, da je treba okrepiti raziskave in razvoj, tudi z združevanjem in s souporabo virov;

38. poudarja, da bi morala celovita strategija EU za kibernetsko varnost upoštevati dodano vrednost obstoječih agencij in organov, pa tudi primere dobre prakse iz držav članic, ki so že uvedle lastne nacionalne strategije za kibernetsko varnost;

39. poziva podpredsednico/visoko predstavnico, naj vključi upravljanje kibernetskih kriz med načrte za krizno upravljanje, in poudarja, da morajo države članice v sodelovanju z Evropsko obrambno agencijo oblikovati načrte za varovanje misij in operacij v okviru skupne varnostne in obrambne politike pred kibernetskimi napadi; poziva jih, naj s

skupnimi močni oblikujejo evropsko skupino za kibernetsko zaščito;

40. poudarja dobro praktično sodelovanje z Natom na področju kibernetske varnosti in meni, da je treba sodelovanje še poglobiti, zlasti s tesnejšim usklajevanjem na področjih načrtovanja, tehnologije, usposabljanja in opreme;

41. poziva Unijo, naj si prizadeva za izmenjavo mnenj z mednarodnimi partnerji, vključno z Natom, opredeli področja sodelovanja in, kjer je to mogoče, prepreči podvajanje dejavnosti ter zagotovi njihovo dopolnjevanje;

Mednarodna politika

42. meni, da imata mednarodno sodelovanje in dialog osrednjo vlogo pri ustvarjanju zaupanja in preglednosti, pa tudi pri spodbujanju visoke ravni mreženja in izmenjave informacij na svetovni ravni; zato poziva Komisijo in Evropsko službo za zunanje delovanje, naj ustanovita ekipo za kibernetsko diplomacijo, ki bi bila med drugim odgovorna za spodbujanje dialoga s podobno mislečimi državami in organizacijami; poziva k dejavnejši udeležbi EU na vrsti mednarodnih konferenc na visoki ravni o kibernetski varnosti;

43. meni, da je treba poiskati ravnovesje med konkurenčnimi cilji čezmejnega prenosa podatkov, zaščite podatkov in kibernetske varnosti, v skladu z mednarodnimi obveznostmi Unije, zlasti v okviru sporazuma GATS;

44. poziva podpredsednico/visoko predstavnico, naj vključi razsežnost kibernetske varnosti v zunanje delovanje EU, zlasti v zvezi s tretjimi državami, da bi poglobili sodelovanje in izmenjavo izkušenj in informacij o obravnavi kibernetske varnosti;

45. poziva Unijo, naj si prizadeva vzpostaviti izmenjavo mnenj z mednarodnimi partnerji, da bi opredelili področja sodelovanja in, kjer je to mogoče, preprečili podvajanje dejavnosti ter zagotovili njihovo dopolnjevanje; poziva podpredsednico/visoko predstavnico in Komisijo, naj bosta proaktivna v mednarodnih organizacijah in uskladita stališča držav članic o tem, kako učinkovito spodbujati rešitve in politike na kibernetskem področju;

46. meni, da bi si bilo treba prizadevati za to, da bi se v kibernetskem prostoru uveljavljali mednarodni pravni instrumenti, zlasti konvencija Sveta Evrope o kibernetski kriminaliteti; zato meni, da trenutno ni potrebe po oblikovanju novih pravnih instrumentov na mednarodni ravni; kljub temu pozdravlja mednarodno sodelovanje za pripravo pravil vedenja v kibernetskem prostoru, ki bi podprla načela prava v tem prostoru; meni, da bi veljalo razmisliti o posodobitvi obstoječih pravnih instrumentov, da bi jih prilagodili tehnološkim napredkom; meni, da se je treba v okviru vprašanja pristojnosti temeljito pogovoriti o pravosodnem sodelovanju in kazenskem pregonu v nadnacionalnih kriminalnih zadevah;

47. meni, da bi morala biti predvsem delovna skupina EU–ZDA za kibernetsko varnost in kibernetsko kriminaliteto instrument, s pomočjo katerega bi se, kadar je to mogoče, izmenjevali primeri najboljše prakse pri politikah kibernetske varnosti med EU in ZDA; v zvezi s tem ugotavlja, da bodo področja, povezana s kibernetsko varnostjo, na primer storitve, odvisne od varnega delovanja omrežnih in informacijskih sistemov, vključena v prihodnja pogajanja o čezatlantskem trgovinskem in naložbenem partnerstvu (TTIP), ki ga je treba skleniti tako, da bo ohranil suverenost EU in neodvisnost njenih institucij;

48. ugotavlja, da veščine s področja kibernetske varnosti in sposobnost preprečevanja, odkrivanja in učinkovitega spopadanja z grožnjami in zlonamernimi napadi niso po vsem svetu razvite v enaki meri; poudarja, da prizadevanja za povečanje kibernetske odpornosti in okrepitev boja proti kibernetskim grožnjam ne smejo biti omejena zgolj na enako misleče partnerje, temveč morajo prodreti tudi v regije z manj razvitimi zmogljivostmi, tehnično infrastrukturo in pravnimi okviri; meni, da je pri tem bistvenega pomena usklajevanje med skupinami CERT; poziva Komisijo, naj z ustreznimi sredstvi poenostavi prizadevanja tretjih držav za vzpostavitev lastnih zmogljivosti kibernetske varnosti, po potrebi pa naj jim pri tem tudi pomaga;

Izvajanje

49. poziva k rednim ocenam učinkovitosti nacionalnih strategij za kibernetsko varnost na najvišji politični ravni, da bi se prilagodili novim svetovnim grožnjam in v državah članicah zagotovili enako raven kibernetske varnosti;

50. poziva Komisijo, naj pripravi jasen načrt, v katerem bi določila časovni okvir za cilje, ki jih je treba v sklopu strategije za kibernetsko varnost doseči na ravni Unije, in za njihovo oceno; poziva države članice, naj se dogovorijo o podobnem načrtu za nacionalne dejavnosti v okviru te strategije;

51. zahteva, da mu Komisija, države članice, Europol ter novoustanovljeni EC3, Eurojust in ENISA redno posredujejo poročila, v katerih ocenijo napredek pri doseganju zastavljenih ciljev v okviru strategije za kibernetsko varnost, vključno z osrednjimi kazalniki uspešnosti, ki merijo napredek pri izvajanju;

o

o o

52. naroči svojemu predsedniku, naj to resolucijo posreduje Svetu, Komisiji, vladam in parlamentom držav članic, Europolu, Eurojustu ter Svetu Evrope.