EVROPSKI PARLAMENT 2009 - 2014

Dokument zasedanja

A7-0335/2012

17.10.2012

POROČILO

o kibernetski varnosti in obrambi
(2012/2096(INI))

Odbor za zunanje zadeve

Poročevalec: Tunne Kelam

PR_INI

VSEBINA

Stran

PREDLOG RESOLUCIJE EVROPSKEGA PARLAMENTA

o kibernetski varnosti in obrambi

(2012/2096(INI))

Evropski parlament,

– ob upoštevanju poročila o izvajanju evropske varnostne strategije, ki ga je Evropski svet podprl 11. in 12. decembra 2008,

– ob upoštevanju Konvencije Sveta Evrope o kibernetski kriminaliteti, podpisane 23. novembra 2001 v Budimpešti

– ob upoštevanju sklepov Sveta o zaščiti kritične informacijske infrastrukture z dne 27. maja 2011 in predhodnih sklepov Sveta o kibernetski varnosti,

– ob upoštevanju sporočila Komisije z naslovom „Evropska digitalna agenda“ z dne 19. maja 2010 (COM(2010)0245),

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

– ob upoštevanju nedavnega sporočila Komisije o ustanovitvi Evropskega centra za boj proti kibernetski kriminaliteti kot prednostne naloge strategije notranje varnosti (COM(2012)0140),

– ob upoštevanju resolucije z dne 10. marca 2010 o izvajanju evropske varnostne strategije v okviru evropske varnostne in obrambne politike[2],

– ob upoštevanju svoje resolucije z dne 11. maja 2011 o razvoju skupne varnostne in obrambne politike po začetku veljavnosti Lizbonske pogodbe[3],

– ob upoštevanju svoje resolucije z dne 22. maja 2012 o strategiji Evropske unije o notranji varnosti[4],

– ob upoštevanju svoje resolucije z dne 27. septembra 2011 o predlogu uredbe Evropskega parlamenta in Sveta o spremembi uredbe (EU) št. 1334/2000 o vzpostavitvi režima Skupnosti za nadzor izvoza blaga in tehnologije z dvojno rabo[5],

– ob upoštevanju svoje resolucije z dne 12. junija 2012 o zaščiti kritične informacijske

[1] UL L 345, 23.12.2008, str. 75.
[2] Sprejeta besedila, P7_TA(2010)0061.
[3] Sprejeta besedila, P7_TA(2011)0228.
[4] Sprejeta besedila, P7_TA(2012)0207.
[5] Sprejeta besedila, P7_TA(2012)0406.

infrastrukture – dosežki in naslednji koraki: h globalni kibernetski varnosti[1],

– ob upoštevanju resolucije Sveta ZN za človekove pravice z dne 5. julija 2012 o spodbujanju, varstvu in uživanju človekovih pravic na internetu[2], ki priznava pomen varstva človekovih pravic in prostega pretoka informacij na internetu,

– ob upoštevanju sklepov z vrhunskega srečanja v Chicagu dne 20. maja 2012,

– – ob upoštevanju Naslova V Pogodbe EU,

– ob upoštevanju člena 48 Poslovnika,

– ob upoštevanju poročila Odbora za zunanje zadeve (A7-0335/2012),

A. ker so EU in njene države članice v času globalizacije postale močno odvisne od varnega kibernetskega prostora, varne uporabe informacij in digitalnih tehnologij ter odpornih in zanesljivih informacijskih storitev in s tem povezane infrastrukture;

B. ker se informacijska in komunikacijska tehnologija uporablja tudi kot orodje za represijo; ker kontekst, v katerem se ta tehnologija uporablja, v veliki meri določa, ali bodo te tehnologije prispevale k pozitivnemu razvoju ali k represiji;

C. ker kibernetski izzivi, grožnje in napadi zelo hitro naraščajo ter predstavljajo veliko grožnjo za varnost, obrambo, stabilnost in konkurenčnost nacionalnih držav in tudi zasebnega sektorja; ker teh groženj prav zato ne bi smeli jemati kot zadeve, ki bodo obravnavane v prihodnosti; ker je večina zelo vidnih in motečih kibernetskih incidentov politično motiviranih; čeprav je velika večina kibernetskih incidentov še vedno primitivne oblike, grožnje kritičnim sredstvom postajajo vedno bolj prefinjene in zahtevajo dobro zaščito;

D. ker je kibernetski prostor s skoraj dvema milijardama medsebojno povezanih uporabnikov po vsem svetu postal eno najmočnejših in najučinkovitejših sredstev za spodbujanje demokratičnih idej in organiziranje ljudi v njihovem boju za svobodo in proti diktatorskim režimom; ker je uporaba kibernetskega prostora s strani nedemokratičnih in avtoritarnih režimov čedalje večja grožnja za pravice posameznikov do svobode izražanja in združevanja; ker je zato treba nujno zagotoviti, da bo kibernetski prostor ostal odprt za prost pretok idej, informacij in izražanja;

E. ker v EU in njenih državah članicah obstajajo številne politične, zakonodajne in organizacijske ovire za razvoj obsežnega in enotnega pristopa do kibernetske obrambe in kibernetske varnosti; ker na občutljivem in ranljivem področju kibernetske varnosti ni enotnih opredelitev, standardov in enotnih ukrepov;

F. ker izmenjava in usklajevanje v institucijah EU ter z državami članicami in med njimi in z zunanjimi partnerji še vedno ne zadoščata;

G. ker ni jasnih in usklajenih opredelitev „kibernetske varnosti“ na ravni EU in niti na

[1] Sprejeta besedila, P7_TA(2012)0237.
[2] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

mednarodni ravni; ker se razumevanje kibernetske varnosti in opredelitev drugih osrednjih pojmov med državami članicami močno razlikujeta;

H. ker EU še ni razvila samostojnih skladnih politik za varovanje kritične informacijske infrastrukture, kar zahteva multidisciplinaren pristop, torej zagotavljanje varnosti ob spoštovanju temeljnih pravic;

I. ker je EU predlagala več pobud za odpravo kibernetske kriminalitete na civilni ravni, vključno z ustanovitvijo novega evropskega centra za boj proti kibernetski kriminaliteti, a še nima konkretnega načrta na ravni varnosti in obrambe;

J. ker je vzpostavljanje zaupanja med zasebnim sektorjem, organi kazenskega pregona ter institucijami za obrambo in drugimi pristojnimi institucijami izjemno pomembno v boju proti kibernetski kriminaliteti;

K. ker je medsebojno zaupanje v odnosih med državnimi in nedržavnimi akterji osnovni pogoj za zanesljivo kibernetsko varnost;

L. ker večina kibernetskih incidentov tako v javnem kot v zasebnem sektorju ostane neprijavljenih zaradi občutljive narave informacij in morebitnega zmanjšanja ugleda vpletenih družb;

M. ker se veliko število kibernetskih incidentov zgodi zaradi pomanjkanja vzdržljivosti in odpornosti zasebne in javne omrežne infrastrukture, slabo zaščitenih ali varovanih podatkovnih baz in drugih pomanjkljivosti v kritični informacijski infrastrukturi; ker le malo držav članic obravnava zaščito svojih omrežij in informacijskih sistemov ter s tem povezanih podatkov kot del svojih dolžnosti, kar pojasnjuje pomanjkanje naložb v sodobno varnostno tehnologijo, usposabljanje in razvoj ustreznih smernic; ker je veliko držav članic odvisnih od varnostne tehnologije iz tretjih držav in bi morale okrepiti prizadevanja za zmanjšanje te odvisnosti;

N. ker se večine povzročiteljev kibernetskih napadov na visoki ravni, ki ogrožajo nacionalno ali mednarodno varnost in zaščito, nikoli ne identificira in kazensko preganja; ker ni mednarodno dogovorjenega odziva na državno podprt kibernetski napad na drugo državo niti dogovora, ali se tak napad lahko obravnava kot povod za vojno;

O. ker je Evropska agencija za varnost omrežij in informacij (ENISA) vključena kot posrednik, ki pomaga državam članicam pri izmenjavi primerov dobre prakse na področju kibernetske varnosti s priporočili o tem, kako razviti, izvajati in vzdrževati strategijo za kibernetsko varnost, ter ima podporno vlogo v nacionalnih strategijah za kibernetsko varnost, nacionalnih načrtih odzivnosti na incidente, pri organizaciji vseevropskih in mednarodnih vaj iz zaščite kritične informacijske infrastrukture (CIIP) ter pri oblikovanju scenarijev za vaje na nacionalni ravni;

P. ker je od junija 2012 samo 10 držav članic EU uradno sprejelo nacionalno strategijo za kibernetsko varnost;

Q. ker je kibernetska obramba ena glavnih prednostnih nalog Evropske obrambne agencije (EDA), ki je na podlagi načrta za razvoj zmogljivosti ustanovila projektno skupino za

kibernetsko varnost, v okviru katere večina držav članic sodeluje z zbiranjem izkušenj in svojimi predlogi;

R. ker so naložbe v raziskave in razvoj kibernetske varnosti in obrambe ključne za napredek in vzdrževanje visoke ravni kibernetske varnosti in obrambe; ker so se izdatki za obrambo, namenjeni raziskavam in razvoju, znižali, namesto da bi dosegli dogovorjena 2 % skupnih izdatkov za obrambo;

S. ker bi moralo biti ozaveščanje in izobraževanje državljanov o kibernetski varnosti temelj vsake celovite strategije za kibernetsko varnost;

T. ker je treba vzpostaviti jasno ravnovesje med varnostnimi ukrepi in državljanskimi pravicami v skladu s PDEU, na primer pravico do zasebnosti, varstva podatkov in svobode izražanja, pri čemer se ne sme žrtvovati ene strani na račun druge;

U. ker je vse bolj treba v večji meri spoštovati in zaščititi pravice posameznikov do zasebnosti, kot je navedeno v Listini EU in členu 16 PDEU; ker se potreba po varovanju in obrambi kibernetskega prostora na nacionalni ravni, na primer za institucije in obrambne organe, čeprav je pomembna, v nobenem primeru ne bi smela uporabiti kot izgovor za kakršno koli omejevanje pravic in svoboščin v kibernetskem in informacijskem prostoru;

V. ker globalna in brezmejna narava interneta zahteva nove oblike mednarodnega sodelovanja in upravljanja, pri katerih sodeluje več zainteresiranih strani;

W. ker se vlade pri varovanju svoje kritične infrastrukture vedno bolj zanašajo na zasebne akterje;

X. ker Evropska služba za zunanje delovanje (ESZD) vidika kibernetske varnosti še ni proaktivno vključila v svoje odnose s tretjimi državami;

Y. ker je instrument za stabilnost doslej edini program EU za odzivanje na nenadne krize ali globalne/nadregionalne varnostne izzive, vključno z grožnjami kibernetski varnosti;

Z. ker je skupni odziv – prek delovne skupine EU-ZDA za kibernetsko varnost in kibernetsko kriminaliteto – na grožnje kibernetski varnosti eno od prednostnih vprašanj v odnosih EU-ZDA;

Ukrepi in usklajevanje v EU

1. ugotavlja, da so kibernetske grožnje in napadi na vlado, upravne, vojaške in mednarodne organe v EU in v svetu čedalje večja nevarnost in vse pogostejši in da obstajajo resni razlogi za zaskrbljenost, da bi lahko državni in nedržavni akterji, zlasti teroristične organizacije in kriminalne združbe, napadli kritične informacijske in komunikacijske strukture ter infrastrukture institucij EU in članic, kar bi utegnilo povzročiti veliko škodo, vključno s kinetičnimi učinki;

2. zato poudarja potrebo po globalnem in usklajenem pristopu k tem izzivom na ravni EU z razvojem celovite strategije EU za kibernetsko varnost, ki bi morala vsebovati enotno

opredelitev kibernetske varnosti in obrambe ter sestave obrambnega kibernetskega napada, podati enotno vizijo delovanja in upoštevati dodano vrednost obstoječih agencij in organov; prav tako bi morala vsebovati primere dobre prakse iz držav članic, ki so že sprejele nacionalne strategije za kibernetsko varnost; poudarja ključni pomen usklajevanja in ustvarjanja sinergij na ravni Unije za povezovanje različnih pobud, programov ter vojaških in civilnih dejavnosti; poudarja, da bi takšna strategija morala zagotoviti prožnost in da bi jo bilo treba redno posodabljati, da bi jo prilagajali hitrim spremembam v kibernetskem prostoru;

3. poziva Komisijo in visoko predstavnico Unije za zunanje zadeve in varnostno politiko, naj v prihodnjem predlogu ureditve za izvajanje solidarnostne klavzule (člen 222 PDEU) razmislita o nevarnosti resnega kibernetskega napada na državo članico; prav tako meni, da bi bilo mogoče kibernetske napade, ki ogrožajo nacionalno varnost, čeprav jih je še treba terminološko opredeliti, zajeti v klavzulo o medsebojni obrambi (člen 42.7 PEU), brez poseganja v načelo sorazmernosti;

4. poudarja, da mora SVOP zaščititi sile, ki se nahajajo na vojaških operacijah in civilnih misijah EU, pred kibernetskimi napadi; poudarja, da bi morala kibernetska obramba postati dejavna zmožnost SVOP;

5. poudarja, da bi morale vse politike EU na področju kibernetske varnosti temeljiti in biti zasnovane tako, da bi zagotavljale največjo možno raven zaščite in ohranitev digitalnih svoboščin ter spoštovanje človekovih pravic na spletu; meni, da bi bilo treba internet ter informacijsko in komunikacijsko tehnologijo vključiti v zunanjo in varnostno politiko EU, da bi poudarili ta prizadevanja;

6. poziva Komisijo in Svet, naj digitalno svobodo enoglasno priznata kot temeljno pravico in nujen pogoj za uživanje splošnih človekovih pravic; poudarja, da bi moral biti cilj držav članic, da nikoli ne ogrozijo pravic in svoboščin svojih državljanov pri oblikovanju odzivov na kibernetske grožnje in napade, ter da bi morale v zakonodaji ustrezno razlikovati med civilno in vojaško naravo kibernetskih incidentov; poziva k previdnosti pri uvedbi omejitev uporabe orodij komunikacijske in informacijske tehnologije za državljane;

7. poziva Svet in Komisijo, naj skupaj z državami članicami pripravita belo knjigo o kibernetski obrambi, v kateri bi podala jasne opredelitve in merila za ločevanje stopenj kibernetskih napadov na civilnem in vojaškem področju, v skladu z njihovo motivacijo in učinki, pa tudi stopnje odzivov, vključno s preiskovanjem, odkrivanjem in kazenskim pregonom povzročiteljev napadov;

8. poudarja, da je treba obvezno posodobiti evropsko varnostno strategijo, da se poišče in opredeli ukrepe za zasledovanje in preganjanje posameznih, v mrežo povezanih in s strani države podprtih povzročiteljev napadov;

Raven EU

9. poudarja pomen horizontalnega sodelovanja in usklajevanja na področju kibernetske varnosti v institucijah in agencijah EU in med njimi;

10. poudarja, da nove tehnologije postavljajo na preizkušnjo način, na katerega vlade izvajajo svoje osnovne naloge; ponovno poudarja, da je obrambna in varnostna politika v končni fazi v rokah vlade ter vključuje ustrezen demokratični nadzor; je seznanjen s čedalje pomembnejšo vlogo zasebnih akterjev pri izvajanju nalog na področju varnosti in obrambe, ki pogosto potekajo brez preglednosti in odgovornosti ali mehanizma demokratičnega nadzora;

11. poudarja, da morajo vlade upoštevati osnovna mednarodna javna in humanitarna pravna načela, kot je spoštovanje državne suverenosti in človekovih pravic, kadar uporabljajo nove tehnologije na področju varnostne in obrambne politike; spominja na dragocene izkušnje držav članic EU, kot je Estonija, pri opredelitvi in zasnovi politik kibernetske varnosti ter obrambe;

12. priznava potrebo po oceni splošne ravni kibernetskih napadov na informacijske sisteme in infrastrukturo EU; v zvezi s tem posebej poudarja potrebo po stalnem ocenjevanju stopnje pripravljenosti institucij EU na reševanje potencialnih kibernetskih napadov; še posebej vztraja, da je treba okrepiti kritično informacijsko infrastrukturo;

13. poudarja tudi, da je treba zagotavljati obveščanje o šibkih točkah, nevarnostih in opozorilih o novih grožnjah za informacijske sisteme;

14. ugotavlja, da so nedavni kibernetski napadi na evropska informacijska omrežja in vladne informacijske sisteme povzročili večjo škodo gospodarstvu in varnosti, sam obseg te škode pa ni bil ustrezno ocenjen;

15. poziva vse institucije EU, naj v najkrajšem možnem času izdelajo strategije za kibernetsko varnost in načrte odzivnosti na incidente za lastne sisteme;

16. poziva vse institucije EU, naj v svojo analizo tveganj in načrte za obvladovanje kriz vključijo vprašanje obvladovanja kibernetskih kriz; prav tako poziva vse institucije EU, naj vsem članom svojega osebja omogočijo tečaje ozaveščanja o kibernetski varnosti; predlaga, da bi enkrat letno podobno kot vaje za ukrepanje v sili izvedli vaje za kibernetsko varnost;

17. poudarja pomen učinkovite vzpostavitve skupine EU za posredovanje pri omrežnih incidentih (EU-CERT) in drugih nacionalnih skupin CERT ter oblikovanja nacionalnih načrtov odzivnosti na incidente v primerih, ko je treba ukrepati; pozdravlja dejstvo, da so vse države članice EU do maja 2012 ustanovile nacionalne skupine CERT; poziva k nadaljnjemu razvoju nacionalnih CERT in skupine CERT EU, ki po potrebi lahko začnejo ukrepati v 24 urah; poudarja potrebo, da se preuči izvedljivost javno-zasebnih partnerstev na tem področju;

18. priznava, da se je „Cyber Europe 2010“, prva vseevropska vaja za zaščito kritične informacijske infrastrukture, pri kateri je sodelovalo več držav članic in jo je vodila ENISA, izkazala za koristen ukrep in primer dobre prakse; poudarja tudi, da je treba čim prej vzpostaviti informacijsko omrežje za opozarjanje o kritični infrastrukturi na evropski ravni;

19. poudarja pomen vseevropskih vaj, ki služijo pripravam na obsežne varnostne incidente v

omrežjih, ter opredelitve enotnih standardov za ocenjevanje groženj;

20. poziva Komisijo, naj preuči potrebo po centru EU za usklajevanje kibernetske varnosti (EU Cyber Coordination post) in njegovo izvedljivost;

21. meni, da bi morali Komisija, Svet in države članice glede na visoko raven usposobljenosti, ki je potrebna tako pri ustrezni obrambi kibernetskih sistemov in infrastruktur kot tudi pri napadu nanje, razmisliti o možnosti razvoja strategije etičnih hekerjev; ugotavlja, da je potencial za beg možganov v teh primerih visok in da imajo zlasti mladoletni, ki so bili obtoženih takšnih napadov, visok potencial za rehabilitacijo in integracijo v obrambne agencije in organe;

Evropska obrambna agencija (EDA)

22. pozdravlja nedavne pobude in projekte v zvezi s kibernetsko obrambo, zlasti glede zbiranja in razporejanja podatkov, izzivov in potreb v zvezi s kibernetsko varnostjo in obrambo, in poziva države članice, naj v zvezi s kibernetsko obrambo v večji meri sodelujejo, tudi na vojaški ravni, z Evropsko obrambno agencijo;

23. poudarja pomen tesnega sodelovanja držav članic z EDA za razvoj nacionalnih zmogljivosti za kibernetsko obrambo; je prepričan, da so ustvarjanje sinergij, združevanje in souporaba na evropski ravni ključni za učinkovito kibernetsko obrambo na evropski in nacionalni ravni;

24. spodbuja EDA, naj okrepi svoje sodelovanje z Natom ter nacionalnimi in mednarodnimi centri odličnosti, Evropskim centrom za kibernetsko kriminaliteto pri Europolu, ki prispeva k hitrejšim odzivom v primeru kibernetskega napada, še zlasti s Centrom odličnosti za sodelovanje pri kibernetski obrambi (CCDCOE), in se osredotoči na izgradnjo zmogljivosti, usposabljanje ter na izmenjavo informacij in prakse;

25. z zaskrbljenostjo opaža, da je ena sama država članica do leta 2010 za raziskave in razvoj namenila 2 % izdatkov za obrambo in da pet držav članic leta 2010 ničesar ni vložilo v raziskave in razvoj; poziva EDA, naj skupaj z državami članicami združi sredstva in dejansko vlaga v skupne raziskave in razvoj, zlasti za kibernetsko varnost in obrambo;

Države članice

26. poziva vse države članice, naj nemudoma razvijejo in dopolnijo svoje nacionalne strategije za kibernetsko varnost in obrambo ter zagotovijo solidno oblikovanje politike ter regulatorno okolje, obsežne postopke za obvladovanje tveganj in ustrezne pripravljalne ukrepe ter mehanizme; poziva ENISA, naj pomaga državam članicam; izraža svojo podporo ENISA pri oblikovanju vodnika dobre prakse o dobrih praksah in priporočilih o tem, kako razviti, izvajati in vzdrževati strategijo za kibernetsko varnost;

27. spodbuja vse države članice, naj v svoji vojaški strukturi uvedejo posebne enote za kibernetsko varnost in kibernetsko obrambo, z namenom sodelovanja s podobnimi organi v drugi državah članicah EU;

28. spodbuja države članice, naj na regionalni ravni uvedejo specializirana sodišča, ki bodo

učinkoviteje kaznovala napade na informacijske sisteme; vztraja, da je treba spodbujati prilagajanje nacionalnih zakonodaj tehničnemu razvoju in razvoju uporabe;

29. poziva Komisijo, naj si še naprej prizadeva za skladen in učinkovit evropski pristop, da bi se izognili nepotrebnim pobudam, ter spodbuja in podpira države članice v njihovih prizadevanjih za razvoj mehanizmov sodelovanja in obsežnejšo izmenjavo informacij; meni, da bi morali med državami članicami vzpostaviti vsaj minimalno raven obveznega sodelovanja in izmenjave;

30. poziva države članice, naj razvijejo nacionalne načrte odzivnosti na incidente ter vključijo obvladovanje kibernetskih kriz v načrte za obvladovanje kriz in analizo tveganj; nadalje poudarja pomen ustreznega usposabljanja na področju osnovne kibernetske varnosti za vse zaposlene v javnih subjektih, zlasti pa ustreznega usposabljanja za člane pravosodnih in varnostnih institucij v izobraževalnih ustanovah; poziva ENISA in druge ustrezne organe, naj pomagajo državam članicam pri združevanju in izmenjavi sredstev ter pri preprečevanju podvajanja;

31. poziva države članice, naj raziskave in razvoj postavijo za enega od temeljnih stebrov kibernetske varnosti in obrambe ter naj spodbujajo usposabljanje inženirjev, ki so specializirani za varovanje informacijskih sistemov; poziva države članice, naj izpolnijo svoje zaveze in povečajo delež izdatkov za obrambo za raziskave in razvoj na najmanj 2%, zlasti v zvezi s kibernetsko varnostjo in obrambo;

32. poziva Komisijo in države članice, naj pripravijo programe, s katerimi bi spodbujali splošno varno uporabo informacijskih in komunikacijskih tehnologij ter ozaveščali zasebne in poslovne uporabnike; predlaga, naj Komisija v zvezi s tem sproži javno vseevropsko izobraževalno pobudo, ter poziva države članice, naj izobraževanje o kibernetski varnosti vključijo v šolski učni načrt od najnižje možne starosti;

Sodelovanje javnega in zasebnega sektorja

33. poudarja ključno vlogo smiselnega in dopolnjujočega sodelovanja na področju kibernetske varnosti med javnimi organi in zasebnim sektorjem na ravni EU in na nacionalni ravni, katerega cilj je vzpostaviti medsebojno zaupanje; se zaveda, da bosta še večja zanesljivost in učinkovitost zadevnih javnih ustanov prispevala k izgradnji zaupanja in izmenjavi kritičnih informacij;

34. poziva partnerje v zasebnem sektorju, naj preučijo rešitve varnosti s pomočjo zasnove, kadar oblikujejo nove proizvode, naprave, storitve in aplikacije, ter spodbude za tiste, ki oblikujejo nove proizvode, naprave, storitve in aplikacije, katerih osrednja naloga je varnost s pomočjo zasnove; poziva, naj se v sodelovanju z zasebnim sektorjem oblikujejo minimalni standardi preglednosti in mehanizmi odgovornosti, da bi preprečili kibernetske napade in se borili proti njim;

35. poudarja, da je zaščita kritične informacijske infrastrukture vključena v strategijo EU o notranji varnosti zaradi povečanja varnosti državljanov in podjetij v kibernetskem prostoru;

36. zahteva, da se s temi partnerji vzpostavi stalni dialog o najboljši uporabi in odpornosti

informacijskih sistemov ter delitvi odgovornosti pri zagotavljanju varnega in dobrega delovanja teh sistemov;

37. meni, da bi morale države članice, institucije EU in zasebni sektor v sodelovanju z Evropsko agencijo za varnost omrežij in informacij sprejeti ukrepe za povečanje varnosti in celovitosti informacijskih sistemov, da bi preprečili napade in kolikor mogoče zmanjšali njihove posledice; podpira Komisijo pri njenih prizadevanjih za oblikovanje minimalnih standardov kibernetske varnosti in sistemov potrjevanja za podjetja ter zagotavljanje ustreznih spodbud za povečanje prizadevanj zasebnega sektorja, da izboljša varnost;

38. poziva Komisijo in vlade držav članic, naj spodbudijo zasebni sektor in akterje civilne družbe, naj obvladovanje kibernetskih kriz vključijo v svoje načrte obvladovanja kriz in analizo tveganj; nadalje poziva k uvedbi ozaveščevalnega usposabljanja o osnovni kibernetski varnosti in kibernetski higieni za vse člane njihovega osebja;

39. poziva Komisijo, naj v sodelovanju z državami članicami ter ustreznimi organi in agencijami oblikuje okvire in instrumente za sistem hitre izmenjave informacij, ki bi zagotovil anonimnost poročanja o kibernetskih incidentih za zasebni sektor, dosledno obveščal javne akterje in po potrebi zagotavljal pomoč;

40. poudarja potrebo, da EU poenostavi vzpostavitev konkurenčnega in inovativnega trga za kibernetsko varnost v EU, da bi MSP lažje delovala na tem področju, kar bo prispevalo k večji gospodarski rasti in ustvarjanju novih delovnih mest;

Mednarodno sodelovanje

41. poziva ESZD, naj proaktivno pristopi h kibernetski varnosti in naj vidik kibernetske varnosti prednostno vključi v vse svoje ukrepe, zlasti v zvezi s tretjimi državami; poziva k pospešenemu sodelovanju in izmenjavi informacij o tem, kako reševati vprašanja kibernetske varnosti s tretjimi državami;

42. poudarja, da je izoblikovanje celovite strategije EU za kibernetsko varnost osnovni pogoj za vzpostavitev takšnega učinkovitega mednarodnega sodelovanja na področju kibernetske varnosti, kakršnega terja čezmejni značaj kibernetskih groženj;

43. poziva tiste države članice, ki še niso podpisale ali ratificirale konvencije Sveta Evrope o kibernetski kriminaliteti (konvencija iz Budimpešte), naj to nemudoma storijo; podpira Komisijo in ESZD v njunih prizadevanjih za spodbujanje konvencije in njenih načel med tretjimi državami;

44. se zaveda potrebe po mednarodno dogovorjenem in usklajenem odzivu na kibernetske grožnje; zato poziva Komisijo, ESZD in države članice, naj prevzamejo vodilno vlogo v vseh forumih, zlasti v Združenih narodih, ter si prizadevajo za obsežnejše mednarodno sodelovanje ter končni sporazum o skupni opredelitvi pravil vedenja v kibernetskem prostoru, prav tako pa naj spodbujajo sodelovanje pri oblikovanju sporazumov o nadzoru nad kibernetskim orožjem;

45. spodbuja izmenjave znanja na področju kibernetske varnosti z državami BRICS in

drugimi državami z gospodarstvi v vzponu, da se preučijo možnosti enotnih odzivov na naraščajočo kibernetsko kriminaliteto, grožnje in napade, tako na civilni kot na vojaški ravni;

46. poziva ESZD in Komisijo, naj bo njun pristop v okviru zadevnih mednarodnih forumov in organizacij, zlasti ZN, OVSE, OECD in Svetovne banke, proaktiven, in sicer zato, da bi se uporabljalo obstoječe mednarodno pravo in doseglo soglasje o merilih odgovornega ravnanja držav na področju kibernetske varnosti in obrambe, ter z usklajevanjem stališč držav članic, da bi spodbujali temeljne vrednote in politike EU na področju kibernetske varnosti in obrambe;

47. poziva Svet in Komisijo, naj v dialogih, odnosih in sporazumih o sodelovanju s tretjimi državami, zlasti tistimi, ki zagotavljajo tehnološko sodelovanje ali izmenjavo, vztrajata pri minimalnih zahtevah v zvezi s preprečevanjem kibernetske kriminalitete in kibernetskih napadov ter bojem proti njim; in tudi pri minimalnih standardih varnosti informacijskih sistemov;

48. poziva Komisijo, naj tretjim državam po potrebi pomaga vzpostaviti zmogljivosti za kibernetsko varnost in kibernetsko obrambo;

Sodelovanje z Natom

49. ponovno poudarja, da imata EU in NATO zaradi svojih skupnih vrednot in strateških interesov posebno odgovornost in zmožnost, da se z naraščajočimi izzivi kibernetske varnosti soočita učinkoviteje in v tesnem sodelovanju, tako da poiščeta morebitna dopolnjevanja, brez podvajanja in s spoštovanjem pristojnosti drug drugega;

50. poudarja potrebo po zbiranju in izmenjavi na praktični ravni, ob upoštevanju dopolnjevanja v pristopu EU in NATO h kibernetski varnosti in obrambi; poudarja potrebo po tesnejšem sodelovanju, zlasti v zvezi z načrtovanjem, tehnologijo, usposabljanjem in opremo za kibernetsko varnost in obrambo;

51. na podlagi obstoječih dopolnilnih dejavnosti pri razvoju obrambnih zmogljivosti poziva vse ustrezne organe v EU, ki se ukvarjajo s kibernetsko varnostjo in obrambo, naj okrepijo svoje praktično sodelovanje z Natom, da bi si izmenjali izkušnje in se naučili, kako poskrbeti za odpornost sistemov EU;

Sodelovanje z ZDA

52. meni, da bi morale EU in ZDA okrepiti medsebojno sodelovanje v boju proti kibernetskim napadom in kibernetski kriminaliteti, saj je to prednostna naloga čezatlantskih odnosov po srečanju na vrhu EU-ZDA leta 2010 v Lizboni;

53. pozdravlja oblikovanje delovne skupine EU-ZDA o kibernetski varnosti in kibernetskem kriminalu na vrhunskem srečanju med EU in ZDA novembra 2010 ter podpira njena prizadevanja za vključitev vprašanj kibernetske varnosti v čezatlantski politični dialog;

54. pozdravlja, da sta Komisija in ameriška vlada pod okriljem delovne skupine EU-ZDA izdelala skupen program in časovni načrt za skupne/sinhronizirane medcelinske vaje za

kibernetsko varnost v letih 2012 in 2013; je seznanjen s prvo vajo „Cyber Atlantic“ v letu 2011;

55. poudarja, da je nujno tako za ZDA kot tudi za EU, da kot največja vira kibernetskega prostora in uporabnikov sodelujeta pri zaščiti pravic in svoboščin državljanov pri uporabi tega prostora; poudarja, da je nacionalna varnost sicer najpomembnejši cilj, a je treba vseeno varovati in ščititi kibernetski prostor;

56. naroči svojemu predsedniku, naj to resolucijo posreduje Svetu, Komisiji, visoki predstavnici/podpredsednici, Evropski obrambni agenciji, Evropski agenciji za varnost omrežij in informacij in Natu.

IZID KONČNEGA GLASOVANJA V ODBORU

Datum sprejetja	10.10.2012
Izid končnega glasovanja	+: 47 –: 3 0: 6
Poslanci, navzoči pri končnem glasovanju	Bastiaan Belder, Franziska Katharina Brantner, Elmar Brok, Jerzy Buzek, Tarja Cronberg, Arnaud Danjean, Mário David, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Liisa Jaakonsaari, Anneli Jäätteenmäki, Jelko Kacin, Ioanis Kasulidis (Ioannis Kasoulides), Tunne Kelam, Nicole Kiil-Nielsen, Evgeni Kirilov, Maria Eleni Kopa (Maria Eleni Koppa), Wolfgang Kreissl-Dörfler, Eduard Kukan, Vytautas Landsbergis, Krzysztof Lisek, Sabine Lösing, Mario Mauro, Francisco José Millán Mon, Alexander Mirsky, María Muñiz De Urquiza, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Justas Vincas Paleckis, Bernd Posselt, Cristian Dan Preda, Fiorello Provera, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Sofokles Sofokleus (Sophocles Sophocleous), Laurence J.A.J. Stassen, Kristian Vigenin, Sir Graham Watson, Karim Zéribi
Namestniki, navzoči pri končnem glasovanju	Haralampos Angurakis (Charalampos Angourakis), Elena Băsescu, Jean-Jacob Bicep, Véronique De Keyser, Diogo Feio, Elisabeth Jeggle, Indrek Tarand, Sampo Terho, László Tőkés, Traian Ungureanu, Luis Yáñez-Barnuevo García
Namestniki (člen 187(2)), navzoči pri končnem glasovanju	Joseph Cuschieri