65. atrage atenția asupra nevoii de a promova voluntariatul, în special în timpul Anului European al Cetățenilor 2013, și solicită Comisiei să includă susținerea activităților de voluntariat în politicile internaționale de asistență pentru dezvoltare, inclusiv cu scopul de a realiza toate obiectivele identificate în Obiectivele de dezvoltare ale mileniului;

66. susține examinarea formală a propunerii „Solidarité", vizând crearea unui program interinstituțional de resurse umane în instituțiile UE care să faciliteze implicarea personalului instituțiilor și a stagiarilor în activități de voluntariat, umanitare și sociale, atât ca parte a formării profesionale, cât și ca voluntariat în timpul lor liber;

67. subliniază faptul că programul propus va conduce la o scădere a cheltuielilor, are o valoare adăugată ridicată și va contribui la implementarea politicilor și programelor UE;

68. recomandă Comisiei să mențină punctele de contact utile stabilite atât cu „EYV 2011 Alliance" și cu succesoarea sa, Platforma Voluntarilor, care include multe organizații de voluntariat și rețele ale societății civile, cât și cu organismele naționale de coordonare, cu partenerii strategici și cu purtătorii de cuvânt ai guvernelor naționale în domeniu, având în vedere varietatea largă a organismelor implicate în voluntariat în UE, și încurajează aceste puncte de contact să se implice în mod activ în proiectul de portal centralizat al UE, în calitate de platformă paneuropeană, pentru a facilita coordonarea și intensificarea activităților transfrontaliere;

69. subliniază importanța rețelelor de contact și a schimburilor de bune practici pentru difuzarea informațiilor cu privire la procedurile UE care pot ajuta și sprijini activitățile de voluntariat transfrontaliere;

70. solicită Comisiei să ia măsurile necesare, atunci când consideră oportun, în legătură cu Agenda politică pentru voluntariat în Europa (PAVE), care a fost elaborată de organizațiile de voluntariat implicate în EYV 2011 Alliance.

71. încredințează Președintelui sarcina de a transmite prezenta rezoluție Consiliului și Comisiei, precum și guvernelor și parlamentelor statelor membre.

Protecția infrastructurilor informatice critice: către un context global de securitate cibernetică

P7_TA(2012)0237

Rezoluția Parlamentului European din 12 iunie 2012 referitoare la protecția infrastructurilor critice de informație - realizări și etape următoare: către un context global de securitate cibernetică (2011/2284(INI))

(2013/C 332 E/03)

Parlamentul European,

— având în vedere Rezoluția sa din 5 mai 2010 intitulată „O nouă agendă digitală pentru Europa: 2015.eu" ([1]),

— având în vedere Rezoluția sa din 15 iunie 2010 intitulată „Guvernanța internetului: etapele următoare" ([2]),

— având în vedere Rezoluția sa din 6 iulie 2011 intitulată „Banda largă europeană: o investiție într-un promotor digital al creșterii" ([3]),

— având în vedere articolul 48 din Regulamentul său de procedură,

— având în vedere raportul Comisiei pentru industrie, cercetare și energie și avizul Comisiei pentru libertăți civile, justiție și afaceri interne (A7-0167/2012),

([1]) JO C 81 E, 15.3.2011, p. 45.
([2]) JO C 236 E, 12.8.2011, p. 33.
([3]) Texte adoptate, P7_TA(2011)0322.

A. întrucât tehnologiile informației și comunicațiilor (TIC) pot să își mobilizeze întreaga capacitate pentru avansarea economiei și a societății doar dacă utilizatorii au încredere în siguranța și reziliența acestora și dacă legislația în domenii precum confidențialitatea datelor și drepturile de proprietate intelectuală este pusă în execuție în mod eficient în mediul online;

B. întrucât impactul internetului și al TIC asupra diferitelor aspecte ale vieții cetățenilor devine cu rapiditate din ce în ce mai puternic și întrucât acestea reprezintă un factor esențial al interacțiunii sociale, al îmbogățirii culturale și al creșterii economice;

C. întrucât securitatea TIC și a internetului reprezintă un concept cuprinzător, cu incidență globală asupra aspectelor economice, sociale, tehnologice și militare și care necesită atât definirea și diferențierea clară a responsabilităților, cât și un mecanism solid de cooperare internațională;

D. întrucât inițiativa emblematică Agenda digitală a UE are ca obiectiv creșterea competitivității Europei, pe baza consolidării TIC, și crearea condițiilor atât pentru o creștere economică ridicată și solidă, cât și pentru locuri de muncă bazate pe tehnologie;

E. întrucât sectorul privat rămâne investitorul, proprietarul și administratorul de prim rang al produselor, al serviciilor, al aplicațiilor și al infrastructurii de securitate a informațiilor, investind miliarde de euro în ultimul deceniu; întrucât această implicare ar trebui consolidată prin strategii corespunzătoare în materie de politici pentru promovarea rezilienței infrastructurilor fie aflate în proprietatea sectorului public, a sectorului privat sau a unor parteneriate public-private, fie operate de acestea;

F. întrucât dezvoltarea unui înalt nivel de securitate și de reziliență a rețelelor, a serviciilor și a tehnologiilor TIC ar trebui să consolideze competitivitatea economiei europene, atât prin îmbunătățirea evaluării și a gestionării riscurilor cibernetice, cât și prin punerea la dispoziția economiei UE în general a unor infrastructuri informaționale mai solide pentru a susține inovarea și creșterea economică, creând noi oportunități pentru creșterea productivității întreprinderilor;

G. întrucât datele disponibile privind aplicarea legislației în materie de infracționalitate cibernetică – vizând atacurile cibernetice, dar și alte tipuri de infracțiuni online – sugerează o creștere semnificativă în diverse țări europene; întrucât, totuși, în ceea ce privește atacurile cibernetice există în continuare prea puține date reprezentative din punct de vedere statistic furnizate atât de autoritățile responsabile cu aplicarea legislației, cât și de CERT (echipele de intervenție în caz de urgențe informatice) și este necesar ca acestea să fie mai bine agregate în viitor, ceea ce va permite intervenții mai semnificative din partea autorităților responsabile cu aplicarea legislației la nivelul întregii UE și va asigura adoptarea unor intervenții legislative bazate pe informații mai bune privind aceste amenințări cibernetice tot mai evoluate;

H. întrucât este esențial un nivel adecvat de securitate a informațiilor pentru a se asigura o extindere puternică a serviciilor bazate pe internet;

I. întrucât incidentele, perturbările și atacurile cibernetice recente împotriva infrastructurii de informație a instituțiilor UE, a industriei și a statelor membre demonstrează necesitatea de a stabili un sistem solid, inovator și eficient de protejare a infrastructurii critice de informație (CIIP), pe baza unei cooperări internaționale depline între statele membre și a unor standarde minime de rezistență în cadrul acestora;

J. întrucât dezvoltarea rapidă a noilor mijloace ale TIC, precum informatica dematerializată (cloud computing), impune acordarea unei atenții deosebite securității pentru a putea profita pe deplin de beneficiile realizărilor tehnologice;

K. întrucât Parlamentul European a insistat în repetate rânduri asupra aplicării unor standarde ridicate pentru confidențialitatea și protecția datelor, pentru neutralitatea internetului și protecția drepturilor de proprietate intelectuală;

Măsuri pentru consolidarea CIIP la nivel național și la nivelul Uniunii

1. salută implementarea de către statele membre a Programului european pentru CIIP, inclusiv stabilirea rețelei de alertă privind infrastructurile critice (CIWIN);

2. consideră că eforturile de protejare a infrastructurilor critice de informație vor îmbunătăți nu doar securitatea generală a cetățenilor, ci și percepția acestora asupra securității și încrederea lor în măsurile adoptate de guvern cu scopul de a-i proteja;

3. recunoaște că Comisia are în vedere posibila revizuire a Directivei 2008/114/CE a Consiliului ([1]) și solicită să se furnizeze dovezi privind eficacitatea și impactul directivei înainte de întreprinderea altor demersuri; solicită să se examineze posibilitatea lărgirii domeniului său de aplicare, în special prin includerea sectorului TIC și a serviciilor financiare; solicită, pe lângă acestea, să se acorde atenție domeniilor precum sistemele de sănătate, de alimentație și de furnizare a apei, cercetarea nucleară și industria nucleară (dacă nu sunt acoperite de dispoziții specifice); consideră că aceste sectoare ar trebui, de asemenea, să beneficieze de abordarea transsectorială adoptată de CIWIN (constând în cooperare, un sistem de avertizare și schimbul de bune practici);

4. subliniază importanța asigurării și implementării unei integrări durabile a activităților de cercetare europene pentru a menține și a consolida excelența europeană în domeniul CIIP;

5. solicită, având în vedere natura interconectată și deosebit de interdependentă, sensibilă, strategică și vulnerabilă a CIIP naționale și ale UE, actualizarea periodică a standardelor minime de reziliență în ceea ce privește pregătirea și reacția în caz de perturbări, incidente, tentative de distrugere sau atacuri, precum cele rezultate din cauza unei infrastructuri insuficient de solide sau a unor terminale finale insuficient securizate;

6. subliniază importanța standardelor și a protocoalelor de securitate informatică și salută mandatarea în 2011 a CEN, Cenelec și ETSI să stabilească standarde de securitate;

7. se așteaptă ca proprietarii și operatorii de infrastructuri critice de informație să permită și, dacă este necesar, să asiste utilizatorii să utilizeze mijloacele adecvate pentru a se proteja împotriva atacurilor și/sau a perturbărilor rău intenționate, atât prin supraveghere manuală, cât și prin supraveghere automată, când este necesar;

8. susține cooperarea între părțile interesate publice și private la nivelul Uniunii și încurajează eforturile acestora de a dezvolta și de a implementa standarde de securitate și de rezistență pentru infrastructurile critice de informație civile (publice, private sau public-private) de la nivel național și european;

9. subliniază importanța exercițiilor paneuropene în vederea pregătirii pentru incidente la scară largă legate de securitatea rețelelor și importanța definirii unui singur set de standarde pentru evaluarea amenințărilor;

10. solicită Comisiei, în cooperare cu statele membre, să evalueze implementarea planului de acțiune CIIP; îndeamnă statele membre să organizeze echipe naționale de intervenție în caz de urgență informatică (CERT), să dezvolte strategii naționale în materie de securitate cibernetică, să organizeze exerciții periodice privind incidente cibernetice la nivel național și paneuropean, să dezvolte planuri naționale de urgență privind incidentele cibernetice și să contribuie la dezvoltarea unui plan european de urgență privind incidentele cibernetice până la sfârșitul anului 2012;

11. recomandă stabilirea unor planuri de securitate ale operatorului sau a unor măsuri echivalente pentru toate infrastructurile critice de informație europene și numirea unor ofițeri de legătură pentru securitate;

12. salută revizuirea actuală a Deciziei-cadru 2005/222/JAI a Consiliului privind atacurile împotriva sistemelor informaționale ([2]); constată nevoia de a coordona eforturile UE de combatere a atacurilor cibernetice de mare anvergură prin includerea competențelor ENISA, ale echipelor CERT ale statelor membre și ale viitoarei echipe CERT europene;

13. consideră că ENISA poate să îndeplinească un rol-cheie la nivel european în ceea ce privește protecția infrastructurilor critice de informație oferind informații tehnice de specialitate statelor membre și instituțiilor și organismelor Uniunii Europene, precum și realizând rapoarte și analize privind securitatea sistemelor de informație la nivel european și global;

Activități suplimentare întreprinse de UE pentru a garanta că internetul beneficiază de o securitate solidă

14. solicită ENISA să coordoneze și să implementeze anual Lunile de conștientizare a securității internetului ale UE, astfel încât problemele care au legătură cu securitatea cibernetică să devină o preocupare specială pentru statele membre și cetățenii UE;

([1]) JO L 345, 23.12.2008, p. 75.
([2]) JO L 69, 16.3.2005, p. 67.

15. susține ENISA, în conformitate cu obiectivele Agendei digitale, în exercitarea sarcinilor sale privind securitatea informațiilor în rețea îndeplinite, în special, prin asigurarea de îndrumare și de consultanță pentru statele membre privind modul în care să asigure capabilitățile de bază ale echipelor lor CERT, precum și modul în care să susțină schimbul de bune practici prin intermediul dezvoltării unui mediu de încredere; solicită agenției să consulte părțile interesate relevante pentru definirea unor măsuri similare de securitate cibernetică pentru proprietarii și operatorii de rețele și de infrastructuri private, precum și să furnizeze asistență Comisiei și statelor membre pentru a contribui la dezvoltarea și la asimilarea de sisteme de certificare a securității informațiilor, de coduri de conduită și de practici de cooperare în rândul echipelor CERT naționale și europene și al proprietarilor/operatorilor de infrastructuri, când este nevoie inclusiv prin definirea unor cerințe minime neutre și comune în materie de tehnologie;

16. salută propunerea actuală de revizuire a mandatului ENISA, în special prelungirea acestuia, și de extindere a sarcinilor agenției; consideră că, pe lângă asistența oferită statelor membre prin furnizarea de expertiză și analiză, ENISA ar trebui să aibă dreptul de a gestiona un număr de sarcini executive la nivelul UE și, în cooperare cu omologii săi din SUA, de sarcini care sunt legate de prevenirea și detectarea incidentelor în domeniul securității rețelelor și a informațiilor și care întăresc coordonarea între statele membre; subliniază că, în temeiul Regulamentului ENISA, agenției i s-ar putea atribui responsabilități suplimentare privind intervenția în caz de atacuri prin internet, în măsura în care asigură o valoare adăugată clară pentru mecanismele naționale de intervenție.

17. salută rezultatele exercițiilor paneuropene privind securitatea cibernetică din 2010 și din 2011, realizate la nivelul întregii Uniuni și monitorizate de ENISA, al căror scop a fost să furnizeze asistență statelor membre pentru proiectarea, întreținerea și testarea unui plan paneuropean de urgență; solicită ENISA să mențină în programul său astfel de exerciții și să implice treptat operatorii privați relevanți, dacă este cazul, pentru a spori capacitățile generale în materie de securitate a internetului ale Europei; așteptă cu interes continuarea extinderii la nivel internațional alături de parteneri care împărtășesc aceeași viziune;

18. solicită statelor membre să stabilească planuri naționale de urgență în caz de incidente cibernetice, care să includă elemente-cheie, precum punctele de contact relevante și dispozițiile privind asistența, limitarea extinderii incidentului și remedierea daunelor în cazul unor defecțiuni sau atacuri cibernetice cu relevanță regională, națională sau transfrontalieră; observă faptul că statele membre trebuie să instituie, de asemenea, mecanisme și structuri corespunzătoare de coordonare la nivel național, care ar trebui să ajute la o mai bună coordonare în rândul autorităților naționale competente și să asigure o mai mare coerență a acțiunilor acestora;

19. sugerează Comisiei să propună măsuri obligatorii prin intermediul planului UE de urgență privind incidentele cibernetice pentru a asigura o mai bună coordonare la nivelul UE a funcțiilor tehnice și de conducere în rândul echipelor CERT naționale și guvernamentale;

20. solicită Comisiei și statelor membre să adopte măsurile necesare în vederea protejării infrastructurilor critice împotriva atacurilor cibernetice și să asigure mijloacele necesare pentru întreruperea ermetică a accesului la o infrastructură critică în cazul în care un atac cibernetic direct amenință în mod grav funcționarea corespunzătoare a acesteia;

21. așteaptă cu interes implementarea completă a CERT-UE, care va fi un factor important în prevenirea, detectarea, intervenția și recuperarea în urma unor atacuri cibernetice voluntare și rău-intenționate care au ca țintă instituțiile UE;

22. recomandă propunerea de către Comisie a unor măsuri obligatorii destinate să impună standarde minime în materie de securitate și de reziliență și să îmbunătățească coordonarea la nivelul CERT naționale;

23. solicită statelor membre și instituțiilor UE să asigure existența unor echipe CERT funcționale, care să aibă în dotare capacități minime de securitate și de reziliență, pe baza celor mai bune practici convenite; subliniază că echipele CERT naționale ar trebui să facă parte dintr-o rețea eficientă, în cadrul căreia să se facă schimb de informații relevante, în conformitate cu standardele necesare de confidențialitate; solicită asigurarea unei permanențe 24 ore din 24, 7 zile din 7 în cadrul serviciilor CIIP pentru fiecare stat membru, precum și crearea unui protocol de urgență comun la nivel european care să fie aplicabil între punctele de contact naționale;

24. subliniază că sunt esențiale consolidarea încrederii și promovarea cooperării dintre statele membre pentru protejarea datelor și a rețelelor și infrastructurilor naționale; solicită Comisiei să propună o procedură comună pentru identificarea și desemnarea unei abordări comune în vederea gestionării amenințărilor transfrontaliere de tip TIC, cu condiția ca statele membre să furnizeze Comisiei informații generice privind riscurile, amenințările și vulnerabilitățile propriilor infrastructuri critice de informație;

25. salută inițiativa Comisiei de a dezvolta până în 2013 un sistem european de alertare și partajare a informațiilor;

26. salută diversele consultări cu părțile interesate privind securitatea internetului și CIIP inițiate de Comisie, precum Parteneriatul european public-privat pentru reziliență; recunoscând implicarea și angajamentul deja semnificative ale furnizorilor de TIC în ceea ce privește aceste eforturi, încurajează Comisia să facă eforturi suplimentare pentru a încuraja mediul universitar și asociațiile de utilizatori TIC să joace un rol mai activ și să stimuleze un dialog constructiv, cu mai multe părți interesate, pe probleme de securitate cibernetică; susține dezvoltarea în continuare a Agendei digitale, ca un cadru pentru guvernanța CIIP;

27. salută activitatea realizată până în prezent de Forumul european al statelor membre în ceea ce privește stabilirea de criterii specifice sectorului pentru identificarea infrastructurilor europene critice, acordând atenție comunicațiilor fixe și mobile, precum și în ceea ce privește discutarea principiilor și a orientărilor UE privind reziliența și stabilitatea internetului; așteaptă cu interes continuarea procesului de obținere a unui consens între statele membre, iar în acest context încurajează forumul să completeze abordarea actuală axată pe active corporale cu eforturi de a include și active ale infrastructurii logice care, datorită dezvoltării virtualizării și a tehnologiilor dematerializate, vor deveni tot mai relevante pentru eficacitatea CIIP;

28. sugerează Comisiei să lanseze o inițiativă de educație publică paneuropeană, axată pe educarea și sensibilizarea utilizatorilor finali atât din mediul privat, cât și din cel de afaceri, cu privire la eventuale amenințări împotriva internetului și a dispozitivelor TIC fixe și mobile de la toate nivelurile lanțului de utilități, precum și pe promovarea unei conduite individuale online mai sigure; reamintește, în această privință, riscurile asociate echipamentelor și programelor IT depășite;

29. solicită statelor membre să consolideze, cu ajutorul Comisiei, programele de formare și de educare în domeniul securității informațiilor, destinate autorităților naționale de aplicare a legislației și celor judiciare, precum și agențiilor UE relevante;

30. susține crearea unui program de învățământ al UE pentru experții universitari în domeniul securității informațiilor, deoarece aceasta ar avea un impact pozitiv asupra cunoștințelor și gradului de pregătire ale UE în ceea ce privește spațiul cibernetic și amenințările la adresa acestuia, care se află în continuă evoluție;

31. susține promovarea învățământului în domeniul securității cibernetice (stagii pentru doctoranzi, cursuri universitare, ateliere, cursuri de formare pentru studenți etc.) și a exercițiilor de formare specializate în domeniul CIIP;

32. solicită Comisiei să propună, până la sfârșitul anului 2012, o strategie cuprinzătoare privind securitatea internetului pentru Uniune, pe baza unei terminologii clare; consideră că strategia privind securitatea internetului ar trebui să aibă ca scop crearea unui spațiu cibernetic – sprijinit de o infrastructură sigură și rezilientă și de standarde deschise – care să fie favorabil inovării și prosperității prin libera circulație a informațiilor, asigurându-se în același timp o protecție puternică a vieții private și a celorlalte libertăți civile; susține că strategia ar trebui să detalieze principiile, obiectivele, metodele, instrumentele și politicile (atât interne, cât și externe) necesare pentru a raționaliza eforturile naționale și ale UE și pentru a stabili standarde minime de reziliență între statele membre pentru a asigura un serviciu sigur, continuu, solid și rezilient, fie în ceea ce privește infrastructura critică, fie în ceea ce privește utilizarea generală a internetului;

33. subliniază faptul că viitoarea strategie privind securitatea internetului a Comisiei ar trebui să aibă ca punct central de referință activitatea privind CIIP și să urmărească o abordare globală și sistematică a securității cibernetice prin includerea atât a unor măsuri proactive, precum introducerea de standarde minime privind măsurile de securitate sau instruirea utilizatorilor individuali, a întreprinderilor și a instituțiilor publice, cât și a unor măsuri luate ca răspuns la o acțiune, precum sancțiuni penale, civile și administrative;

34. îndeamnă Comisia să propună un mecanism solid pentru coordonarea implementării și a actualizării periodice a strategiei privind securitatea internetului; consideră că acest mecanism ar trebui să fie susținut de suficiente resurse administrative, specializate și financiare și să aibă competența de a facilita elaborarea de poziții ale UE în relațiile atât cu părțile interesate interne, cât și cu cele internaționale, privind aspecte legate de securitatea internetului;

35. solicită Comisiei să propună un cadru UE pentru notificarea cazurilor de încălcare a securității în sectoarele critice cum ar fi energia, transporturile, aprovizionarea cu apă și alimente, precum și în sectorul tehnologiei informației și comunicațiilor și al serviciilor financiare, pentru a garanta că autoritățile competente ale statelor membre și utilizatorii sunt notificați cu privire la incidentele, atacurile și perturbările cibernetice;

36. îndeamnă Comisia să îmbunătățească disponibilitatea datelor relevante din punct de vedere statistic privind costurile atacurilor cibernetice în UE, în statele membre și în industrie (în special în sectorul serviciilor financiare și al TIC) prin consolidarea capacităților de colectare a datelor ale Centrului european de combatere a criminalității cibernetice a cărei înființare este prevăzută până în 2013, ale echipelor CERT și ale altor inițiative ale Comisiei, precum sistemul european de schimb de informații și de alertă, astfel încât să se asigure raportarea și schimbul de date sistematice privind atacurile cibernetice și alte forme de criminalitate cibernetică care afectează industria europeană și statele membre și astfel încât să se consolideze măsurile de asigurare a aplicării legii;

37. susține o legătură și o interacțiune strânse între sectoarele private naționale și ENISA pentru a se asigura interfața dintre echipele CERT naționale/guvernamentale și dezvoltarea sistemului european de alertă și schimb de informații (EISAS);

38. subliniază faptul că forța motrice primară din spatele dezvoltării și utilizării tehnologiilor destinate îmbunătățirii securității internetului este industria TIC; reamintește faptul că politicile UE trebuie să evite împiedicarea creșterii economiei europene bazate pe internet și să includă stimulentele necesare pentru a exploata în totalitate potențialul afacerilor și al parteneriatelor publice-private; recomandă examinarea altor stimulente pentru industrie în vederea dezvoltării de planuri de securitate mai solide pentru operatori, în conformitate cu Directiva 2008/114/CE;

39. solicită Comisiei să prezinte o propunere legislativă pentru o mai bună încadrare penală a atacurilor cibernetice ((adică practica „spear-phishing", frauda online etc.);

Cooperarea internațională

40. reamintește că procesul de cooperare internațională este instrumentul esențial pentru introducerea unor măsuri eficiente privind securitatea cibernetică; recunoaște că, în prezent, UE nu este implicată permanent în mod activ în procesele internaționale de cooperare și dialogurile cu privire la securitatea cibernetică; solicită Comisiei și Serviciului European de Acțiune Externă (SEAE) să înceapă un dialog constructiv cu toate țările care împărtășesc aceeași viziune în vederea dezvoltării unei înțelegeri și a unor politici comune, cu scopul de a spori reziliența internetului și a infrastructurii critice; susține că, în același timp, UE ar trebui să includă în permanență problemele privind securitatea internetului în sfera de aplicare a relațiilor sale externe, printre altele la crearea diverselor instrumente financiare sau la angajarea în acorduri internaționale care implică schimbul și stocarea de date sensibile;

41. ia act de realizările pozitive ale Convenției Consiliului Europei privind criminalitatea cibernetică, care a avut loc în 2001 în Budapesta; subliniază, totuși, că, în timp ce încurajează mai multe țări să semneze și să ratifice Convenția, SEAE ar trebui, de asemenea, să elaboreze acorduri bilaterale și multilaterale privind securitatea internetului și reziliența acestuia împreună cu parteneri internaționali care împărtășesc aceeași viziune;

42. evidențiază faptul că, pentru a evita dublarea unor acțiuni, este necesară coordonarea marelui număr de activități care sunt desfășurate în prezent de către diverse instituții, organisme și agenții internaționale și ale UE, precum și de către statele membre, în acest sens meritând să se aibă în vedere desemnarea unei persoane oficiale care să fie responsabile cu această coordonare, eventual prin numirea unui coordonator pentru securitatea cibernetică al UE;

43. subliniază importanța unui dialog structurat între principalii actori și legislatori din UE și din SUA implicați în activități legate de CIIP, pentru a asigura o viziune comună și pentru a stabili interpretări și poziții comune în ceea ce privește cadrul juridic și de guvernanță;

44. salută crearea, la Summitul UE-SUA din noiembrie 2010, a Grupului de lucru UE-SUA privind securitatea și infracționalitatea cibernetică și susține eforturile sale de a include problemele privind securitatea internetului în dialogul politic transatlantic; salută stabilirea în comun de Comisie și Guvernul SUA, în cadrul Grupului de lucru UE-SUA, a unui program comun și a unei foi de parcurs pentru realizarea de exerciții transcontinentale comune/sincronizate în domeniul securității și infracționalității cibernetice în 2012-2013;

45. sugerează stabilirea unui dialog structurat între legislatorii din UE și SUA pentru a discuta problemele legate de internet ca parte a unei cercetări pentru o înțelegere, interpretare și poziții comune;

46. solicită SEAE și Comisiei, pe baza lucrărilor desfășurate de forumul european al statelor membre, să garanteze o poziție activă în cadrul forumurilor internaționale de profil, printre altele prin coordonarea pozițiilor statelor membre, având în vedere promovarea valorilor, obiectivelor și politicilor esențiale ale UE în domeniul securității și rezilienței internetului; observă că aceste forumuri includ NATO, ONU (în special prin Uniunea Internațională a Telecomunicațiilor și Forumul pentru guvernarea internetului), Internet Corporation for Assigned Names and Numbers, Internet Assigned Numbers Authority, OSCE, OCDE și Banca Mondială;

47. încurajează Comisia și ENISA să participe la dialogurile dintre principalele părți interesate pentru a defini norme tehnice și juridice privind spațiul cibernetic la nivel internațional;

*

* *

48. încredințează Președintelui sarcina de a transmite prezenta rezoluție Consiliului și Comisiei.

Cooperarea în domeniul politicii energetice cu parteneri din afara frontierelor noastre

P7_TA(2012)0238

Rezoluția Parlamentului European din 12 iunie 2012 referitoare la angajarea în relații de cooperare în domeniul politicii energetice cu parteneri din afara frontierelor noastre: o abordare strategică privind aprovizionarea sigură, sustenabilă și competitivă cu energie (2012/2029(INI))

(2013/C 332 E/04)

Parlamentul European,

— având în vedere Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social și Comitetul Regiunilor privind securitatea aprovizionării cu energie și cooperarea internațională – „Politica energetică a UE: angajarea în relații cu parteneri din afara frontierelor noastre” (COM(2011)0539),

— având în vedere propunerea Comisiei de decizie a Parlamentului European și a Consiliului de instituire a unui mecanism de schimb de informații cu privire la acordurile interguvernamentale dintre statele membre și țări terțe în domeniul energiei (COM(2011)0540),

— având în vedere concluziile Consiliului din 24 noiembrie 2011 privind securitatea aprovizionării cu energie și cooperarea internațională – „Politica energetică a UE: angajarea în relații cu parteneri din afara frontierelor noastre”,

— având în vedere Rezoluția sa din 25 noiembrie 2010 intitulată „Către o nouă strategie energetică pentru Europa 2011-2020” ([1]),

— având în vedere articolul 48 din Regulamentul său de procedură,

— având în vedere raportul Comisiei pentru industrie, cercetare și energie și avizul Comisiei pentru afaceri externe, al Comisiei pentru dezvoltare și al Comisiei pentru comerț internațional (A7-0168/2012),

([1]) JO C 99 E, 3.4.2012, p. 64.