65. richiama l'attenzione sulla necessità di promuovere il volontariato, in particolare durante l'Anno europeo dei Cittadini nel 2013, e invita la Commissione a includere il sostegno al volontariato nelle politiche internazionali di aiuto allo sviluppo, in particolare al fine di conseguire tutti gli obiettivi previsti dagli Obiettivi di Sviluppo del Millennio;

66. è favorevole a un esame formale della proposta "Solidarietà" di programma interistituzionale in materia di risorse umane nelle istituzioni dell'UE per facilitare la partecipazione del personale e dei tirocinanti delle istituzioni alle attività di volontariato, umanitarie e sociali, in quanto parte della formazione del personale e delle attività di volontariato nel loro tempo libero;

67. sottolinea il fatto che il programma proposto proposto permette di ridurre i costi e rappresenta un considerevole valore aggiunto e contribuirebbe all'attuazione delle politiche e dei programmi dell'UE;

68. raccomanda alla Commissione di mantenere gli utili punti di contatto stabiliti sia con "EYV 2011 Alliance" e la piattaforma di volontariato subentrante, che includono molte organizzazioni di volontariato e network della società civile, sia con gli organi nazionali di coordinamento, partner strategici e portavoci dei governi nazionali in questo settore, data l'estrema varietà di servizi responsabili del volontariato nell'UE, e incoraggia questi punti di contatto a partecipare al portale europeo centralizzato proposto, quale piattaforma paneuropea, per facilitare l'ulteriore coordinamento e una maggiore attività transfrontaliera;

69. sottolinea l'importanza di queste reti di contatti e dello scambio delle migliori pratiche per diffondere le informazioni sui dispositivi esistenti in seno all'UE, in grado di aiutare e accompagnare i progetti di volontariato transfrontaliero;

70. invita la Commissione ad attivarsi, qualora lo ritenga opportuno, in relazione all'Agenda politica per il volontariato in Europa (PAVE), che è stata elaborata dalle organizzazioni di volontariato riunite in seno all'"Alleanza per l'anno europeo del volontariato 2011";

71. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione nonché ai governi e ai parlamenti degli Stati membri.

Infrastrutture critiche informatizzate: verso una sicurezza informatica mondiale

P7_TA(2012)0237

Risoluzione del Parlamento europeo del 12 giugno 2012 sulla protezione delle infrastrutture critiche informatizzate – realizzazioni e prossime tappe: verso una sicurezza informatica mondiale (2011/2284(INI))

(2013/C 332 E/03)

Il Parlamento europeo,

— vista la sua risoluzione del 5 maggio 2010 dal titolo "Una nuova Agenda digitale per l'Europa: 2015.eu" ([1]),

— vista la sua risoluzione del 15 giugno 2010 dal titolo "Governance di Internet: le prossime tappe ([2]),

— vista la sua risoluzione del 6 luglio 2011 dal titolo "La banda larga in Europa: investire nella crescita indotta dalla tecnologia digitale" ([3]),

— visto l'articolo 48 del suo regolamento,

— visti la relazione della commissione per l'industria, la ricerca e l'energia e il parere della commissione per le libertà civili, la giustizia e gli affari interni (A7-0167/2012),

([1]) GU C 81 E del 15.3.2011, pag. 45.
([2]) GU C 236 E del 12.8.2011, pag. 33.
([3]) Testi approvati, P7_TA(2011)0322.

A. considerando che le tecnologie dell'informazione e della comunicazione (TIC) sono in grado di fornire appieno il loro potenziale per favorire lo sviluppo dell'economia e della società solo se gli utenti hanno fiducia nella sicurezza e nella resilienza delle stesse e se la legislazione vigente in merito a questioni quali la riservatezza dei dati e i diritti di proprietà intellettuale è applicata efficacemente nell'ambiente Internet;

B. considerando che l'impatto di Internet e delle TIC sui diversi aspetti della vita dei cittadini sta aumentando rapidamente, e che essi rappresentano un motore fondamentale per l'interazione sociale, l'arricchimento culturale e la crescita economica;

C. considerando che la sicurezza delle TIC e di Internet costituisce un concetto ampio, che incide globalmente sugli aspetti economici, sociali, tecnologici e militari e richiede una chiara definizione e differenziazione delle responsabilità nonché un solido meccanismo di cooperazione internazionale;

D. considerando che l'obiettivo dell'iniziativa faro "Agenda digitale" dell'UE è rafforzare la competitività dell'Europa, sulla base del consolidamento delle TIC, e creare le condizioni per una crescita elevata e solida e per posti di lavoro basati sulla tecnologia;

E. considerando che il settore privato resta il principale investitore in prodotti, servizi, applicazioni e infrastrutture nel campo della sicurezza dell'informazione come pure il loro principale proprietario e gestore, con miliardi di euro di investimenti nell'ultimo decennio; che tale coinvolgimento dovrebbe essere rinsaldato mediante adeguate strategie politiche volte a promuovere la resilienza delle infrastrutture pubbliche, private, oppure di proprietà o in gestione pubblico-privata;

F. considerando che lo sviluppo di un alto livello di sicurezza e resilienza nelle reti, nei servizi e nelle tecnologie TIC dovrebbe accrescere la competitività dell'economia dell'Unione, sia migliorando l'analisi e la gestione del rischio cibernetico sia fornendo all'economia dell'UE in generale infrastrutture informatizzate più solide per promuovere l'innovazione e la crescita, creando nuove opportunità per permettere alle imprese di diventare più produttive;

G. considerando che i dati di carattere giudiziario disponibili relativi alla criminalità informatica (riguardanti gli attacchi cibernetici ma anche altri tipi di reati online) indicano un forte aumento di tali reati in diversi paesi europei; che tuttavia i dati statisticamente rappresentativi riguardanti gli attacchi cibernetici, forniti dalle forze dell'ordine e dalla comunità dei CERT (computer emergency response team), sono ancora limitati e in futuro sarà necessaria una loro migliore aggregazione, che consenta una reazione più efficace da parte delle forze dell'ordine dell'UE e risposte legislative maggiormente informate alle minacce informatiche in continua evoluzione;

H. considerando che un livello adeguato di sicurezza dell'informazione è di fondamentale importanza ai fini della solida espansione dei servizi basati su Internet;

I. considerando che i recenti incidenti informatici, le perturbazioni e gli attacchi ai danni delle infrastrutture informatizzate delle istituzioni, dell'industria e degli Stati membri dell'UE hanno evidenziato l'esigenza di creare un sistema solido, innovativo ed efficace per la protezione delle infrastrutture critiche informatizzate (CIIP) basato sulla piena cooperazione internazionale e su norme minime in materia di resilienza negli Stati membri;

J. considerando che, alla luce del rapido sviluppo delle nuove potenzialità delle TIC, come il *cloud computing*, è necessario prestare particolare attenzione alla sicurezza per poter trarre il massimo vantaggio dai benefici dell'avanzamento tecnologico;

K. considerando che il Parlamento europeo ha ripetutamente insistito sull'applicazione di norme elevate in materia di riservatezza e protezione dei dati, neutralità della rete e protezione dei diritti di proprietà intellettuale;

Misure atte a rafforzare la CIIP a livello nazionale e di Unione

1. valuta positivamente l'attuazione da parte degli Stati membri del programma europeo per la CIIP, compresa la creazione della rete informativa di allarme sulle infrastrutture critiche (CIWIN);

2. ritiene che gli sforzi volti a proteggere le infrastrutture critiche informatizzate non solo accresceranno la sicurezza complessiva dei cittadini, ma miglioreranno anche la percezione che essi hanno della sicurezza e la loro fiducia nelle misure adottate dal governo per proteggerli;

3. constata che la Commissione sta valutando di rivedere la direttiva 2008/114/CE [1] del Consiglio e chiede che vengano forniti dati circa l'efficacia e l'impatto di tale direttiva prima di intraprendere altre iniziative; chiede che venga considerata la possibilità di ampliare il suo ambito di applicazione, in particolare includendo il settore delle TIC e i servizi finanziari; chiede inoltre che si tenga conto di settori quali la sanità, i sistemi per l'approvvigionamento alimentare e idrico, la ricerca e l'industria nucleari (laddove questi non siano oggetto di disposizioni specifiche); ritiene che questi settori debbano altresì beneficiare dell'approccio intersettoriale adottato nell'ambito della CIWIN (basato sulla cooperazione, su un sistema di allarme e sullo scambio delle migliori prassi);

4. sottolinea l'importanza di creare e garantire un'integrazione durevole della ricerca europea per mantenere e potenziare l'eccellenza europea nel settore della CIIP;

5. chiede, in considerazione della natura interconnessa ed estremamente interdipendente, sensibile, strategica e vulnerabile delle infrastrutture critiche informatizzate nazionali ed europee, che venga effettuato un aggiornamento regolare delle norme minime in materia di resilienza per assicurare la preparazione e la capacità di reazione in caso di perturbazioni, incidenti, tentativi di distruzione o attacchi quali quelli risultanti da infrastrutture non sufficientemente solide o terminali non sufficientemente sicuri;

6. sottolinea l'importanza delle norme e dei protocolli di sicurezza dell'informazione e plaude al mandato conferito nel 2011 al CEN, al Cenelec e all'ETSI per l'istituzione di norme di sicurezza;

7. si attende che i proprietari e gli operatori delle infrastrutture critiche informatizzate consentano agli utenti di impiegare i mezzi appropriati per proteggersi da attacchi e/o interruzioni dolosi e li assistano mediante vigilanza umana e automatizzata, ove necessario;

8. sostiene la cooperazione a livello dell'Unione tra le parti interessate del settore pubblico e privato e ne incoraggia gli sforzi volti a definire e attuare norme in materia di sicurezza e resilienza per le infrastrutture critiche informatizzate civili nazionali ed europee (che siano pubbliche, private o miste);

9. sottolinea l'importanza di esercitazioni paneuropee per prepararsi ad incidenti di ampia portata che incidono sulla sicurezza delle reti, e della definizione di un'unica serie di criteri per valutare la minaccia;

10. chiede alla Commissione, in cooperazione con gli Stati membri, di valutare l'attuazione del piano d'azione CIIP; esorta gli Stati membri a istituire CERT nazionali o governativi efficienti, a sviluppare strategie nazionali in materia di sicurezza informatica, a organizzare esercitazioni periodiche di incidenti informatici a livello nazionale e paneuropeo, a elaborare piani di emergenza nazionali in caso di incidenti informatici e a contribuire all'elaborazione di un piano di emergenza europeo in caso di incidenti informatici entro la fine del 2012;

11. raccomanda che vengano disposti piani di sicurezza per gli operatori o misure equivalenti per tutte le infrastrutture critiche informatizzate europee e che vengano nominati funzionari di collegamento in materia di sicurezza;

12. accoglie con favore l'attuale revisione della decisione quadro 2005/222/GAI [2] del Consiglio relativa agli attacchi contro i sistemi di informazione; rileva la necessità di coordinare gli sforzi dell'UE nella lotta agli attacchi cibernetici su larga scala, attraverso l'inclusione delle competenze dell'ENISA, dei CERT degli Stati membri e del futuro CERT europeo;

13. ritiene che l'ENISA possa svolgere un ruolo cruciale a livello europeo per la protezione delle infrastrutture critiche informatizzate, mettendo a disposizione competenza tecnica agli Stati membri nonché alle istituzioni e agli organismi dell'Unione europea, oltre a relazioni e analisi concernenti la sicurezza dei sistemi d'informazione a livello europeo e globale;

Altre attività dell'UE per una solida sicurezza di Internet

14. esorta l'ENISA a coordinare e a mettere in atto, con cadenza annuale, mesi dedicati alla sensibilizzazione sulla sicurezza di Internet nell'UE, in modo che le questioni relative alla sicurezza informatica diventino oggetto di un'attenzione particolare da parte degli Stati membri e dei cittadini dell'Unione;

[1] GU L 345 del 23.12.2008, pag. 75.
[2] GU L 69 del 16.3.2005, pag. 67.

15. sostiene l'ENISA, in conformità con gli obiettivi dell'agenda digitale, nell'esercizio delle sue funzioni relative alla sicurezza delle reti d'informazione, in particolare attraverso la fornitura di orientamenti e consulenza agli Stati membri circa la modalità di sviluppo delle capacità di base dei propri CERT e il sostegno allo scambio delle migliori prassi mediante la promozione di un clima di fiducia; invita l'agenzia a consultare le parti interessate competenti al fine di individuare misure di sicurezza informatica simili per i proprietari e gli operatori delle reti e delle infrastrutture private, come pure ad assistere la Commissione e gli Stati membri nel contribuire allo sviluppo e alla diffusione di sistemi di certificazione della sicurezza dell'informazione, di norme comportamentali e di pratiche di cooperazione tra i CERT nazionali e quello europeo e i proprietari/operatori delle infrastrutture, ove necessario, attraverso la definizione di requisiti comuni minimi tecnologicamente neutrali;

16. accoglie con favore l'attuale proposta di rivedere il mandato dell'ENISA, in particolare la sua estensione, e di ampliare i compiti dell'agenzia; ritiene che l'ENISA, oltre a fornire assistenza agli Stati membri attraverso la fornitura di competenza e analisi, dovrebbe poter gestire diversi compiti esecutivi, sia a livello di UE sia in cooperazione con le rispettive controparti negli Stati Uniti, relativi alla prevenzione e al rilevamento di incidenti legati alla sicurezza delle reti e dell'informazione e volti a migliorare la cooperazione tra gli Stati membri; fa notare che, nel quadro del regolamento ENISA, all'agenzia potrebbero inoltre essere affidati compiti aggiuntivi inerenti alla risposta agli attacchi a Internet, in modo da apportare un chiaro valore aggiunto agli esistenti meccanismi di risposta nazionali;

17. accoglie con favore i risultati delle esercitazioni paneuropee per la sicurezza informatica del 2010 e 2011, condotte in tutta l'Unione e monitorate dall'ENISA, il cui obiettivo era assistere gli Stati membri nella progettazione, nel mantenimento e nella verifica di un piano di emergenza paneuropeo; invita l'ENISA a mantenere tali esercitazioni nel suo programma e, se del caso, a coinvolgere progressivamente i relativi operatori privati, al fine di accrescere le capacità complessive europee in termini di sicurezza di Internet; auspica un ulteriore ampliamento internazionale con partner che condividono lo stesso approccio;

18. invita gli Stati membri a elaborare piani di emergenza nazionali in caso di incidenti informatici e a prevedere elementi chiave, quali punti di contatto pertinenti, la fornitura di assistenza, il contenimento e la riparazione in caso di perturbazioni o attacchi informatici di portata regionale, nazionale o transfrontaliera; osserva che gli Stati membri dovrebbero inoltre sviluppare adeguati meccanismi e strutture di coordinamento a livello nazionale volti a garantire un migliore coordinamento tra le autorità nazionali competenti e a rendere le loro azioni più coerenti;

19. suggerisce che la Commissione proponga, attraverso il piano di emergenza UE in caso di incidenti informatici, misure vincolanti finalizzate a un migliore coordinamento a livello di UE delle funzioni tecniche e di comando dei CERT nazionali e governativi;

20. invita la Commissione e gli Stati membri ad adottare le misure necessarie al fine di proteggere le infrastrutture critiche da attacchi cibernetici e a fornire le modalità per bloccare ermeticamente l'accesso a un'infrastruttura critica nel caso in cui un attacco cibernetico diretto ne minacci gravemente il corretto funzionamento;

21. auspica una piena attuazione del CERT dell'UE, che rappresenterà un fattore fondamentale per la prevenzione e il rilevamento di attacchi cibernetici intenzionali e dolosi nei confronti delle istituzioni dell'UE, la risposta ad essi e la successiva ripresa;

22. raccomanda alla Commissione di proporre misure vincolanti volte a imporre norme minime in materia di sicurezza e resilienza e a migliorare il coordinamento tra i CERT nazionali;

23. invita gli Stati membri e le istituzioni dell'UE a garantire l'esistenza di CERT efficienti, caratterizzati da capacità di sicurezza e di resilienza minime basate sulle migliori prassi concordate; sottolinea che i CERT nazionali dovrebbero far parte di una rete efficace, all'interno della quale lo scambio di informazioni avviene in conformità delle necessarie norme di riservatezza; chiede l'istituzione di un servizio CIIP sempre attivo per tutti gli Stati membri, nonché la definizione di un protocollo di emergenza comune europeo applicabile tra i punti di contatto nazionali;

24. sottolinea che la creazione di un clima di fiducia e la promozione della cooperazione tra gli Stati membri è fondamentale per proteggere i dati, le reti e le infrastrutture nazionali; invita la Commissione a suggerire una procedura comune per l'individuazione e l'elaborazione di un approccio congiunto volto ad affrontare le minacce alle TIC di portata transfrontaliera, tenendo conto del fatto che gli Stati membri dovrebbero fornire alla Commissione informazioni generali concernenti i rischi e le minacce per le loro infrastrutture critiche informatizzate nonché le vulnerabilità delle stesse;

25. plaude all'iniziativa della Commissione tesa a sviluppare entro il 2013 un sistema europeo di condivisione delle informazioni e di allarme;

26. valuta positivamente le varie consultazioni con le parti interessate avviate dalla Commissione in merito alla sicurezza di Internet e alla CIIP, quale il partenariato pubblico-privato europeo per la resilienza; riconosce il già significativo coinvolgimento e l'impegno dei fornitori delle TIC in tali attività ed esorta la Commissione a compiere ulteriori sforzi per incoraggiare il mondo accademico e le associazioni degli utenti delle TIC a svolgere un ruolo più attivo, nonché a promuovere un dialogo costruttivo tra le parti interessate sulle questioni riguardanti la sicurezza informatica; sostiene un ulteriore sviluppo dell'assemblea sul digitale quale quadro per la gestione della CIIP;

27. si compiace del lavoro compiuto finora dal Forum europeo degli Stati membri per quanto concerne la definizione di criteri specifici del settore volti a individuare le infrastrutture critiche europee, con particolare riguardo alle comunicazioni fisse e mobili, nonché l'esame dei principi e delle linee guida dell'UE per la resilienza e la stabilità di Internet; auspica che si prosegua con la formazione del consenso negli Stati membri e, a tale proposito, incoraggia il Forum a integrare nell'approccio attuale, basato su infrastrutture materiali, sforzi volti a includere anche elementi infrastrutturali logici, i quali, con lo sviluppo della virtualizzazione e delle tecnologie *cloud*, acquisiranno un'importanza crescente per l'efficacia della CIIP;

28. suggerisce che la Commissione lanci un'iniziativa educativa pubblica paneuropea, volta a educare e sensibilizzare gli utenti finali privati e le imprese sulle possibili minacce a Internet e alle apparecchiature fisse e mobili delle TIC a ogni livello della filiera e a promuovere comportamenti più sicuri da parte dei singoli durante le attività online; rammenta a tale proposito i rischi legati ad attrezzature informatiche e software obsoleti;

29. invita gli Stati membri, con il sostegno della Commissione, a consolidare i programmi di istruzione e formazione sulla sicurezza dell'informazione, destinati alle autorità di polizia e giudiziarie nazionali e alle pertinenti agenzie dell'UE;

30. sostiene la creazione di un curriculum UE per gli esperti accademici nel settore della sicurezza dell'informazione, in quanto ciò avrebbe un impatto positivo sulla competenza e sulla preparazione dell'Unione alla luce della continua evoluzione del ciberspazio e delle minacce nei suoi confronti;

31. auspica la promozione dell'istruzione sulla sicurezza informatica (tirocini per dottorandi, corsi universitari, laboratori, formazione per studenti, ecc…) e delle attività di formazione specializzata in materia di CIIP;

32. invita la Commissione a proporre, entro la fine del 2012, una strategia globale dell'UE per la sicurezza di Internet basata su una terminologia chiara; è del parere che l'obiettivo della strategia per la sicurezza di Internet debba essere quello di creare un ciberspazio (sostenuto da un'infrastruttura sicura e resiliente e da norme aperte) che favorisca l'innovazione e la prosperità attraverso il libero flusso di informazioni e garantisca contestualmente una solida protezione della vita privata e delle altre libertà civili; ritiene che la strategia debba riportare in dettaglio i principi, gli obiettivi, i metodi, gli strumenti e le politiche (sia interni sia esterni) necessari a ottimizzare gli sforzi a livello nazionale e di UE, e stabilire norme minime di resilienza tra gli Stati membri, al fine di garantire un servizio sicuro, continuo, solido e resiliente, con riferimento sia alle infrastrutture critiche sia a un uso generico di Internet;

33. sottolinea che la prossima strategia per la sicurezza di Internet della Commissione dovrebbe prendere il lavoro sulla CIIP quale punto centrale di riferimento e mirare a un approccio olistico e sistematico finalizzato alla sicurezza informatica, includendo sia misure proattive, quali l'introduzione di norme minime per le misure di sicurezza o la formazione di singoli utenti, imprese e istituzioni pubbliche, sia misure reattive, quali sanzioni penali, civili e amministrative;

34. invita la Commissione a proporre un solido meccanismo atto a coordinare l'attuazione e il regolare aggiornamento della strategia per la sicurezza di Internet; ritiene che tale meccanismo debba essere sostenuto da sufficienti risorse amministrative, tematiche e finanziarie e che il suo compito debba essere quello di agevolare la definizione della posizione dell'UE nei confronti delle parti interessate interne e internazionali sulle questioni relative alla sicurezza di Internet;

35. invita la Commissione a proporre un quadro UE per la comunicazione delle violazioni della sicurezza nei settori critici quali quello dell'energia, dei trasporti, dell'approvvigionamento alimentare e idrico nonché delle TIC e dei servizi finanziari, al fine di garantire che le autorità pertinenti degli Stati membri e gli utenti siano informati su incidenti, attacchi e perturbazioni di natura cibernetica;

36. invita la Commissione a migliorare la disponibilità di dati statisticamente rappresentativi riguardanti i costi degli attacchi cibernetici nell'UE, negli Stati membri e nell'industria (in particolare nei settori dei servizi finanziari e delle TIC) accrescendo le capacità di raccolta dati del futuro centro europeo per la criminalità informatica (la cui istituzione è prevista entro il 2013), dei CERT e di altre iniziative della Commissione, quale il sistema europeo di condivisione delle informazioni e di allarme, in modo da garantire la comunicazione e condivisione sistematica dei dati relativi agli attacchi cibernetici e ad altre forme di criminalità informatica di cui sono vittime l'industria europea e gli Stati membri e assicurare una più efficace applicazione della legge;

37. auspica un rapporto e un'interazione stretti tra i settori privati nazionali e l'ENISA per interfacciare i CERT nazionali/governativi con lo sviluppo del sistema europeo di condivisione delle informazioni e di allarme (EISAS);

38. precisa che il principale fattore trainante dello sviluppo e dell'uso delle tecnologie progettate per incrementare la sicurezza di Internet è rappresentato dal settore delle TIC; ricorda che le politiche dell'Unione devono evitare di ostacolare la crescita dell'economia europea basata su Internet e includere gli incentivi necessari al fine di sfruttare al massimo le potenzialità delle imprese e dei partenariati pubblico-privato; raccomanda di individuare ulteriori incentivi destinati all'industria per l'elaborazione di piani più solidi per la sicurezza degli operatori, conformemente a quanto previsto dalla direttiva 2008/114/CE;

39. invita la Commissione a presentare una proposta legislativa per criminalizzare ulteriormente gli attacchi cibernetici ((*spear phishing*, frodi online, ecc.);

Cooperazione internazionale

40. ricorda che la cooperazione internazionale costituisce lo strumento principale per introdurre misure efficaci per la sicurezza informatica; riconosce che attualmente l'UE non è coinvolta attivamente, su base continuativa, in dialoghi e processi di cooperazione internazionale relativi alla sicurezza informatica; invita la Commissione e il Servizio europeo per l'azione esterna (SEAE) ad avviare un dialogo costruttivo con tutti i paesi che condividono la stessa visione, al fine di sviluppare un approccio e politiche comuni volti a migliorare la resilienza di Internet e delle infrastrutture critiche; sostiene che, allo stesso tempo, l'UE dovrebbe includere, su base permanente, le questioni legate alla sicurezza di Internet nel quadro delle sue relazioni esterne, anche nel corso dell'elaborazione dei vari strumenti finanziari o nel momento in cui si impegna in accordi internazionali che prevedono lo scambio e la conservazione di dati sensibili;

41. prende atto degli esiti positivi della convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest nel 2001; sottolinea, tuttavia, che il SEAE dovrebbe incoraggiare un maggior numero di paesi a sottoscrivere e ratificare la convenzione e, contestualmente, redigere accordi bilaterali e multilaterali in materia di sicurezza di Internet e resilienza con partner internazionali che condividono la stessa visione;

42. rileva che il vasto numero di attività in corso svolte da diverse istituzioni, organismi e agenzie internazionali e dell'UE, così come dagli Stati membri, richiede un coordinamento allo scopo di evitare duplicazioni, motivo per cui è opportuno considerare la designazione di un funzionario responsabile per il coordinamento, possibilmente attraverso la nomina di un coordinatore della sicurezza informatica dell'UE;

43. sottolinea che il dialogo strutturato tra i principali operatori e legislatori dell'UE e degli Stati Uniti coinvolti nella protezione delle infrastrutture critiche informatizzate riveste una particolare importanza ai fini della comprensione comune e interpretazioni e posizioni comuni in materia di quadri giuridici e di governance;

44. valuta positivamente la creazione, in occasione del vertice Unione europea-Stati Uniti del novembre 2010, del gruppo di lavoro UE-USA sulla sicurezza informatica e sui reati informatici e sostiene i suoi sforzi volti a includere le questioni concernenti la sicurezza di Internet nel dialogo politico transatlantico; accoglie con favore la creazione congiunta da parte della Commissione e del governo USA, sotto l'egida del gruppo di lavoro UE-USA, di un programma e una tabella di marcia comuni relativi all'organizzazione nel 2012/2013 di esercitazioni transcontinentali comuni/sincronizzate nel settore della sicurezza informatica;

45. suggerisce di stabilire un dialogo strutturato tra i legislatori dell'UE e degli Stati Uniti, al fine di esaminare le questioni legate a Internet nell'ambito della ricerca di un approccio, di un'interpretazione e di posizioni comuni;

46. sollecita il SEAE e la Commissione, sulla base del lavoro svolto dal Forum europeo degli Stati membri, a svolgere un ruolo attivo nell'ambito dei consessi internazionali pertinenti, in particolare coordinando le posizioni degli Stati membri, con l'intento di promuovere i valori fondamentali, gli obiettivi e le politiche dell'UE nel settore della sicurezza di Internet e della resilienza; osserva che tra tali consessi si annoverano la NATO, l'ONU (in particolare attraverso l'Unione internazionale delle telecomunicazioni e il Forum sulla governance di Internet), la Corporazione Internet per i nomi e i numeri assegnati, l'Autorità per l'assegnazione dei numeri per Internet, l'OSCE, l'OCSE e la Banca mondiale;

47. incoraggia la Commissione e l'ENISA a partecipare ai principali dialoghi con le parti interessate, al fine di individuare disposizioni tecniche e giuridiche sul ciberspazio a livello internazionale;

*

* *

48. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione.

Cooperazione in materia di politica energetica con i partner al di là delle nostre frontiere

P7_TA(2012)0238

Risoluzione del Parlamento europeo del 12 giugno 2012 sull'impegno nella cooperazione nel settore della politica energetica con i partner al di là delle nostre frontiere: un approccio strategico per un approvvigionamento energetico sicuro, sostenibile e competitivo (2012/2029(INI))

(2013/C 332 E/04)

Il Parlamento europeo,

— vista la comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla sicurezza dell'approvvigionamento energetico e la cooperazione internazionale – "La politica energetica dell'UE: un impegno con i partner al di là delle nostre frontiere"(COM(2011)0539),

— vista la proposta della Commissione di decisione del Parlamento europeo e del Consiglio che istituisce un meccanismo per lo scambio di informazioni riguardo ad accordi intergovernativi fra gli Stati membri e i paesi terzi nel settore dell'energia (COM (2011)0540),

— viste le conclusioni del Consiglio del 24 novembre 2011 sulla sicurezza dell'approvvigionamento energetico e la cooperazione internazionale – "La politica energetica dell'UE: un impegno con i partner al di là delle nostre frontiere",

— vista la sua risoluzione del 25 novembre 2010 intitolata "Verso una nuova strategia energetica per l'Europa 2011-2020" ([1]),

— visto l'articolo 48 del suo regolamento,

— visti la relazione della commissione per l'industria, la ricerca e l'energia e i pareri della commissione per gli affari esteri, della commissione per lo sviluppo e della commissione per il commercio internazionale (A7-0168/2012),

([1]) GU C 99 E del 3.4.2012, pag. 64.