65. upozorňuje na to, že je potrebné podporovať dobrovoľníctvo, a to najmä počas Európskeho roku občanov, ktorým bude rok 2013, a vyzýva Komisiu, aby podporu dobrovoľníctva zahrnula do politík medzinárodnej rozvojovej pomoci, a to okrem iného aj s cieľom splniť všetky ciele stanovené v miléniových rozvojových cieľoch;

66. podporuje formálne preskúmanie návrhu Solidarité na medziinštitucionálny program zdrojov v inštitúciách EÚ s cieľom uľahčiť zapojenie zamestnancov a stážistov do dobrovoľníckych, humanitárnych a sociálnych činností či už v rámci odbornej prípravy zamestnancov alebo v rámci dobrovoľníckej činnosti v ich voľnom čase;

67. zdôrazňuje skutočnosť, že navrhovaný program šetrí náklady a prináša pridanú hodnotu a pomohol by uskutočňovať politiky a programy EÚ;

68. odporúča, aby Komisia zachovala užitočné kontaktné miesta vytvorené jednak v rámci EYV 2011 Alliance a nadväzujúcej dobrovoľníckej platformy, ktorá spája mnoho dobrovoľných organizácií a sietí občianskej spoločnosti, ako aj vnútroštátnymi koordinačnými orgánmi, strategickými partnermi a hovorcami vnútroštátnych vlád v tejto oblasti, vzhľadom na širokú škálu subjektov zainteresovaných v oblasti dobrovoľníctva v rámci EÚ, a nabáda, aby tieto kontaktné miesta pracovali s navrhovaným centralizovaným portálom EÚ ako celoeurópskou platformou s cieľom uľahčiť ďalšiu koordináciu a zvýšenú cezhraničnú činnosť;

69. zdôrazňuje, aké sú dôležité kontaktné siete a výmena osvedčených postupov s cieľom šíriť informácie o existujúcich postupoch EÚ, ktoré môžu pomôcť cezhraničnému dobrovoľníctvu;

70. žiada Európsku komisiu aby v prípade potreby prijala opatrenia týkajúce sa politického programu dobrovoľníckej práce v Európe, ktorý bol vypracovaný dobrovoľníckymi organizáciami združenými v Aliancii pre Európsky rok dobrovoľníckej práce 2011;

71. poveruje svojho predsedu, aby postúpil toto uznesenie Rade, Komisii a vládam a parlamentom členských štátov.

Ochrana kritických informačných infraštruktúr – Dosiahnuté ciele a ďalšie kroky: na ceste ku globálnej kybernetickej bezpečnosti

P7_TA(2012)0237

Uznesenie Európskeho parlamentu z 12. júna 2012 o ochrane kritických informačných infraštruktúr – Dosiahnuté ciele a ďalšie kroky: na ceste ku globálnej kybernetickej bezpečnosti (2011/2284(INI))

(2013/C 332 E/03)

Európsky parlament,

— so zreteľom na svoje uznesenie z 5. mája 2010 s názvom Nová digitálna agenda pre Európu: 2015.eu ([1]),

— so zreteľom na svoje uznesenie z 15. júna 2010 s názvom Správa internetu: ďalšie kroky ([2]),

— so zreteľom na svoje uznesenie zo 6. júla 2011 s názvom Širokopásmové pripojenie v Európe: investície do digitálne riadeného rastu ([3]),

— so zreteľom na článok 48 rokovacieho poriadku,

— so zreteľom na správu Výboru pre priemysel, výskum a energetiku a stanovisko Výboru pre občianske slobody, spravodlivosť a vnútorné veci (A7-0167/2012),

([1]) Ú. v. EÚ C 81 E, 15.3.2011, s. 45.
([2]) Ú. v. EÚ C 236 E, 12.8.2011, s. 33.
([3]) Prijaté texty, P7_TA(2011)0322.

A. keďže informačné a komunikačné technológie (IKT) môžu naplno využiť svoju kapacitu na zaistenie pokroku hospodárstva a spoločnosti len vtedy, ak používatelia dôverujú v ich bezpečnosť a odolnosť a ak sa v internetovom prostredí účinne presadzujú právne predpisy týkajúce sa oblastí, ako sú ochrana osobných údajov a práva duševného vlastníctva;

B. keďže vplyv internetu a IKT na rôzne aspekty života občanov sa rýchlo zvyšuje a keďže internet a IKT sú kľúčovými hybnými silami sociálnej integrácie, kultúrneho obohatenia a hospodárskeho rastu;

C. keďže bezpečnosť IKT a internetu predstavuje komplexnú koncepciu, ktorá sa v celosvetovom meradle prejavuje v hospodárskych, sociálnych, technologických a vojenských aspektoch a vyžaduje si zreteľné vymedzenie a rozlíšenie zodpovednosti, ako aj stabilné mechanizmy medzinárodnej spolupráce;

D. keďže hlavným cieľom digitálnej agendy EÚ je zvýšenie konkurencieschopnosti Európy na základe posilnenia IKT a vytvorenie podmienok pre výrazný a silný rast a pracovné miesta založené na technológiách;

E. keďže pokiaľ ide o produkty, služby, aplikácie a infraštruktúru v oblasti bezpečnosti informácií, hlavným investorom, vlastníkom a manažérom naďalej ostáva súkromný sektor, ktorý za posledné desaťročie investoval miliardy eur; keďže toto zapojenie by sa malo posilniť primeranými politickými stratégiami na podporu odolnosti infraštruktúr vo verejnom, súkromnom alebo verejno-súkromnom vlastníctve či prevádzke;

F. keďže vytvorením vysokej úrovne bezpečnosti a odolnosti informačných a komunikačných sietí, služieb a technológií by sa mala zvýšiť konkurencieschopnosť hospodárstva EÚ, a to prostredníctvom zlepšenia posudzovania a riadenia kybernetických rizík, ako aj zabezpečenia stabilnejšej informačnej infraštruktúry pre celé hospodárstvo EÚ v záujme podpory inovácie a rastu, čím sa vytvoria nové príležitosti na zvýšenie produktivity podnikov;

G. keďže dostupné údaje pri presadzovaní práva týkajúce sa počítačovej kriminality (zahŕňajúce kybernetické útoky, ako aj ďalšie druhy internetovej trestnej činnosti) vykazujú v jednotlivých európskych krajinách prudký nárast; keďže orgány presadzovania práva a tímy reakcie na núdzové počítačové situácie (CERT) neposkytujú však v dostatočnej miere štatisticky reprezentatívne údaje týkajúce sa kybernetických útokov a tieto údaje sa budú musieť v budúcnosti lepšie zhromažďovať, čo umožní ráznejšiu reakciu orgánov presadzovania práva v celej EÚ a legislatívnu reakciu na stále sa vyvíjajúce kybernetické hrozby vychádzajúcu z relevantnejších informácií;

H. keďže primeraná úroveň bezpečnosti informácií má zásadný význam pre rozsiahle rozšírenie služieb poskytovaných prostredníctvom internetu;

I. keďže nedávne kybernetické incidenty, narušenia a útoky na informačné infraštruktúry inštitúcií EÚ, priemyslu a členských štátov dokazujú potrebu zaviesť stabilný, inovačný a účinný systém ochrany kritických informačných infraštruktúr (CIIP), ktorý bude založený na úplnej medzinárodnej spolupráci a normách minimálnej odolnosti platných v členských štátoch;

J. keďže prudký rozvoj nových prvkov v oblasti IKT, ako je výpočtové mračno (cloud computing), si vyžaduje silné zameranie na bezpečnosť v záujme úplného využitia prínosu technologických výdobytkov;

K. keďže Európsky parlament opakovane nástojil na uplatňovaní prísnych noriem v oblasti ochrany súkromia a údajov, neutrality siete a ochrany práv duševného vlastníctva;

Opatrenia na posilnenie ochrany kritických informačných infraštruktúr (CIIP) na vnútroštátnej úrovni a na úrovni Únie

1. víta skutočnosť, že členské štáty vykonávajú európsky program na ochranu kritických informačných infraštruktúr a že vytvorili varovnú informačnú sieť kritickej infraštruktúry (CIWIN);

2. domnieva sa, že úsilie o ochranu kritických informačných infraštruktúr nielen zvýši celkovú bezpečnosť občanov, ale aj zlepší ich vnímanie bezpečnosti a ich dôveru v opatrenia, ktoré vláda prijíma na ich ochranu;

Utorok 12. júna 2012

3. berie na vedomie, že Komisia uvažuje o revízii smernice Rady 2008/114/ES ([1]), a žiada poskytnutie dôkazov o účinnosti a vplyve smernice pred prijatím ďalších opatrení; požaduje, aby sa zvážilo rozšírenie jej rozsahu pôsobnosti, najmä o sektor IKT a finančné služby; okrem toho žiada, aby sa zohľadnili oblasti, ako sú zdravotníctvo, systémy dodávok potravín a vody, jadrový výskum a priemysel (pokiaľ sa na ne nevzťahujú osobitné ustanovenia); domnieva sa, že tieto odvetvia by mali mať tiež prospech z medziodvetvového prístupu, ktorý sa prijal v rámci siete CIWIN a pozostáva zo spolupráce, varovného systému a výmeny najlepších postupov;

4. zdôrazňuje, že pre zachovanie a posilnenie jedinečných európskych kvalít v oblasti ochrany kritických informačných infraštruktúr je dôležité zaviesť a zabezpečiť trvalú integráciu európskeho výskumu;

5. žiada, aby sa vzhľadom na vzájomne prepojenú a do veľkej miery vzájomne závislú, citlivú, strategickú a zraniteľnú povahu kritických informačných infraštruktúr na vnútroštátnej úrovni a na úrovni EÚ pravidelne aktualizovali minimálne normy odolnosti v oblasti pripravenosti a reakcie na akékoľvek narušenia, incidenty, pokusy o útoky alebo útoky, ako sú útoky vyplývajúce z nedostatočnej stability infraštruktúry alebo nedostatočného zabezpečenia koncových zariadení;

6. zdôrazňuje význam noriem a protokolov pre bezpečnosť informácií a víta skutočnosť, že v roku 2011 bol vypracovaním bezpečnostných noriem poverený Európsky výbor pre normalizáciu (CEN), Európsky výbor pre normalizáciu v elektrotechnike (Cenelec) a Európsky inštitút pre telekomunikačné normy (ETSI);

7. očakáva, že vlastníci a prevádzkovatelia kritických informačných infraštruktúr umožnia používateľom využívať primerané prostriedky ochrany pred škodlivými útokmi a/alebo narušeniami prostredníctvom ľudského a podľa potreby automatizovaného dohľadu a v prípade potreby im poskytnú pomoc;

8. vyjadruje podporu spolupráci medzi verejnými a súkromnými zainteresovanými stranami na úrovni Únie a ich úsiliu o rozvoj a uplatňovanie noriem bezpečnosti a odolnosti v rámci civilných – či už verejných, súkromných alebo verejno-súkromných – vnútroštátnych a európskych kritických informačných infraštruktúr;

9. zdôrazňuje význam celoeurópskych cvičných simulácií v rámci prípravy na rozsiahle bezpečnostné sieťové incidenty a význam vymedzenia jednotného súboru noriem v oblasti posudzovania hrozieb;

10. vyzýva Komisiu, aby v spolupráci s členskými štátmi posúdila realizáciu akčného plánu ochrany kritických informačných infraštruktúr; naliehavo vyzýva členské štáty, aby zriadili dobre fungujúce vnútroštátne/vládne tímy reakcie na núdzové počítačové situácie, vypracovali národné stratégie kybernetickej bezpečnosti, organizovali pravidelné vnútroštátne a celoeurópske cvičné simulácie kybernetických incidentov, vypracovali vnútroštátne pohotovostné plány pre prípady kybernetických incidentov a do konca roku 2012 prispeli k rozvoju európskeho pohotovostného plánu pre prípady kybernetických incidentov;

11. odporúča, aby sa zaviedli do praxe bezpečnostné plány prevádzkovateľa alebo rovnocenné opatrenia pre všetky európske kritické informačné infraštruktúry a aby boli vymenovaní bezpečnostní styční úradníci;

12. víta súčasnú revíziu rámcového rozhodnutia Rady 2005/222/SVV ([2]) o útokoch na informačné systémy; poznamenáva, že je potrebné koordinovať úsilie EÚ v boji proti rozsiahlym kybernetickým útokom prostredníctvom zapojenia Európskej agentúry pre bezpečnosť sietí a informácií (ENISA), tímov reakcie na núdzové počítačové situácie pôsobiacich v jednotlivých členských štátoch a kompetencií budúceho európskeho tímu CERT;

13. domnieva sa, že agentúra ENISA môže na európskej úrovni zohrávať kľúčovú úlohu v oblasti ochrany kritických informačných infraštruktúr tým, že členským štátom a inštitúciám a orgánom Európskej únie poskytne technické odborné znalosti, ako aj správy a analýzy o bezpečnosti informačných systémov na európskej a celosvetovej úrovni;

Ďalšie opatrenia EÚ na zaistenie odolnej internetovej bezpečnosti

14. naliehavo vyzýva Európsku agentúru pre bezpečnosť sietí a informácií (ENISA), aby každý rok koordinovala a vykonávala Európsky mesiac informovanosti o internetovej bezpečnosti, aby sa tak otázky týkajúce sa kybernetickej bezpečnosti stali predmetom osobitnej pozornosti členských štátov a občanov EÚ;

([1]) Ú. v. EÚ L 345, 23.12.2008, s. 75.
([2]) Ú. v. EÚ L 69, 16.3.2005, s. 67.

15. v súlade s cieľmi digitálnej agendy podporuje agentúru ENISA pri plnení povinností v oblasti sieťovej a informačnej bezpečnosti, predovšetkým poskytovaním usmernení a rád členským štátom, pokiaľ ide o spôsob dosiahnutia základných zručností ich tímov CERT, ako aj prostredníctvom podpory výmeny najlepších postupov vytváraním ovzdušia dôvery; vyzýva agentúru ENISA, aby konzultovala s príslušnými zainteresovanými stranami s cieľom vymedziť podobné opatrenia v oblasti kybernetickej bezpečnosti pre vlastníkov/prevádzkovateľov súkromných sietí a infraštruktúr a aby pomohla Komisii a členským štátom a prispela k vytváraniu a zavádzaniu systémov certifikácie informačnej bezpečnosti, noriem správania a postupov spolupráce medzi vnútroštátnymi a európskymi tímami CERT a vlastníkmi a prevádzkovateľmi infraštruktúr vždy a všade, kde je to potrebné, prostredníctvom vymedzenia technologicky neutrálnych spoločných minimálnych požiadaviek;

16. víta súčasný návrh na revíziu mandátu agentúry ENISA, predovšetkým pokiaľ ide o jeho rozsah a rozšírenie úloh agentúry; domnieva sa, že agentúra ENISA by okrem poskytovania pomoci členským štátom prostredníctvom odborných poznatkov a analýz mala byť poverená aj plnením viacerých exekutívnych úloh na úrovni EÚ a v spolupráci s príslušnými partnermi v USA úlohami, ktoré sa budú týkať prevencie a zisťovania incidentov v oblasti sieťovej a informačnej bezpečnosti a posilňovania spolupráce medzi členskými štátmi; zdôrazňuje, že podľa nariadenia o agentúre ENISA je tiež možné prideliť jej ďalšie povinnosti súvisiace s reakciou na internetové útoky do takej miery, aby priniesla zreteľnú pridanú hodnotu pre súčasné vnútroštátne mechanizmy reakcie;

17. víta výsledky celoeurópskej cvičnej simulácie v oblasti kybernetickej bezpečnosti, ktorá sa uskutočnila v rokoch 2010 a 2011 v celej Európskej únii pod dohľadom agentúry ENISA a ktorej cieľom bolo pomôcť členským štátom pri príprave, dodržiavaní a testovaní celoeurópskeho pohotovostného plánu; vyzýva agentúru ENISA, aby ponechala takéto cvičné simulácie vo svojom programe a postupne do nich podľa potreby zapájala príslušných súkromných prevádzkovateľov s cieľom zvýšiť celkové kapacity internetovej bezpečnosti v Európe; očakáva ďalšie medzinárodné rozšírenie s podobne uvažujúcimi partnermi;

18. vyzýva členské štáty, aby vypracovali vnútroštátne pohotovostné plány pre prípady kybernetických incidentov a aby do nich zahrnuli kľúčové prvky, ako sú príslušné kontaktné miesta a ustanovenia týkajúce sa pomoci, izolácie a opravy v prípade kybernetických narušení alebo útokov s regionálnym, vnútroštátnym alebo cezhraničným významom; poznamenáva, že členské štáty by mali tiež zaviesť primerané koordinačné mechanizmy a štruktúry na vnútroštátnej úrovni, ktoré by pomohli zaistiť lepšiu koordináciu medzi príslušnými vnútroštátnymi orgánmi a zabezpečiť väčšiu súdržnosť ich činností;

19. navrhuje, aby Komisia v rámci pohotovostného plánu EÚ pre prípady kybernetických incidentov predložila záväzné opatrenia na dosiahnutie lepšej koordinácie technických a riadiacich funkcií na úrovni EÚ medzi vnútroštátnymi a vládnymi tímami CERT;

20. vyzýva Komisiu a členské štáty, aby prijali potrebné opatrenia na ochranu kritickej infraštruktúry pred kybernetickými útokmi a zabezpečili prostriedky na uzatvorenie prístupu ku kritickej infraštruktúre v prípade, že priamy kybernetický útok výrazne ohrozuje jej riadne fungovanie;

21. očakáva úplné vytvorenie tímu CERT na úrovni EÚ, ktorý sa stane hlavným činiteľom v oblasti prevencie a zisťovania úmyselných a škodlivých kybernetických útokov zameraných na inštitúcie EÚ, reakcie na ne a obnovy po takýchto útokoch;

22. odporúča, aby Komisia navrhla záväzné opatrenia zamerané na zavedenie minimálnych noriem bezpečnosti a odolnosti a zlepšenie koordinácie medzi vnútroštátnymi tímami reakcie na núdzové počítačové situácie;

23. vyzýva členské štáty a inštitúcie EÚ, aby zabezpečili existenciu riadne fungujúcich tímov CERT s požadovanou minimálnou úrovňou spôsobilosti v oblasti bezpečnosti a odolnosti na základe schválených najlepších postupov; zdôrazňuje, že vnútroštátne tímy CERT by sa mali stať súčasťou efektívnej siete, v ktorej sa budú vymieňať relevantné informácie v súlade s nevyhnutnými normami dôvernosti; požaduje zriadenie nepretržitej prevádzky služby ochrany kritických informačných infraštruktúr pre jednotlivé členské štáty, ako aj ustanovenie spoločného európskeho núdzového protokolu, ktorý by sa uplatňoval medzi kontaktnými miestami jednotlivých členských štátov;

24. zdôrazňuje, že budovanie dôvery a podpora spolupráce medzi členskými štátmi má zásadný význam pre ochranu údajov a vnútroštátnych sietí a infraštruktúr; vyzýva Komisiu, aby navrhla spoločný postup identifikácie a určenia spoločného prístupu k riešeniu cezhraničných hrozieb v oblasti IKT, a očakáva, že členské štáty poskytnú Komisii všeobecné informácie o rizikách, hrozbách a zraniteľných miestach svojich kritických informačných infraštruktúr;

Utorok 12. júna 2012

25. víta iniciatívu Komisie na rozvoj Európskeho systému výmeny informácií a varovania (EISAS) do roku 2013;

26. víta konzultácie s rôznymi zainteresovanými stranami o internetovej bezpečnosti a CIIP, ktoré sa začali na podnet Komisie, napríklad Európske verejno-súkromné partnerstvo pre odolnosť; uznáva doterajšie významné zapojenie a aktivitu dodávateľov v oblasti IKT v rámci tejto snahy a podporuje Komisiu v jej ďalšom úsilí o podporu akademickej obce a združení používateľov IKT v tom, aby zohrávali aktívnejšiu úlohu a presadzovali konštruktívny dialóg o otázkach kybernetickej bezpečnosti medzi viacerými zúčastnenými stranami; podporuje ďalší rozvoj zhromaždenia pre digitálnu agendu ako rámca na riadenie ochrany kritických informačných infraštruktúr;

27. víta prácu, ktorú doteraz vykonalo Európske fórum členských štátov, pokiaľ ide o stanovenie odvetvových kritérií na identifikáciu európskych kritických infraštruktúr s dôrazom na pevnú a mobilnú komunikáciu, ako aj o diskusiu o zásadách a usmerneniach EÚ na podporu odolnosti a stability na internete; očakáva pokračovanie budovania konsenzu medzi členskými štátmi a v tejto súvislosti nabáda fórum, aby rozšírilo súčasný prístup zameraný na fyzické prostriedky a snažilo sa doň zahrnúť logické infraštruktúrne prostriedky, ktoré budú s rozvojom virtualizácie a technológií výpočtového mračna zohrávať čoraz významnejšiu úlohu z hľadiska účinnosti ochrany kritických informačných infraštruktúr;

28. navrhuje, aby Komisia začala verejnú celoeurópsku vzdelávaciu iniciatívu zameranú na vzdelávanie a zvyšovanie informovanosti súkromných aj podnikových koncových používateľov o možných hrozbách na internete a pri používaní pevných a mobilných informačných a komunikačných zariadení na všetkých úrovniach reťazca služieb, ako aj na propagáciu bezpečnejšieho správania jednotlivcov na internete; v tejto súvislosti pripomína riziká súvisiace so zastaraným IT vybavením a softvérom;

29. vyzýva členské štáty, aby s pomocou Komisie posilnili programy vzdelávania a odbornej prípravy v oblasti informačnej bezpečnosti, zamerané na vnútroštátne orgány presadzovania práva a súdne orgány, ako aj príslušné agentúry EÚ;

30. podporuje vypracovanie vzdelávacieho programu pre akademických odborníkov v oblasti informačnej bezpečnosti, keďže by mal kladný vplyv na odborné poznatky a pripravenosť EÚ z hľadiska stále sa vyvíjajúceho kybernetického priestoru a jeho hrozieb;

31. zasadzuje sa o podporu vzdelávania v oblasti kybernetickej bezpečnosti (stáže doktorandov, univerzitné prednášky, semináre, školenia pre študentov atď.) a špecializovaných školení v oblasti ochrany kritických informačných infraštruktúr;

32. vyzýva Komisiu, aby do konca roku 2012 navrhla komplexnú stratégiu Únie v oblasti internetovej bezpečnosti, ktorá bude založená na jasnej terminológii; zastáva názor, že stratégia v oblasti internetovej bezpečnosti by sa mala zamerať na vytvorenie kybernetického priestoru – podporeného bezpečnou a pružnou infraštruktúrou a otvorenými normami –, ktorý prispieva k inováciám a prosperite prostredníctvom voľného toku informácií a zároveň zaisťuje stabilnú ochranu súkromia a ostatných občianskych slobôd; trvá na tom, že v stratégii by sa mali uviesť zásady, ciele, metódy, nástroje a politiky (vnútorné aj vonkajšie), ktoré sú potrebné na zjednodušenie úsilia jednotlivých členských štátov a EÚ, a stanoviť minimálne normy odolnosti pre členské štáty s cieľom zaistiť bezpečnú, trvalú, stabilnú a odolnú službu, či už v súvislosti s kritickou infraštruktúrou alebo so všeobecným používaním internetu;

33. zdôrazňuje, že ústredným referenčným hľadiskom budúcej stratégie internetovej bezpečnosti vypracovanej Komisiou by mala byť práca v oblasti ochrany kritických informačných infraštruktúr a že táto stratégia by sa mala zameriavať na holistický a systematický prístup ku kybernetickej bezpečnosti, a to tým, že bude obsahovať proaktívne opatrenia, napríklad zavedenie minimálnych noriem pre bezpečnostné opatrenia alebo výučbu jednotlivých používateľov, podnikov a verejných inštitúcií, ako aj reaktívne opatrenia, napríklad trestnoprávne, občianskoprávne a administratívne sankcie;

34. naliehavo žiada Komisiu, aby navrhla stabilný mechanizmus na koordináciu realizácie a pravidelných aktualizácií stratégie v oblasti internetovej bezpečnosti; zastáva názor, že tento mechanizmus by sa mal opierať o primerané administratívne zázemie a odborné a finančné zdroje a v jeho kompetencii by malo byť uľahčovanie vypracovávania stanovísk EÚ vo vzťahoch s domácimi aj medzinárodnými subjektmi v oblasti internetovej bezpečnosti;

35. vyzýva Komisiu, aby navrhla rámec EÚ na oznamovanie porušení bezpečnosti v kritických odvetviach, ako je energetika, doprava, dodávky vody a potravín, ako aj v odvetviach informačných a komunikačných technológií a finančných služieb s cieľom zabezpečiť, aby boli príslušné orgány členských štátov a používatelia informovaní o kybernetických incidentoch, útokoch a narušeniach;

36. naliehavo vyzýva Komisiu, aby zlepšila dostupnosť štatisticky reprezentatívnych údajov o nákladoch súvisiacich s kybernetickými útokmi v EÚ, členských štátoch a priemysle (predovšetkým v odvetví finančných služieb a informačných a komunikačných technológií), a to prostredníctvom posilnenia spôsobilostí na zhromažďovanie údajov plánovaného Európskeho centra pre počítačovú kriminalitu, ktoré sa má zriadiť v roku 2013, tímov CERT a ďalších iniciatív Komisie, ako je Európsky systém výmeny informácií a varovania, s cieľom zabezpečiť systematické vykazovanie a výmenu údajov o kybernetických útokoch a ďalších formách počítačovej kriminality poškodzujúcej európsky priemysel a členské štáty, ako aj posilniť presadzovanie práva;

37. zasadzuje sa o blízky vzťah a interakciu medzi národnými súkromnými sektormi a agentúrou ENISA v záujme prepojenia vnútroštátnych/vládnych tímov CERT s vývojom Európskeho systému výmeny informácií a varovania (EISAS);

38. upozorňuje, že primárnou hybnou silou rozvoja a používania technológií navrhnutých na zvyšovanie internetovej bezpečnosti je odvetvie IKT; pripomína, že politiky EÚ nesmú brániť rastu európskeho internetového hospodárstva a musia zahŕňať potrebné stimuly s cieľom naplno využiť potenciál obchodných a verejno-súkromných partnerstiev; odporúča preskúmanie ďalších podnetov pre priemysel na vypracovanie stabilnejších bezpečnostných plánov prevádzkovateľa v súlade so smernicou 2008/114/ES;

39. vyzýva Komisiu, aby predložila legislatívny návrh ďalšej kriminalizácie kybernetických útokov ((t. j. cieleného podvodného vylákania údajov (tzv. spear-phishing), internetových podvodov atď.);

Medzinárodná spolupráca

40. pripomína, že medzinárodná spolupráca je základným nástrojom na zavedenie účinných opatrení v oblasti kybernetickej bezpečnosti; uznáva, že v súčasnosti sa EÚ trvale aktívne nepodieľa na procesoch a dialógoch medzinárodnej spolupráce týkajúcich sa kybernetickej bezpečnosti; vyzýva Komisiu a Európsku službu pre vonkajšiu činnosť (ESVČ) na začatie konštruktívneho dialógu so všetkými podobne zmýšľajúcimi krajinami, aby sa rozvíjala spoločná dohoda a politiky s cieľom zvýšiť odolnosť internetu a kritickej infraštruktúry; trvá na tom, že EÚ by zároveň mala – trvalo – začleňovať otázky kybernetickej bezpečnosti do rámca svojich vonkajších vzťahov, okrem iného pri navrhovaní rôznych finančných nástrojov alebo uzatváraní medzinárodných dohôd, ktoré zahŕňajú výmenu a uchovávanie citlivých údajov;

41. berie na vedomie pozitívne výsledky Dohovoru o počítačovej kriminalite, ktorý prijala Rada Európy v Budapešti v roku 2011; zdôrazňuje, že ESVČ by mala nabádať ďalšie krajiny, aby podpísali a ratifikovali uvedený dohovor a zároveň by mala uzatvárať dvojstranné a viacstranné dohody o internetovej bezpečnosti a odolnosti s podobne zmýšľajúcimi medzinárodnými partnermi;

42. poukazuje na to, že veľký počet prebiehajúcich činností, ktoré vykonávajú rôzne medzinárodné a európske inštitúcie, orgány a agentúry, ako aj členské štáty, si vyžaduje koordináciu, aby sa zabránilo ich opakovaniu, pričom na tento účel je vhodné zvážiť určenie úradníka zodpovedného za koordináciu, napríklad menovaním koordinátora EÚ pre kybernetickú bezpečnosť;

43. zdôrazňuje, že štruktúrovaný dialóg medzi hlavnými aktérmi a zákonodarcami v EÚ a USA zapojenými do projektu ochrany kritických informačných infraštruktúr má mimoriadny význam pre stanovenie spoločnej dohody, spoločného výkladu a postoja k právnemu rámcu a rámcu riadenia;

44. víta vytvorenie pracovnej skupiny EÚ – USA pre kybernetickú bezpečnosť a počítačovú kriminalitu na samite EÚ – USA, ktorý sa konal v novembri 2010, a podporuje jej úsilie zahrnúť otázky týkajúce sa internetovej bezpečnosti do transatlantického politického dialógu; víta skutočnosť, že Komisia vypracovala spolu s vládou USA pod záštitou pracovnej skupiny EÚ – USA pre kybernetickú bezpečnosť a počítačovú kriminalitu spoločný program a plán spojenej/synchronizovanej transkontinentálnej počítačovej cvičnej simulácie v rokoch 2012/2013;

45. navrhuje zaviesť štruktúrovaný dialóg medzi zákonodarnými inštitúciami EÚ a USA s cieľom diskutovať o otázkach týkajúcich sa internetu v rámci hľadania spoločnej dohody, spoločného výkladu a spoločných pozícií;

46. naliehavo vyzýva ESVČ a Komisiu, aby na základe práce, ktorú vykonalo Európske fórum členských štátov, zabezpečili aktívnu pozíciu v rámci príslušných medzinárodných fór, okrem iného koordináciou pozícií členských štátov, s cieľom podporiť základné hodnoty, ciele a politiky EÚ v oblasti bezpečnosti a odolnosti internetu; poznamenáva, že medzi tieto fóra patrí NATO, OSN (najmä prostredníctvom Medzinárodnej telekomunikačnej únie a Fóra pre riadenie internetu), Internetová spoločnosť pre pridelené mená a čísla (ICANN), Internetový orgán pre prideľovanie čísel, OBSE, OECD a Svetová banka;

47. nabáda Komisiu a agentúru ENISA, aby sa zapojili do dialógov hlavných zainteresovaných strán s cieľom vymedziť technické a právne normy v kybernetickom priestore na medzinárodnej úrovni;

*

* *

48. poveruje svojho predsedu, aby postúpil toto uznesenie Rade a Komisii.

Spolupráca s partnermi za našimi hranicami v oblasti energetickej politiky

P7_TA(2012)0238

Uznesenie Európskeho parlamentu z 12. júna 2012 o zapájaní sa do spolupráce s partnermi za našimi hranicami v oblasti energetickej politiky: strategický prístup k bezpečným, udržateľným a konkurencieschopným dodávkam energie (2012/2029(INI))

(2013/C 332 E/04)

Európsky parlament,

— so zreteľom na oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov s názvom O zabezpečení dodávok energie a medzinárodnej spolupráci: „Energetická politika EÚ: budovanie vzťahov s partnermi za hranicami EÚ (COM(2011)0539),

— so zreteľom na návrh rozhodnutia Európskeho parlamentu a Rady predložený Komisii, ktorým sa stanovuje mechanizmus výmeny informácií, pokiaľ ide o medzivládne dohody v oblasti energetiky medzi členskými štátmi a tretími krajinami (COM(2011)0540),

— so zreteľom na závery Rady z 24. novembra 2011 o zabezpečení dodávok energie a medzinárodnej spolupráci – „Energetická politika EÚ: budovanie vzťahov s partnermi za hranicami EÚ“,

— so zreteľom na svoje uznesenie z 25. novembra 2010 s názvom Na ceste k novej energetickej stratégii pre Európu na roky 2011 – 2020 ([1]),

— so zreteľom na článok 48 rokovacieho poriadku,

— so zreteľom na správu Výboru pre priemysel, výskum a energetiku a stanoviská Výboru pre zahraničné veci, Výboru pre rozvoj a Výboru pre medzinárodný obchod (A7-0168/2012),

([1]) Ú. v. EÚ C 99 E, 3.4.2012, s. 64.