65. upozorňuje na to, že je nutné propagovat dobrovolnictví zejména během Evropského roku občanů 2013, a vyzývá Komisi, aby zařadila podporu dobrovolnictví do politik mezinárodní rozvojové pomoci, mimo jiné s cílem splnit veškeré úkoly stanovené rozvojovými cíli tisíciletí;

66. podporuje formální přezkoumání návrhu interinstitucionálního programu v oblasti lidských zdrojů „Solidarité" v orgánech a institucích EU, jehož cílem je usnadnit zapojení zaměstnanců orgánů a institucí a stážistů do dobrovolných, humanitárních a sociálních činností, a to jak jako součásti odborného vzdělávání zaměstnanců, tak i dobrovolných činností v jejich volném čase;

67. zdůrazňuje skutečnost, že navrhovaný program je z hlediska nákladů úsporný, má vysokou přidanou hodnotu a napomohl by provádění politik a programů EU;

68. doporučuje Komisi, aby vzhledem k mimořádné různorodosti útvarů odpovědných za dobrovolnou činnost v EU zachovala užitečná kontaktní místa vytvořená buď v rámci „EYV 2011 Alliance" či její nástupnické dobrovolnické platformy, která spojuje mnohé dobrovolnické organizace se sítí občanské společnosti, nebo vnitrostátními koordinačními orgány, strategickými partnery a vládami členských států v této oblasti, a vybízí tato kontaktní místa, aby se zasadila o návrh na zřízení centrálního portálu EU jako panevropské platformy za účelem usnadnění další koordinace a větší přeshraniční aktivity;

69. zdůrazňuje důležitost sítí kontaktů a výměny osvědčených postupů pro šíření informací o stávajících postupech v rámci EU, které mohou napomáhat přeshraniční dobrovolné činnosti a podporovat ji;

70. žádá Komisi, aby případně přijala opatření týkající se politické agendy pro dobrovolnictví v Evropě (PAVE), kterou vypracovaly dobrovolnické organizace shromážděné v rámci „EYV 2011 Alliance";

71. pověřuje svého předsedu, aby předal toto usnesení Radě, Komisi a vládám a parlamentům členských států.

Ochrana kritické informační infrastruktury: směrem ke globální kybernetické bezpečnosti

P7_TA(2012)0237

Usnesení Evropského parlamentu 12. června 2012 o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti" (2011/2284(INI))

(2013/C 332 E/03)

Evropský parlament,

— s ohledem na své usnesení ze dne 5. května 2010 nazvané „Nová digitální agenda pro Evropu: 2015.eu" ([1]),

— s ohledem na své usnesení ze dne 15. června 2010 nazvané „Řízení internetu: další kroky" ([2]),

— s ohledem na své usnesení ze dne 6. července 2011 nazvané „Evropské širokopásmové sítě: investice do digitálního růstu" ([3]),

— s ohledem na článek 48 jednacího řádu,

— s ohledem na zprávu Výboru pro průmysl, výzkum a energetiku a stanovisko Výboru pro občanské svobody, spravedlnost a vnitřní věci (A7-0167/2012),

([1]) Úř. věst. C 81E, 15.3.2011, s. 45.
([2]) Úř. věst. C 236E, 12.8.2011, s. 33.
([3]) Přijaté texty, P7_TA(2011)0322.

A. vzhledem k tomu, že schopnost informačních a komunikačních technologií (IKT) podpořit hospodářství a společnost může být plně využita pouze tehdy, budou-li mít uživatelé důvěru v jejich bezpečnost a odolnost, a pokud budou v internetovém prostředí účinně vymáhány již existující právní předpisy v oblastech, jako jsou ochrana údajů a práva duševního vlastnictví;

B. vzhledem k tomu, že dopad internetu a informačních a komunikačních technologií (IKT) na různé aspekty života občanů sílí a že internet a IKT jsou zásadní hybnou silou sociální interakce, kulturního rozvoje a hospodářského růstu;

C. vzhledem k tomu, že bezpečnost IKT a internetu je komplexní otázkou, která má globální dopad v oblasti ekonomiky, sociálních věcí, technologie a vojenství, což vyžaduje jednoznačné vymezení a odlišení povinností a stabilní mechanismus mezinárodní spolupráce;

D. vzhledem k tomu, že stěžejním cílem Digitální agendy pro Evropu je zvýšení konkurenceschopnosti Evropy díky posílení IKT a vytvoření podmínek pro stabilně vysoký růst a pro pracovní místa založená na technologiích;

E. vzhledem k tomu, že soukromý sektor v minulém desetiletí investoval miliardy eur a je i nadále primárním investorem, vlastníkem a správcem produktů týkajících se bezpečnosti informací, opatření, služeb, aplikací a příslušné infrastruktury; vzhledem k tomu, že zapojení soukromých podniků by mělo být posíleno vhodnými politickými strategiemi na podporu odolnosti infrastruktury, která je vlastněna nebo provozována veřejným či soukromým sektorem nebo v rámci partnerství veřejného a soukromého sektoru;

F. vzhledem k tomu, že podaří-li se dosáhnout vysoké úrovně bezpečnosti a odolnosti sítí, služeb a technologií IKT, zvýší se i konkurenceschopnost hospodářství EU, a to jak díky tomu, že se zlepší posuzování a řízení kybernetických rizik, tak tím, že hospodářství EU jako celek bude mít k dispozici robustnější informační infrastrukturu na podporu inovací a růstu, která vytvoří nové příležitosti pro zvyšování produktivity podniků;

G. vzhledem k tomu, že dostupné údaje o vymáhání práva v oblasti kybernetické trestné činnosti – patří sem počítačové útoky, ale také další druhy trestné činnosti on-line – svědčí o tom, že v různých evropských zemích dochází k jejímu výraznému nárůstu; vzhledem však k tomu, že orgány činné v trestním řízení ani skupiny CERT (skupiny pro reakci na počítačové hrozby) neposkytují v dostatečné míře statisticky reprezentativní údaje týkající se kybernetických útoků; tyto údaje budou v budoucnu vyžadovat lepší sumarizaci, díky níž budou policejní orgány moci tyto útoky důrazněji stíhat a která umožní, aby legislativní reakce na stále se vyvíjející kybernetické hrozby vycházely z relevantnějších informací;

H. vzhledem k tomu, že přiměřená míra bezpečnosti informací je zásadní pro výraznější rozmach internetových služeb;

I. vzhledem k tomu, že nedávné kybernetické incidenty, narušení a útoky proti informační infrastruktuře orgánů EU, průmyslu a členských států ukazují, že je nutno zavést robustní, inovativní a účinný systém ochrany kritické informační infrastruktury (CIIP), který bude založen na plné mezinárodní spolupráci a minimálních normách odolnosti platných v členských státech;

J. vzhledem k tomu, že rychlý rozvoj nových prvků v oblasti IKT, jako je např. cloud computing, vyžaduje, abychom věnovali velkou pozornost bezpečnosti, chceme-li plně využívat možností, které nové technologie skýtají;

K. vzhledem k tomu, že se Evropský parlament opakovaně zasazuje o uplatňování vysokých nároků na ochranu soukromí a údajů, neutralitu sítí a na ochranu práv duševního vlastnictví;

Opatření k posílení ochrany kritické informační infrastruktury na vnitrostátní a unijní úrovni

1. vítá, že členské státy provádějí evropský program na ochranu kritické informační infrastruktury a že byla zřízena výstražná informační síť kritické infrastruktury (CIWIN);

2. domnívá se, že snahy o ochranu kritických informačních infrastruktur nejen posílí celkovou bezpečnost občanů, ale zlepší také jejich pocit bezpečnosti a posílí jejich důvěru v opatření, která vláda přijímá na jejich ochranu;

3. bere na vědomí, že Komise zvažuje revizi směrnice Rady 2008/114/ES ([1]), a vyzývá, aby byly ještě před přijetím dalších opatření předloženy doklady o účinnosti a dopadu této směrnice; požaduje, aby se zvážilo rozšíření její působnosti, a to zejména na odvětví IKT a na finanční služby; dále žádá, aby byla pozornost věnována oblastem, jako je zdraví, systémy dodávek potravin a vody, jaderný výzkum a průmysl (pokud se na ně nevztahují zvláštní ustanovení); zastává názor, že tato odvětví by měla rovněž využívat výhod meziodvětvového přístupu, jaký se zaujímá v rámci výstražné informační sítě kritické infrastruktury (spočívající ve spolupráci, systému varování a výměně osvědčených postupů);

4. vyzdvihuje význam zavedení a zaručení trvalé integrace evropského výzkumu pro to, aby se zachovaly a dále vyvíjely evropské špičkové znalosti v oblasti ochrany kritických informačních infrastruktur;

5. s ohledem na propojenou, vysoce vzájemně závislou, citlivou, strategickou a zranitelnou povahu kritické informační infrastruktury na vnitrostátní úrovni a na úrovni EU vyzývá, aby byly pravidelně aktualizovány minimální standardy odolnosti, jejichž cílem je zajistit připravenost na narušení, incidenty, pokusy o destrukci či útoky (např. v důsledku nedostatečné odolnosti infrastruktury nebo nedostatečně zabezpečenými koncovými terminály) a odpovídající reakci;

6. zdůrazňuje význam norem a protokolů pro bezpečnost informací a vítá, že organizace CEN, Cenelec a ETSI byly v roce 2011 pověřeny vytvořením bezpečnostních norem;

7. očekává, že vlastníci a provozovatelé kritické informační infrastruktury umožní a v případě potřeby pomohou uživatelům uplatnit vhodné nástroje ochrany před poškozujícími útoky nebo narušeními, případně prostřednictvím lidského i automatizovaného dohledu;

8. podporuje spolupráci mezi veřejnými a soukromými subjekty na úrovni EU a rovněž jejich úsilí o vytvoření a provádění norem pro bezpečnost a odolnost vnitrostátní či celoevropské civilní – veřejné, soukromé nebo veřejně-soukromé – kritické informační infrastruktury;

9. zdůrazňuje význam celoevropských cvičení zaměřených na přípravu při rozsáhlých síťových bezpečnostních incidentech a význam vymezení jednotného souboru norem pro posuzování hrozeb;

10. vyzývá Komisi, aby ve spolupráci s členskými státy vyhodnotila provádění akčního plánu ochrany kritické informační infrastruktury; naléhavě žádá členské státy, aby vytvořily dobře fungující vnitrostátní/vládní skupiny CERT, vypracovaly vnitrostátní strategie v oblasti počítačové bezpečnosti, pořádaly pravidelné vnitrostátní a celoevropské simulace kybernetických incidentů, vypracovaly vnitrostátní krizové plány proti počítačovým útokům a přispěly k vytvoření evropského krizového plánu pro případy kybernetických incidentů do roku 2012;

11. doporučuje, aby byly pro všechny evropské kritické informační infrastruktury zavedeny bezpečnostní plány provozovatele nebo rovnocenná opatření a aby byli jmenováni styční bezpečnostní úředníci;

12. vítá probíhající revizi rámcového rozhodnutí Rady 2005/222/SVV ([2]) o útocích proti informačním systémům; připomíná, že je třeba koordinovat úsilí EU v boji proti rozsáhlým počítačovým útokům prostřednictvím zapojení agentury ENISA, skupin CERT v členských státech a kompetencí budoucích evropských skupin CERT;

13. domnívá se, že agentura ENISA může na evropské úrovni hrát klíčovou roli při ochraně kritické informační infrastruktury tím, že členským státům a orgánům a institucím EU bude poskytovat odborné technické poznatky a bude vypracovávat zprávy a analýzy bezpečnosti informačního systému na evropské a světové úrovni;

Další aktivity EU pro robustní bezpečnost na internetu

14. naléhavě vyzývá Evropskou agenturu pro bezpečnost sítí a informací (ENISA), aby koordinovala a prováděla každoroční akci EU – měsíc zvyšování povědomí o bezpečnosti internetu, díky níž se otázky bezpečnosti internetu dostanou do popředí zájmu členských států i občanů EU;

([1]) Úř. věst. L 345, 23.12.2008, s. 75.
([2]) Úř. věst. L 69, 16.3.2005, s. 67.

15. podporuje agenturu ENISA v plnění jejích povinností v oblasti bezpečnosti sítí a informací, a to v souladu s cíli digitální agendy, zejména pomocí pokynů a poradenství poskytovaných členským státům v otázce zajištění základních schopností pro jejich skupiny CERT, jakož i prostřednictvím podpory výměny osvědčených postupů prostřednictvím budování atmosféry důvěry; vyzývá agenturu, aby otázky týkající se vymezení podobných opatření v oblasti počítačové bezpečnosti pro soukromé vlastníky a provozovatele sítě a infrastruktury konzultovala s relevantními subjekty a aby Komisi a členským státům pomáhala při podpoře rozvoje a osvojování systémů certifikace v oblasti bezpečnosti informací, norem chování a postupů spolupráce mezi vnitrostátními a evropskými skupinami CERT a vlastníky a provozovateli infrastruktury, kdykoli a kdekoli to bude potřeba, a to prostřednictvím stanovení technologicky neutrálních společných minimálních požadavků;

16. vítá současný návrh revize mandátu agentury ENISA, zejména jeho rozšíření, jakož i rozšíření úkolů agentury; je přesvědčen, že úkolem agentury ENISA by mělo být nejen pomáhat členským státům prostřednictvím poskytování poradenství a analýz, ale také řídit řadu exekutivních úkolů na úrovni EU a ve spolupráci s protějšky v USA, pokud jde o prevenci a odhalování narušení sítě a bezpečnosti informací a rozvoj spolupráce mezi členskými státy; zdůrazňuje, že podle nařízení o ENISA by měly být agentuře uloženy další úkoly související s reakcí na internetové útoky, a to v takovém rozsahu, aby představovaly jednoznačný přínos nad rámec stávajících vnitrostátních mechanismů pro reakci;

17. vítá výsledky celoevropských cvičení v oblasti počítačové bezpečnosti, jež v roce 2010 a 2011 ENISA prováděla a monitorovala v celé Unii s cílem bylo pomoci členským státům při vypracovávání, údržbě a testování celoevropského pohotovostního plánu; vyzývá agenturu ENISA, aby tato cvičení ponechala v programu své činnosti a aby vhodným způsobem postupně zapojovala relevantní soukromé subjekty s cílem zvýšit celkové evropské kapacity v oblasti bezpečnosti na internetu, a těší se na další mezinárodní spolupráci se stejně smýšlejícími partnery;

18. vyzývá členské státy, aby sestavily vnitrostátní plány pro případ krizových situací v kybernetickém prostoru, které by měly definovat příslušné kontaktní body a obsahovat ustanovení o pomoci, kontrole a nápravě v případě kybernetických narušení či útoků regionálního, vnitrostátního nebo přeshraničního významu a jiné klíčové prvky; podotýká, že členské státy by rovněž měly zavést vhodné koordinační mechanismy a struktury na vnitrostátní úrovni, což by přispělo ke zlepšení koordinace mezi příslušnými vnitrostátními orgány a k větší soudržnosti jejich činností;

19. doporučuje, aby Komise v rámci krizových plánů EU pro případy kybernetických incidentů navrhla závazná opatření pro lepší koordinaci technických a řídících funkcí mezi vnitrostátními a vládními skupinami CERT na úrovni EU;

20. vyzývá Komisi a členské státy, aby přijaly nezbytná opatření v zájmu ochrany kritické infrastruktury před počítačovými útoky a poskytly prostředky pro hermetické uzavření přístupu ke kritické infrastruktuře v případě, že přímý počítačový útok vážně ohrozí její řádné fungování;

21. očekává zřízení skupiny CERT EU, které bude klíčovým faktorem při prevenci a odhalování úmyslných a poškozujících počítačových útoků, namířených proti orgánům EU, při reakci na ně a při obnově po takových útocích;

22. doporučuje, aby Komise navrhla závazná opatření, která stanoví minimální standardy bezpečnosti a odolnosti a zlepší koordinaci mezi vnitrostátními skupinami pro reakci na počítačové hrozby (CERT);

23. vyzývá členské státy a orgány EU, aby zajistily existenci správně fungujících skupin CERT, jež na základě osvědčených postupů vymezí minimální funkce v oblasti bezpečnosti a odolnosti; poukazuje na to, že vnitrostátní skupiny CERT by měly být součástí účinné sítě, v jejímž rámci dochází k výměně relevantních informací v souladu s nezbytnými standardy důvěrnosti; požaduje, aby byla v každém členském státě vytvořena služba ochrany kritické informační infrastruktury, která bude k dispozici 24 hodin denně, 7 dní v týdnu, a aby byl vytvořen společný evropský protokol pro naléhavé situace, který by se používat pro komunikaci mezi vnitrostátními kontaktními místy;

24. zdůrazňuje, že budování důvěry a podpora spolupráce mezi členskými státy je zásadní pro ochranu údajů a vnitrostátních sítí a infrastruktury; vyzývá Komisi, aby navrhla společný postup pro nalezení a stanovení společného přístupu k řešení přeshraničních hrozeb IKT, přičemž se očekává, že členské státy poskytnou Komisi obecné informace o rizicích, hrozbách a zranitelných místech své kritické informační infrastruktury;

25. vítá iniciativu Komise, v níž se uvádí, že do roku 2013 bude vytvořen Evropský systém pro varování a sdílení informací;

26. vítá, že na základě iniciativy Komise byly otázky bezpečnosti internetu a ochrany kritické informační infrastruktury konzultovány s různými zainteresovanými stranami, jako je například Evropské partnerství veřejného a soukromého sektoru pro odolnost; bere na vědomí významné zapojení a odhodlání prodejců IKT v rámci tohoto úsilí; vybízí Komisi, aby vyvinula další úsilí na podporu akademické obce a sdružení uživatelů IKT, aby se ujímaly aktivnější role, a dále na podporu konstruktivního dialogu mezi větším počtem zainteresovaných stran, který by se věnoval otázkám kybernetické bezpečnosti; podporuje další rozvoj digitálního shromáždění jako rámce pro správu v oblasti ochrany kritické informační infrastruktury;

27. vítá práci, kterou doposud odvedlo Evropské fórum členských států, pokud jde o stanovení zvláštních kritérií pro jednotlivá odvětví, s jejichž pomocí by mohla být určena evropská kritická infrastruktura, se zaměřením na pevné a mobilní komunikace, a dále o projednávání zásad a pokynů EU pro odolnost a stabilitu internetu; těší se na to, že budování konsensu mezi členskými státy bude pokračovat, a v této souvislosti vybízí fórum, aby současný přístup zaměřený na fyzická aktiva rozšířilo o logickou infrastrukturu, jež bude v souvislosti s pokrokem v oblasti virtualizačních technologií a technologií „cloud“ nabývat na významu z hlediska účinnosti ochrany kritických internetových infrastruktur;

28. doporučuje Komisi, aby zahájila veřejnou celoevropskou iniciativu zaměřenou na vzdělávání a zvyšování povědomí koncových uživatelů – jak soukromých osob, tak podniků –, pokud jde o potenciální rizika internetu a nepřenosných i mobilních zařízení využívajících IKT na všech úrovních infrastrukturních řetězců, a na šíření bezpečnějšího individuálního chování na internetu; připomíná v tomto ohledu rizika spojená se zastaralým počítačovým vybavením a softwarem;

29. vyzývá členské státy, aby s podporou Komise posílily programy vzdělávání a odborné přípravy v oblasti bezpečnosti informací, určené pro vnitrostátní policejní a soudní orgány a příslušné agentury EU;

30. souhlasí s myšlenkou vytvoření evropských osnov pro akademické odborníky v oblasti bezpečnosti informací, neboť by to mělo pozitivní vliv na odbornost a připravenost EU s ohledem na neustále se vyvíjející kyberprostor a hrozby, kterým čelí;

31. vyjadřuje se ve prospěch podpory vzdělávání v oblasti kybernetické bezpečnosti (doktorandské studium, univerzitní přednáškové cykly, semináře, kurzy pro studenty atd.) a specializovaných školení o ochraně kritické informační infrastruktury;

32. vyzývá Komisi, aby do konce roku 2012 navrhla komplexní strategii bezpečnosti internetu pro Unii, která bude založena na jednoznačné terminologii; zastává názor, že cílem strategie bezpečnosti internetu by mělo být vytvoření kyberprostoru – podpořeného bezpečnou a odolnou infrastrukturou a otevřenými normami – který prostřednictvím volného toku informací přispívá k inovacím a prosperitě a zajišťuje důkladnou ochranu soukromí a dalších občanských svobod; domnívá se, že strategie by měla podrobně uvádět zásady, cíle, metody, nástroje a politiky (jak vnitřní, tak vnější) nezbytné pro zorganizování vnitrostátního a evropského úsilí a pro vytvoření minimálních standardů odolnosti pro členské státy, aby byla zajištěna bezpečná, kontinuální, robustní a odolná služba, ať v souvislosti s kritickou infrastrukturou, nebo obecným využíváním internetu;

33. zdůrazňuje, že Komisí připravovaná strategie bezpečnosti internetu by měla vycházet zejména z práce na ochraně kritické informační infrastruktury (CIIP) a měla by usilovat o ucelený a systematický přístup ke kybernetické bezpečnosti tím, že bude zahrnovat jak aktivní opatření, jako je zavedení minimálních norem pro bezpečnostní opatření nebo vzdělávání jednotlivých uživatelů, podniků a veřejných institucí, tak i reaktivní opatření, jako jsou sankce v rámci trestního, občanského a správního práva;

34. naléhavě žádá Komisi, aby navrhla účinný mechanismus pro koordinaci provádění strategie bezpečnosti na internetu a pro její pravidelnou aktualizaci; tento mechanismus by měl být podpořen dostatečnými správními, odbornými a finančními zdroji a jedním z jeho úkolů by mělo být pomáhat při utváření postojů EU ve vztazích s vnitřními i mezinárodními zainteresovanými subjekty v otázkách spojených s bezpečností na internetu;

35. vyzývá Komisi, aby navrhla rámec EU pro oznamování případů narušení bezpečnosti v kritických odvětvích, jako je energetika, doprava a dodávky vody a potravin, a rovněž v odvětví IKT a finančních služeb, přičemž cílem je zajistit, aby orgány členských států a uživatelé byli informováni o incidentech a útocích na internetu nebo narušení jeho fungování;

36. naléhavě žádá Komisi, aby zlepšila dostupnost statisticky reprezentativních údajů týkajících se nákladů počítačových útoků v EU, členských státech a průmyslu (zejména v odvětví finančních služeb a IKT), a to zvýšením kapacity shromažďování údajů Centra pro boj proti kyberkriminalitě, které by mělo být založeno v roce 2013, skupin CERT a dalších iniciativ Komise, jako je například Evropský systém pro varování a sdílení informací, aby bylo zajištěno systematické oznamování a sdílení údajů o počítačových útocích a dalších formách počítačové kriminality postihujících evropský průmysl a členské státy a aby bylo posíleno vymáhání práva;

37. podporuje blízký vztah a interakci mezi vnitrostátními soukromými sektory a agenturou ENISA s cílem napojit vnitrostátní/vládní skupiny CERT na vývoj Evropského systému pro varování a sdílení informací (EISAS);

38. zdůrazňuje, že primární hnací silou rozvoje a využívání technologií, které mají zvýšit bezpečnost internetu, je odvětví IKT; připomíná, že politiky EU nesmí bránit růstu evropské internetové ekonomiky a musí zahrnovat nezbytné pobídky, aby bylo možné v plném rozsahu využívat potenciál partnerství mezi podniky a partnerství veřejného a soukromého sektoru; doporučuje zvážit další pobídky pro odvětví IKT s cílem vypracovat solidnější plány bezpečnosti provozovatele v souladu se směrnicí 2008/114/ES;

39. vyzývá Komisi, aby předložila legislativní návrh na kriminalizaci dalších kybernetických útoků ((tj. spear-phishing, internetové podvody atd.);

Mezinárodní spolupráce

40. připomíná, že mezinárodní spolupráce je hlavním nástrojem pro zavedení účinných opatření v oblasti kybernetické bezpečnosti; připouští, že EU v současnosti není trvale aktivně zapojena do procesů a dialogů, jež se v rámci mezinárodní spolupráce zaměřují na kybernetickou bezpečnost; vyzývá Komisi a Evropskou službu pro vnější činnost (ESVČ), aby zahájily konstruktivní dialog se všemi stejně smýšlejícími zeměmi s cílem dospět ke konsensu a vytvořit programy zvyšování odolnosti internetu a kritické infrastruktury; domnívá se, že EU by zároveň měla zahrnovat otázky bezpečnosti internetu do rámce svých vnějších vztahů, a to trvale, mimo jiné tehdy, když navrhuje různé finanční nástroje nebo když přistupuje k mezinárodním dohodám, jejichž součástí je výměna a uchovávání citlivých údajů;

41. bere na vědomí pozitivní přínos Úmluvy Rady Evropy o kybernetické trestné činnosti, podepsané v Budapešti v roce 2001; poukazuje nicméně na to, že ESVČ by měla vyzvat k podpisu a ratifikaci úmluvy více zemí a měla by také rozvíjet dvoustranné a mnohostranné dohody o bezpečnosti a odolnosti internetu s podobně smýšlejícími mezinárodního partnery;

42. poukazuje na to, že různé mezinárodní a evropské orgány, subjekty a agentury a členské státy provádějí širokou škálu činností, které musí být koordinovány, aby nedocházelo k duplikaci, a za tímto účelem je vhodné zvážit jmenování úředníka odpovědného za koordinaci, případně určit koordinátora EU pro oblast kybernetické bezpečnosti;

43. zdůrazňuje, že strukturovaný dialog mezi hlavními aktéry a zákonodárci v EU a USA, kteří jsou zapojeni do projektu CIIP, má velký význam pro vzájemné porozumění a společný výklad a společné postoje v souvislosti s právními a správními rámci;

44. vítá, že na summitu EU-USA v listopadu 2010 byla zřízena pracovní skupina EU-USA pro kybernetickou bezpečnost a kyberkriminalitu, a podporuje její úsilí o zahrnutí otázek bezpečnosti na internetu do transatlantického politického dialogu; vítá, že Komise a vláda USA v rámci pracovní skupiny EU-USA spolu vypracovaly společný program a plán pro společná/synchronizovaná transkontinentální kybernetická cvičení v letech 2012–2013;

45. navrhuje, aby byl v rámci úsilí o společný konsensus, výklad a postoje zahájen strukturovaný dialog mezi tvůrci právních předpisů EU a USA o problematice internetu;

46. naléhavě vyzývá ESVČ a Komisi, aby na základě práce odvedené Evropským fórem členských států zajistily aktivní postavení v rámci příslušných mezinárodních fór, a to mimo jiné koordinací postojů členských států s cílem prosazovat hlavní hodnoty, cíle a politiky EU v oblasti bezpečnosti a odolnosti internetu; podotýká, že mezi tato fóra patří NATO, OSN (zejména prostřednictvím Mezinárodní telekomunikační unie a Fóra pro správu internetu), Internetové sdružení pro přidělování jmen a čísel, Úřad pro přidělování internetových čísel, OBSE, OECD a Světová banka;

47. vybízí Komisi a agenturu ENISA, aby se účastnily hlavních rozhovorů zúčastněných stran s cílem definovat technické a právní normy v kyberprostoru na mezinárodní úrovni;

*

* *

48. pověřuje svého předsedu, aby předal toto usnesení Radě a Komisi.

Spolupráce s partnery za našimi hranicemi v oblasti energetické politiky

P7_TA(2012)0238

Usnesení Evropského parlamentu ze dne 12. června 2012 o zahájení spolupráce s partnery za našimi hranicemi v oblasti energetické politiky: Strategický přístup k zabezpečeným, udržitelným a konkurenceschopným dodávkám energie (2012/2029(INI))

(2013/C 332 E/04)

Evropský parlament,

— s ohledem na sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o zabezpečení dodávek energie a mezinárodní spolupráci „Energetická politika EU: jednání s partnery za našimi hranicemi“ (COM(2011)0539),

— s ohledem na návrh rozhodnutí Evropského parlamentu a Rady, kterým se zřizuje mechanismus výměny informací o mezivládních dohodách mezi členskými státy a třetími zeměmi v oblasti energetiky (COM(2011)0540), který předložila Komise,

— s ohledem na závěry Rady ze dne 24. listopadu 2011 o zabezpečení dodávek energie a mezinárodní spolupráci – „Energetická politika EU: jednání s partnery za našimi hranicemi“,

— s ohledem na své usnesení ze dne 25. listopadu 2010 nazvané „Směrem k nové energetické strategii pro Evropu 2011–2020“ ([1]),

— s ohledem na článek 48 jednacího řádu,

— s ohledem na zprávu Výboru pro průmysl, výzkum a energetiku a na stanoviska Výboru pro zahraniční věci, Výboru pro rozvoj a Výboru pro mezinárodní obchod (A7-0168/2012),

([1]) Úř. věst. C 99 E, 3.4.2012, s. 64.