středisko pro prevenci a kontrolu nemocí a další);

o

o o

48. pověřuje svého předsedu, aby toto usnesení předal místopředsedkyni, vysoké představitelce, Radě, Komisi, parlamentům členských států, parlamentnímu shromáždění NATO a generálnímu tajemníkovi NATO.

---

P7_TA(2012)0457

## Kybernetická bezpečnost a ochrana

**Usnesení Evropského parlamentu ze dne 22. listopadu 2012 o kybernetické bezpečnosti a ochraně (2012/2096 (INI))**

(2015/C 419/22)

*Evropský parlament*,

— s ohledem na zprávu o provádění evropské bezpečnostní strategie, kterou schválila Evropská rada ve dnech 11. a 12. prosince 2008,

— s ohledem na Úmluvu Rady Evropy o kybernetické trestné činnosti z Budapešti ze dne 23. listopadu 2001,

— s ohledem na závěry Rady o ochraně kritické informační infrastruktury ze dne 27. května 2011 a na předešlé závěry Rady o kybernetické bezpečnosti,

— s ohledem na sdělení Komise „Digitální agenda pro Evropu“ (COM(2010)0245) ze dne 19. května 2010,

— s ohledem na směrnici Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu ([1]),

— s ohledem na nedávné sdělení Komise o zřízení Evropského centra pro boj proti kyberkriminalitě jako prioritě strategie vnitřní bezpečnosti (COM(2012)0140),

— s ohledem na své usnesení ze dne 10. března 2010 o uplatňování evropské strategie v oblasti bezpečnosti a společné bezpečnostní a obranné politiky ([2]),

— s ohledem na své usnesení ze dne 11. května 2011 o rozvoji společné bezpečnostní a obranné politiky po vstupu Lisabonské smlouvy v platnost ([3]),

— s ohledem na své usnesení ze dne 22. května 2012 o strategii vnitřní bezpečnosti Evropské unie ([4]),

— s ohledem na své usnesení ze dne 27. září 2011 k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (ES) č. 1334/2000, kterým se zavádí režim Společenství pro kontrolu vývozu zboží a technologií dvojího užití ([5]),

— s ohledem na své usnesení ze dne 12. června 2012 o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“ ([6]),

---

([1]) Úř. věst. L 345, 23.12.2008, s. 75.
([2]) Úř. věst. C 349, 22.12.2010, s. 63.
([3]) Přijaté texty, P7_TA(2011)0228.
([4]) Přijaté texty, P7_TA(2012)0207.
([5]) Přijaté texty, P7_TA(2011)0406.
([6]) Přijaté texty, P7_TA(2012)0237.

**Čtvrtek, 22. listopadu 2012**

— s ohledem na rezoluci Rady OSN pro lidská práva ze dne 5. července 2012 nazvanou „Ochrana, podpora a uplatňování lidských práv na internetu“ ([1]), která uznává význam ochrany lidských práv a volného toku informací přes internet,

— s ohledem na závěry vrcholné schůzky v Chicagu ze dne 20. května 2012,

— s ohledem na hlavu V Smlouvy o EU,

— s ohledem na článek 48 jednacího řádu,

— s ohledem na zprávu Výboru pro zahraniční věci (A7-0335/2012),

A. vzhledem k tomu, že v dnešním globalizovaném světě jsou EU a její členské státy zásadně závislé na bezpečném kyberprostoru, bezpečném využívání informačních a digitálních technologií a na odolných a spolehlivých informačních službách a související infrastruktuře;

B. vzhledem k tomu, že informační a komunikační technologie jsou rovněž využívány jako nástroje represe; vzhledem k tomu, že podmínky, za nichž jsou tyto technologie využívány, ve značné míře určují jejich potenciální dopad, tj. zda jsou hybnou silou pozitivního vývoje, nebo zda naopak slouží k represi;

C. vzhledem k tomu, že výzvy, hrozby a útoky v oblasti kybernetiky narůstají dramatickým tempem a představují vážné ohrožení bezpečnosti, obrany, stability a konkurenceschopnosti národních států i soukromého sektoru; vzhledem k tomu, že by se tedy řešení těchto hrozeb nemělo odkládat do budoucnosti; vzhledem k tomu, že většina dobře viditelných a vysoce ničivých kybernetických incidentů je v současné době politicky motivována; vzhledem k tomu, že ačkoli je naprostá většina kybernetických incidentů jednoduchých jsou hrozby pro klíčová zařízení čím dál tím sofistikovanější a vyžadují důkladnou ochranu;

D. vzhledem k tomu, že se kyberprostor s téměř dvěma miliardami vzájemně globálně propojených uživatelů stal jedním z nejmocnějších a nejúčinnějších prostředků při prosazování demokratických myšlenek a organizování občanů, kteří se snaží naplnit své touhy po svobodě a bojovat proti diktaturám; vzhledem k tomu, že využívání kyberprostoru nedemokratickými a autoritářskými režimy čím dál více ohrožuje práva jednotlivců na svobodu projevu a shromažďování; vzhledem k tomu, že je tedy velmi důležité zajistit, aby kyberprostor zůstal otevřený volnému proudu myšlenek, informací a projevů;

E. vzhledem k tomu, že v EU a jejích členských státech existuje mnoho překážek politického, legislativního a organizačního rázu pro vytvoření komplexního a jednotného přístupu ke kybernetické ochraně a bezpečnosti; vzhledem k tomu, že v citlivé a zranitelné oblasti kybernetické bezpečnosti chybí společná definice, normy a opatření;

F. vzhledem k tomu, že sdílení a koordinace mezi orgány EU a s členskými státy i mezi nimi vzájemně, stejně jako s vnějšími partnery, jsou stále nedostatečné;

G. vzhledem k tomu, že na evropské i mezinárodní úrovni chybí jasné a harmonizované definice pojmů „kybernetická bezpečnost“ a „kybernetická ochrana“; vzhledem k tomu, že chápání pojmu „kybernetická bezpečnost“ a další klíčové terminologie se v různých zemích podstatně liší;

H. vzhledem k tomu, že EU dosud nevytvořila vlastní soudržné politiky týkající se ochrany kritické informační infrastruktury, což vyžaduje multidisciplinární přístup, neboť je nutné zvýšit bezpečnost a zároveň dodržovat základní práva;

I. vzhledem k tomu, že EU navrhla různé iniciativy pro řešení kyberkriminality na civilní úrovni, včetně zřízení nového Evropského centra pro boj proti kyberkriminalitě, avšak dosud nevypracovala žádný konkrétní plán na úrovni bezpečnosti a obrany;

J. vzhledem k tomu, že v boji proti kyberkriminalitě má zásadní význam posilování důvěry mezi soukromým sektorem, donucovacími orgány, obranou a jinými příslušnými institucemi;

([1]) http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

K. vzhledem k tomu, že předpokladem pro spolehlivou kybernetickou bezpečnost je vzájemná důvěra ve vztazích mezi státními a nestátními subjekty;

L. vzhledem k tomu, že většina kybernetických incidentů ve veřejném i soukromém sektoru nebývá nahlášena kvůli citlivé povaze informací a potenciálnímu poškození obrazu dotčených společností;

M. vzhledem k tomu, že k řadě kybernetických útoků dojde z důvodu nedostatečné odolnosti a robustnosti soukromé a veřejné síťové infrastruktury, špatně chráněných či zabezpečených databází a dalších nedostatků v kritické informační infrastruktuře; vzhledem k tomu, že pouze malý počet členských států považuje ochranu své sítě a informačních systémů a souvisejících údajů za součást své povinné péče, což vysvětluje nedostatek investic do nejmodernější zabezpečovací technologie, odborné přípravy a vypracovávání vhodných pokynů; vzhledem k tomu, že mnoho členských států závisí na bezpečnostních technologiích třetích zemí a že by tyto státy měly vyvinout větší úsilí o to, aby tuto závislost omezily;

N. vzhledem k tomu, že většina pachatelů kybernetických útoků na vysoké úrovni, jež ohrožují národní či mezinárodní bezpečnost a obranu, není nikdy odhalena a stíhána; vzhledem k tomu, že neexistuje mezinárodně dohodnutá podoba reakce na státem zosnovaný kybernetický útok proti jinému státu, ani dohoda, zda by takový případ měl být považován za „casus belli“;

O. vzhledem k tomu, že Evropská agentura pro bezpečnost sítí a informací (ENISA) má usnadnit výměnu osvědčených postupů mezi členskými státy v oblasti kybernetické bezpečnosti na základě doporučení, jak rozvíjet, provádět a udržovat strategii kybernetické bezpečnosti; vzhledem k tomu, že hraje také podpůrnou roli ve vnitrostátních strategiích kybernetické bezpečnosti a vnitrostátních krizových plánech a při organizaci celoevropských a mezinárodních cvičení o ochraně kritické informační infrastruktury (CIIP) a vytváření scénářů pro vnitrostátní cvičení;

P. vzhledem k tomu, že k červnu 2012 oficiálně přijalo vnitrostátní strategii kybernetické bezpečnosti pouze 10 členských států EU;

Q. vzhledem k tomu, že kybernetická ochrana je jednou z největších priorit Evropské obranné agentury (EDA), která v rámci plánu rozvoje schopností ustavila projektový tým věnující se kybernetické bezpečnosti, přičemž většina členských států sbírá zkušenosti a předkládá návrhy doporučení;

R. vzhledem k tomu, že investice do výzkumu a vývoje v oblasti kybernetické bezpečnosti a ochrany mají zásadní význam pro to, aby v těchto dvou odvětvích docházelo k pokroku a byla udržována na vysoké úrovni; vzhledem k tomu, že výdaje na výzkum a vývoj v oblasti obrany se snížily, místo aby dosáhly schválených 2 % celkových výdajů na obranu;

S. vzhledem k tomu, že zvyšování povědomí a vzdělávání občanů o kybernetické bezpečnosti by mělo představovat základ každé komplexní strategie v této oblasti;

T. vzhledem k tomu, že v souladu s SFEU musí být stanovena jasná rovnováha mezi bezpečnostními opatřeními a právy občanů, jako je právo na soukromí, ochrana údajů a svoboda projevu, přičemž ani jedno nesmí být jménem druhého obětováno;

U. vzhledem k tomu, že je stále více zapotřebí lépe dodržovat a chránit právo jednotlivců na soukromí, jak stanoví Listina základních práv EU a článek 16 SFEU; vzhledem k tomu, že potřeba institucí a obranných orgánů zabezpečit a chránit kyberprostor na vnitrostátní úrovni by – ač je důležitá – nikdy neměla být využita jako důvod pro jakékoli omezování práv a svobod v kybernetickém a informačním prostoru;

V. vzhledem k tomu, že globální a hranicemi neomezená povaha internetu vyžaduje nové formy mezinárodní spolupráce a správy se zapojením mnoha zúčastněných stran;

W. vzhledem k tomu, že se vlády při zabezpečování své kritické infrastruktury stále více spoléhají na soukromé subjekty;

X. vzhledem k tomu, že Evropská služba pro vnější činnost (ESVČ) do svých vztahů s třetími zeměmi dosud iniciativně nezahrnula otázky kybernetické bezpečnosti;

Y. vzhledem k tomu, že nástroj stability je dosud jediným programem EU zaměřeným na reakce na naléhavé krize či globální/nadregionální problémy v oblasti bezpečnosti, včetně hrozeb v oblasti kybernetické bezpečnosti;

Z. vzhledem k tomu, že společná reakce – prostřednictvím pracovní skupiny EU-USA pro kybernetickou bezpečnost a kyberkriminalitu – na hrozby v oblasti kybernetické bezpečnosti je jednou z prioritních otázek ve vztazích mezi EU a USA;

***Činnosti a koordinace v EU***

1. konstatuje, že hrozby v oblasti kybernetiky a útoky proti vládám, státní správě a vojenským a mezinárodním orgánům jsou rychle rostoucí a stále častější hrozbou jak v EU, tak na celém světě, a že existují pádné důvody pro obavu, že by státní či nestátní subjekty, zejména teroristické a kriminální organizace, mohly zaútočit na kritické informační a komunikační struktury a infrastruktury orgánů EU a členských států, což by mohlo způsobit značné škody, včetně „kinetického efektu";

2. zdůrazňuje proto potřebu globálního a koordinovaného přístupu k těmto problémům na úrovni EU prostřednictvím rozvíjení komplexní strategie kybernetické bezpečnosti EU, která by měla stanovit společnou definici kybernetické bezpečnosti a ochrany, definiční znaky kybernetického útoku souvisejícího s ochranou a společnou operační vizi a vzít v úvahu přidanou hodnotu stávajících agentur a subjektů, stejně jako osvědčené postupy z těch členských států, které již mají vnitrostátní strategie kybernetické bezpečnosti; zdůrazňuje zásadní význam koordinace a vytváření součinnosti na úrovni Unie pro snadnější kombinování různých iniciativ, programů a činností, jak vojenských, tak civilních; zdůrazňuje, že tato strategie by měla zajistit flexibilitu a být pravidelně aktualizována, aby byla přizpůsobována rychle se měnícímu kyberprostoru;

3. naléhavě vyzývá Komisi a vysokou představitelku Unie pro zahraniční věci a bezpečnostní politiku, aby ve svém nadcházejícím návrhu týkajícím se opatření pro provádění doložky solidarity (článek 222 SFEU) zvážily možnost závažného kybernetického útoku proti členskému státu; je dále toho názoru, že ačkoli je stále třeba definovat kybernetické útoky ohrožující národní bezpečnost společnou terminologií, mohly by spadat do oblasti působnosti doložky o vzájemné obraně (čl. 42 odst. 7 SEU), aniž by byla dotčena zásada proporcionality;

4. zdůrazňuje, že SBOP musí zajistit, aby síly, jež se účastní vojenských operací EU a civilních misí, byly chráněny proti kybernetickým útokům; zdůrazňuje, že by z kybernetické ochrany měla být učiněna aktivní schopnost v rámci SBOP;

5. zdůrazňuje, že všechny politiky EU týkající se kybernetické bezpečnosti by měly být koncipovány a navrženy tak, aby zajistily co nejvyšší míru ochrany a zachování digitálních svobod a dodržování lidských práv na internetu; domnívá se, že s cílem pokročit v tomto úsilí by měl být internet spolu s informačními a komunikačními technologiemi zařazen do zahraničních a bezpečnostních politik EU;

6. vyzývá Komisi a Radu, aby jednoznačně uznaly digitální svobody za základní práva a nezbytný předpoklad požívání všeobecných lidských práv; zdůrazňuje, že by členské státy měly usilovat o to, aby v rámci vyvářeení reakcí na kybernetickou hrozbu a útoky nikdy neohrozily práva a svobody svých občanů, a že by měly ve svých právních předpisech náležitě rozlišovat mezi civilní a vojenskou úrovní kybernetických incidentů; vyzývá k opatrnosti při uplatňování omezení, pokud jde o možnosti občanů využívat nástroje komunikačních a informačních technologií;

7. vyzývá Radu a Komisi, aby společně s členskými státy vypracovaly bílou knihu o kybernetické ochraně, která by obsahovala jasné definice a kritéria oddělující úrovně kybernetických útoků v civilní a vojenské oblasti podle jejich účelu a účinků a rovněž podle úrovně reakcí, včetně vyšetřování, odhalování a stíhání pachatelů;

8. domnívá se, že existuje jasná potřeba pro aktualizaci evropské bezpečnostní strategie s cílem stanovit a nalézt způsoby pronásledování a trestního stíhání samostatných i státem podporovaných pachatelů kybernetických útoků na sítě;

***Úroveň EU***

9. zdůrazňuje význam horizontální spolupráce a koordinace v oblasti kybernetické bezpečnosti v rámci orgánů a agentur EU a mezi nimi;

10. zdůrazňuje, že nové technologie jsou výzvou pro způsob, jakým vlády plní své tradiční základní funkce; znovu potvrzuje, že obranná a bezpečnostní politika jsou v konečném důsledku v rukou vlád, a to včetně příslušného demokratického dohledu; bere na vědomí stále významnější úlohu soukromých subjektů při plnění úkolů v oblasti bezpečnosti a obrany, často při neexistenci mechanismů zajišťujících transparentnost a odpovědnost či demokratickou kontrolu;

11. zdůrazňuje, že vlády musí při užívání nových technologií, jež spadají do oblasti působnosti bezpečnostní a obranné politiky, dodržovat základní zásady mezinárodního veřejného a humanitárního práva, jako je respektování státní svrchovanosti a dodržování lidských práv; poukazuje na cennou zkušenost členských států EU, jako je Estonsko, při vymezování a navrhování politik v oblasti kybernetické bezpečnosti a ochrany;

12. uznává potřebu posouzení celkové úrovně kybernetických útoků na informační systémy a infrastrukturu EU; v této souvislosti zdůrazňuje potřebu průběžného posuzování stupně připravenosti orgánů EU čelit možným kybernetickým útokům; zdůrazňuje zejména nutnost posílit kritickou informační infrastrukturu;

13. zdůrazňuje rovněž potřebu informovat o slabinách informačních systémů a poskytovat výstrahy a upozornění o nových hrozbách, kterým tyto systémy čelí;

14. konstatuje, že nedávné kybernetické útoky na evropské informační sítě a vládní informační systémy způsobily vážné hospodářské a bezpečnostní škody, jejichž šíře nebyla odpovídajícím způsobem vyhodnocena;

15. vyzývá všechny orgány EU, aby v co nejkratší době vyvinuly své strategie v oblasti kybernetické bezpečnosti a pohotovostní plány, a to s ohledem na své vlastní systémy;

16. vyzývá všechny orgány EU, aby do své analýzy rizik a plánů na řešení krizí zahrnuly otázku řešení kybernetických krizí; vyzývá dále všechny orgány EU, aby všem svým zaměstnancům poskytly školení, jež by zvýšilo povědomí o kybernetické bezpečnosti; navrhuje, aby byla kybernetická cvičení prováděna jednou ročně podobně jako cvičení pro mimořádné situace;

17. podtrhuje význam účinného rozvíjení skupiny pro reakci na počítačové hrozby na úrovni EU (EU-CERT) a vnitrostátních skupin tohoto druhu (CERT) i rozvíjení vnitrostátních pohotovostních plánů pro případ nutnosti přijetí opatření; vítá skutečnost, že do května 2012 zřídily vnitrostátní skupiny CERT všechny členské státy EU; naléhavě vyzývá k dalšímu rozvoji vnitrostátních skupin CERT a skupiny CERT na úrovni EU, jež by byly v případě potřeby schopné nasazení do 24 hodin; zdůrazňuje nutnost zaměřit se na možnost utvoření partnerství mezi veřejným a soukromým sektorem v této oblasti;

18. uznává, že první celoevropské cvičení o ochraně kritické informační infrastruktury Cyber Europe 2010, do něhož se zapojilo několik členských států pod vedením agentury ENISA, se osvědčilo jako užitečné opatření a příklad osvědčených postupů; zdůrazňuje rovněž potřebu co nejrychleji vytvořit výstražnou informační síť kritické infrastruktury na evropské úrovni;

19. zdůrazňuje význam celoevropských cvičení zaměřených na přípravu na rozsáhlé bezpečnostní incidenty týkající se sítí, stejně jako vymezení jednotného souboru norem pro posuzování hrozeb;

20. vyzývá Komisi, aby prozkoumala potřebu a uskutečnitelnost základny EU pro koordinaci v oblasti kybernetiky;

21. domnívá se, že vzhledem k vysoké úrovni znalostí, jichž je zapotřebí k tomu, aby bylo možné kybernetické systémy a infrastruktury jak odpovídajícím způsobem chránit, tak na ně zaútočit, by měla být Komisí, Radou a členskými státy zvážena možnost vytvoření tzv. strategie „bílých hackerů“; konstatuje, že potenciální odliv mozků v těchto případech je vysoký a že zvláště nezletilé osoby odsouzené za tyto útoky mají vysoký potenciál pro nápravu a začlenění do obranných agentur a orgánů;

***Evropská obranná agentura (EDA)***

22. vítá nedávné iniciativy a projekty vztahující se ke kybernetické ochraně, zvláště týkající se shromažďování a zmapování relevantních údajů, problémů a potřeb v oblasti kybernetické bezpečnosti a ochrany, a naléhavě žádá členské státy, aby více spolupracovaly s agenturou EDA v oblasti kybernetické ochrany, a to i na vojenské úrovni;

23. zdůrazňuje význam úzké spolupráce členských států s agenturou EDA na rozvíjení jejich vnitrostátních ochranných kapacit proti kybernetickým útokům; domnívá se, že pro účinnou kybernetickou ochranu na evropské a vnitrostátní úrovni je zásadní vytváření součinnosti, slučování a sdílení na úrovni evropské;

24. vybízí agenturu EDA, aby prohloubila svou spolupráci s NATO, vnitrostátními a mezinárodními centry excelence, Evropským centrem pro boj proti kyberkriminalitě v rámci Europolu, jež přispívá k urychlení reakce v případě kybernetického útoku, a zvláště se střediskem excelence pro společnou počítačovou obranu (CCDCOE), a aby se soustředila na budování kapacit, odbornou přípravu i na výměnu informací a postupů;

25. se znepokojením si všímá skutečnosti, že do roku 2010 dosáhl pouze jeden členský stát 2 % výše výdajů na výzkum a vývoj v oblasti obrany a že pět členských států nemělo v roce 2010 v oblasti výzkumu a vývoje vůbec žádné výdaje; naléhavě vyzývá agenturu EDA, aby společně s členskými státy sdružila zdroje a účinně investovala do výzkumu a vývoje založeného na spolupráci, se zvláštním důrazem na kybernetickou bezpečnost a ochranu;

***Členské státy***

26. vyzývá všechny členské státy, aby neodkladně vytvořily a dokončily své vnitrostátní strategie kybernetické bezpečnosti a ochrany a aby zajistily dobré prostředí pro tvorbu politik a právních předpisů, komplexní postupy řízení rizik a vhodná přípravná opatření a mechanismy; vyzývá agenturu ENISA, aby členským státům pomáhala; vyjadřuje podporu agentuře ENISA, která vypracovává příručku osvědčených postupů a doporučení, jak vyvíjet, provádět a udržovat strategii kybernetické bezpečnosti;

27. vybízí všechny členské státy k tomu, aby v rámci svých vojenských struktur vytvořily vybrané jednotky pro kybernetickou bezpečnost a ochranu, které by spolupracovaly s podobnými orgány v jiných členských státech EU;

28. vybízí členské státy, aby na regionální úrovni zavedly specializovaná soudní centra pro efektivnější trestání narušování informačních systémů; trvá na nutnosti podpořit přizpůsobování vnitrostátního práva s cílem upravovat jej podle vývoje technologií a postupů;

29. vyzývá Komisi, aby pokračovala v práci na soudržném a účinném evropském přístupu s cílem vyhnout se nadbytečným iniciativám a povzbuzovala a podporovala členské státy v jejich snaze rozvinout mechanismy spolupráce a prohloubit výměnu informací; je toho názoru, že by mezi členskými státy měla být stanovena minimální úroveň povinné spolupráce a sdílení;

30. naléhavě vyzývá členské státy, aby vypracovaly vnitrostátní pohotovostní plány a aby do svých plánů na řešení krizí a analýzy rizik zahrnuly otázku řešení kybernetických krizí; dále zdůrazňuje význam odpovídající odborné přípravy o nezbytné kybernetické bezpečnosti pro všechny zaměstnance veřejných subjektů, a zejména poskytování takového vzdělání členům soudních a bezpečnostních institucí ze strany vzdělávacích institucí; vyzývá agenturu ENISA a ostatní příslušné subjekty, aby pomohly členským státům při zajištění sdružování a sdílení zdrojů i v zamezení zdvojování činností;

31. naléhavě vyzývá členské státy, aby z výzkumu a vývoje učinily jeden z hlavních pilířů kybernetické bezpečnosti a ochrany a aby podporovaly vzdělávání inženýrů specializovaných na oblast ochrany informačních systémů; vyzývá členské státy, aby dostály závazku zvýšení výdajů na výzkum a vývoj v oblasti obrany alespoň na 2 %, se zvláštním zaměřením na kybernetickou bezpečnost a ochranu;

32. vyzývá Komisi a členské státy, aby předložily programy na podporu obecného bezpečného využívání internetu, informačních systémů a komunikačních technologií a na zvýšení obecného povědomí v této oblasti u soukromých i obchodních uživatelů; vyzývá Komisi, aby v tomto ohledu zahájila veřejnou celoevropskou vzdělávací iniciativu, a vyzývá členské státy, aby do školních osnov od co nejranějšího věku začlenily vzdělávání v oblasti kybernetické bezpečnosti;

***Spolupráce mezi veřejným a soukromým sektorem***

33. zdůrazňuje klíčovou úlohu smysluplné a doplňující se spolupráce v oblasti kybernetické bezpečnosti mezi veřejnými orgány a soukromým sektorem, jak na úrovni EU, tak na vnitrostátní úrovni, s cílem navození vzájemné důvěry; je si vědom toho, že další posilování spolehlivosti příslušných veřejných orgánů a jejich účinnosti přispěje k budování důvěry a ke

sdílení kritických informací;

34. vyzývá partnery v soukromém sektoru, aby zvážili řešení, kdy bude na bezpečnost pomýšleno již od fáze návrhu nových produktů, nástrojů, služeb a aplikací, a pobídky pro subjekty, u jejichž návrhů nových produktů, nástrojů, služeb a aplikací je bezpečnost ústředním rysem; vyzývá k tomu, aby byly s ohledem na spolupráci se soukromým sektorem vytvořeny minimální normy transparentnosti a mechanismy pro zajištění odpovědnosti s cílem předcházet kybernetickým útokům a bojovat proti nim;

35. zdůrazňuje, že ochrana kritické informační infrastruktury je začleněna do strategie vnitřní bezpečnosti EU v souvislosti se zvyšováním úrovně bezpečnosti pro občany a podniky v kyberprostoru;

36. vyzývá k tomu, aby byl s těmito partnery navázán stálý dialog o nejlepším využití a odolnosti informačních systémů a o sdílení odpovědnosti, jíž je třeba pro jejich bezpečné a řádné fungování;

37. je toho názoru, že členské státy, orgány EU a soukromý sektor by ve spolupráci s agenturou ENISA měly učinit opatření pro zvýšení bezpečnosti a celistvosti informačních systémů s cílem předcházet útokům a zmírnit jejich dopad na minimum; podporuje Komisi v jejích snahách stanovit minimální normy pro kybernetickou bezpečnost a certifikační systémy týkající se firem a vytvořit vhodné pobídky pro podporu úsilí soukromého sektoru o zlepšení bezpečnosti;

38. vyzývá Komisi a vlády členských států, aby podporovaly soukromý sektor a subjekty občanské společnosti v začleňování otázky řešení kybernetických krizí do plánů na řešení krizí a analýzy rizik; dále vyzývá k tomu, aby pro všechny jejich zaměstnance byla zavedena odborná příprava pro zvýšení povědomí o nezbytné kybernetické bezpečnosti a kybernetické hygieně;

39. vyzývá Komisi, aby ve spolupráci s členskými státy a příslušnými agenturami a institucemi vyvinula rámce a nástroje pro systém rychlé výměny informací, který by zajistil soukromému sektoru anonymitu při ohlašování kybernetických incidentů, umožnil veřejným subjektům neustálý přístup k aktuálním informacím a poskytl pomoc v případě potřeby;

40. zdůrazňuje, že je třeba, aby EU usnadnila rozvoj konkurenceschopného a inovačního trhu pro kybernetickou bezpečnost v EU tak, aby mohly malé a střední podniky v této oblasti lépe provozovat svou činnost, což přispěje k podpoře hospodářského růstu a vytvoření nových pracovních míst;

***Mezinárodní spolupráce***

41. vyzývá Evropskou službu pro vnější činnost, aby k otázce kybernetické bezpečnosti zaujala proaktivní postoj a zohledňovala tuto otázku ve všech svých činnostech, zejména ve vztahu k třetím zemím; vyzývá k urychlení spolupráce a výměny informací o způsobech řešení otázek kybernetické bezpečnosti se třetími zeměmi;

42. zdůrazňuje, že dokončení komplexní strategie kybernetické bezpečnosti EU je předpokladem pro navázání takové účinné mezinárodní spolupráce v otázce kybernetické bezpečnosti, jaká je nezbytná vzhledem k přeshraničnímu rázu kybernetických hrozeb;

43. vyzývá ty členské státy, které ještě nepodepsaly nebo neratifikovaly Úmluvu Rady Evropy o kybernetické trestné činnosti (Budapešťská úmluva), aby tak neprodleně učinily; podporuje Komisi a Evropskou službu pro vnější činnost v jejich snahách propagovat Úmluvu a její hodnoty ve třetích zemích;

44. je si vědom potřeby mezinárodně schválené a koordinované reakce na kybernetické hrozby; vyzývá proto Komisi, Evropskou službu pro vnější činnost a členské státy, aby se ujaly vedoucí úlohy na všech fórech, zejména v OSN, ve snaze dosáhnout širší mezinárodní spolupráce a konečné dohody týkající se definice společného pojetí norem chování v kyberprostoru a aby rovněž prosazovaly spolupráci s cílem vypracovat dohody o kontrole kybernetických zbraní;

45. vybízí k výměně znalostí v oblasti kybernetické bezpečnosti se zeměmi BRICS a s jinými zeměmi s rozvíjejícími se ekonomikami s cílem prozkoumat případné společné reakce na narůstající kyberkriminalitu a kybernetické hrozby a útoky jak na civilní, tak na vojenské úrovni;

46. naléhavě vyzývá Evropskou službu pro vnější činnost a Komisi, aby zaujaly proaktivní přístup v rámci příslušných mezinárodních fór a organizací, zejména OSN, OBSE, OECD a Světové banky, s cílem uplatňovat stávající mezinárodní právo a dosáhnout konsensu ohledně norem pro odpovědné chování státu v otázce kybernetické bezpečnosti a ochrany a aby koordinovaly stanoviska členských států s cílem propagovat základní hodnoty a politiky EU v oblasti kybernetické bezpečnosti a ochrany;

47. vyzývá Radu a Komisi, aby v rámci dialogů a vztahů se třetími zeměmi a dohod o spolupráci s těmito státy a především v případě, že tyto dohody obsahují ustanovení o spolupráci či výměně v oblasti technologií, trvaly na minimálních požadavcích pro předcházení kyberkriminalitě a kybernetickým útokům a pro boj s nimi a na minimálních normách v oblasti bezpečnosti informačních systémů;

48. vyzývá Komisi, aby v případě potřeby usnadnila třetím zemím jejich úsilí o vybudování kybernetické bezpečnosti a ochranné kapacity proti kybernetickým útokům a rovněž jim v této oblasti pomáhala;

***Spolupráce s NATO***

49. opakovaně zdůrazňuje, že EU a NATO mají na základě svých společných hodnot a strategických zájmů zvláštní odpovědnost a způsobilost řešit narůstající problémy v oblasti kybernetické bezpečnosti účinněji a v úzké spolupráci, a to hledáním možné doplňkovosti, aniž by docházelo ke zdvojování úsilí a s ohledem na své příslušné povinnosti;

50. zdůrazňuje potřebu slučování a sdílení v praktické rovině, s přihlédnutím k tomu, že se přístupy EU a NATO v otázce kybernetické bezpečnosti a ochrany doplňují; zdůrazňuje potřebu užší koordinace, zejména ohledně plánování, technologií, odborné přípravy a vybavení vztahujících se ke kybernetické bezpečnosti a ochraně;

51. na základě stávajících doplňkových činností v oblasti rozvoje ochranných kapacit naléhavě vyzývá všechny příslušné instituce v EU zabývající se kybernetickou bezpečností a ochranou, aby prohloubily svou praktickou spolupráci s NATO za účelem výměny zkušeností a znalostí týkajících se toho, jak dosáhnout odolnosti systémů EU;

***Spolupráce se Spojenými státy***

52. domnívá se, že EU a Spojené státy by měly prohloubit vzájemnou spolupráci v boji proti kybernetickým útokům a kyberkriminalitě, neboť na lisabonském summitu EU-USA v roce 2010 byla tato oblast prohlášena za prioritní v transatlantických vztazích;

53. 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 kybernetické bezpečnosti do transatlantického politického dialogu;

54. vítá, že Komise a vláda USA v rámci pracovní skupiny EU-USA společně vypracovaly společný program a plán pro společná/synchronizovaná transkontinentální kybernetická cvičení v letech 2012–2013; bere na vědomí první cvičení Cyber Atlantic 2011;

55. zdůrazňuje, že je zapotřebí, aby USA a EU jakožto největší zdroje kyberprostoru i uživatelů spolupracovaly na ochraně práv a svobod svých občanů při užívání tohoto prostoru; zdůrazňuje, že ačkoli je národní bezpečnost prvořadým cílem, měl by být kyberprostor nejen zabezpečen, ale také chráněn;

o

o o

56. pověřuje svého předsedu, aby předal toto usnesení Radě, Komisi, vysoké představitelce, místopředsedkyni Komise, Evropské obranné agentuře (EDA), Evropské agentuře pro bezpečnost sítí a informací (ENISA) a NATO.