Rada
Evropské unie

Brusel 20. listopadu 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	20. listopadu 2017
Příjemce:	Delegace
Č. předchozího dokumentu:	13943/17 + COR 1
Č. dok. Komise:	12210/17, 12211/17
Předmět:	Závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU – závěry Rady (20. listopadu 2017)

Delegace naleznou v příloze závěry Rady o společném sdělení Evropskému parlamentu a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU, které přijala Rada pro obecné záležitosti dne 20. listopadu 2017.

PŘÍLOHA

Závěry Rady o společném sdělení EP a Radě: Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU

Rada Evropské unie,

1. UZNÁVAJÍC význam kybernetické bezpečnosti pro prosperitu, růst a bezpečnost EU a pro integritu našich svobodných a demokratických společností spolu s jejich podpůrnými procesy v digitálním věku, neboť chrání jak právní stát, tak i lidská práva a základní svobody každého jednotlivce;

2. ZDŮRAZŇUJÍC potřebu řešit kybernetickou bezpečnost soudržným přístupem na vnitrostátní, unijní i celosvětové úrovni, neboť kybernetické hrozby mají dopad na naši demokracii, prosperitu, stabilitu a bezpečnost;

3. KONSTATUJE, že vysoká úroveň kybernetické odolnosti v celé EU je rovněž důležitá pro získání důvěry v jednotný digitální trh a pro další rozvoj digitální Evropy;

4. OPAKUJÍC, že EU bude neustále prosazovat otevřený, globální, svobodný, pokojný a bezpečný kyberprostor, kde jsou v rámci EU i v celosvětovém měřítku v plném rozsahu uplatňována a dodržována lidská práva a základní svobody, zejména právo na svobodu projevu, přístup k informacím, ochrana údajů, soukromí a bezpečnost, jakož i základní hodnoty a zásady EU, a ZDŮRAZŇUJÍC, že je vrcholně důležité zajistit vhodnou rovnováhu mezi lidskými právy a základními svobodami na straně jedné a plněním požadavků v oblasti politiky vnitřní bezpečnosti EU[1] na straně druhé,

5. UZNÁVAJÍC, že v kyberprostoru platí mezinárodní právo včetně Charty OSN v celém jejím rozsahu, mezinárodní humanitární právo a právní předpisy v oblasti lidských práv, a ZDŮRAZŇUJÍC proto, že je nezbytné pokračovat v úsilí, jehož předmětem je zajišťovat dodržování mezinárodního práva v kyberprostoru;

[1] Dokument 12650/17.

6. PŘIPOMÍNAJÍC své závěry o strategii EU pro kybernetickou bezpečnost[2], o správě internetu[3], o posílení kybernetické odolnosti EU[4], o kybernetické diplomacii[5] a o rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru[6], o zlepšení trestního soudnictví v kyberprostoru[7], o bezpečnosti a obraně v kontextu globální strategie EU[8], společný rámec pro boj proti hybridním hrozbám[9] a závěry o přezkumu obnovené strategie vnitřní bezpečnosti Evropské unie 2015–2020 v polovině období[10];

7. UZNÁVAJÍC, že rámec stanovený Úmluvou Rady Evropy o počítačové trestné činnosti (Budapešťská úmluva) představuje pevný základ pro používání účinné právní normy v odlišných vnitrostátních legislativách různorodé skupiny zemí a pro mezinárodní spolupráci týkající se kyberkriminality;

8. UZNÁVAJÍC, že je třeba obnovit důraz kladený na provádění politického rámce EU pro kybernetickou obranu z roku 2014 a jeho aktualizace v zájmu hlubší integrace kybernetické bezpečnosti a obrany do společné bezpečnostní a obranné politiky (SBOP) i do širší bezpečnostní a obranné agendy;

9. UZNÁVAJÍC, že celosvětově konkurenceschopný evropský průmysl je důležitým prvkem, má-li být dosaženo vysoké úrovně kybernetické bezpečnosti na vnitrostátní úrovni i v rámci EU;

10. PŘÍPOMÍNAJÍC, že podle čl. 4 odst. 2 Smlouvy o EU je národní bezpečnost výhradní odpovědností každého členského státu,

---

2 Dokumenty 12109/13 a 6225/13 (společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: „Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor“ (COM JOIN (2013) 1 final).

3 Dokumenty 16200/14 a 6460/14 (sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů „Politika v oblasti internetu a jeho správa: Úloha Evropy při formování budoucnosti internetové správy (COM(2014) 72 final)).

4 Dokumenty 14540/16 a 11013/16 (sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů „Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti“ (COM 2016(410) final).

5 Dokument 6122/15.

6 Dokument 9916/17.

7 Dokument 10007/16.

8 Dokument 9178/17.

9 Dokument 7688/16 (společné sdělení Evropskému parlamentu a Radě: Společný rámec pro boj proti hybridním hrozbám: Reakce Evropské unie).

10 Dokument 12650/17.

TÍMTO

11. VÍTÁ společné sdělení Evropskému parlamentu a Radě nazvané: „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“, které navrhuje ambiciózní cíl posílení kybernetické bezpečnosti v rámci EU. Přispívá i ke strategické nezávislosti uvedené v závěrech Rady o globální strategii zahraniční a bezpečnostní politiky Evropské unie[11], neboť jeho cílem je vybudovat digitální Evropu, která bude bezpečnější, důvěryhodnější, lépe si vědoma svých silných stránek, konkurenceschopnější, otevřenější světu, lépe respektující sdílené hodnoty EU týkající se otevřeného, svobodného, pokojného a bezpečného globálního internetu – a tedy dosažení vyšší úrovně odolnosti v zájmu předcházení kybernetickým hrozbám, odrazováním od nich, jejich odhalováním a reagováním na ně.

12. VYZÝVÁ členské státy, orgány, agentury a subjekty EU, aby při naplňování strategických cílů stanovených v těchto závěrech spolupracovaly a respektovaly přitom své oblasti působnosti a zásadu subsidiarity a proporcionality, a

13. ZDŮRAZŇUJE, že je nezbytné, aby EU, její členské státy a soukromý sektor zajistily s ohledem na dostupné zdroje dostatečné financování na podporu celounijního úsilí v oblasti budování kybernetické odolnosti a výzkumu a vývoje v oblasti kybernetické bezpečnosti v celé EU, jakož i pro posílení spolupráce s cílem předcházet kybernetickým útokům, odrazovat od nich, odhalovat je a reagovat na ně a v zájmu schopnosti společně reagovat na kybernetické incidenty velkého rozsahu a nepřátelské kybernetické činnosti po celé EU;

---

[11] Dokument 13202/16.

Kapitola I

ZAJIŠTĚNÍ ÚČINNÉ KYBERNETICKÉ ODOLNOSTI EU A DŮVĚRA V JEDNOTNÝ DIGITÁLNÍ TRH

14. ZDŮRAZŇUJE, že za posílení vlastní kybernetické bezpečnosti a zajištění reakce na incidenty a krize je primárně odpovědný každý členský stát, EU však může zajistit silnou přidanou hodnotu tím, že podpoří spolupráci mezi členskými státy. ZDŮRAZŇUJE v této souvislosti, že je nutné, aby všechny členské státy zpřístupnily vnitrostátním orgánům odpovědným za kybernetickou bezpečnost potřebné zdroje, aby bylo v celé EU zajištěno předcházení kybernetickým incidentům a krizím, jejich odhalování a reagování na ně;

15. VYZDVIHUJE, že je třeba pokud možno využívat stávajících mechanismů, struktur a organizací na úrovni EU;

16. OCEŇUJE:

- pokrok, jehož členské státy dosáhly v provádění směrnice o bezpečnosti sítí a informací, a ZDŮRAZŇUJE, že je nutné dosáhnout úplného a účinného provedení do května 2018, jak je ve směrnici stanoveno[12];
- práci vykonanou v rámci skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, pokud jde o posílení strategické spolupráce a výměny informací mezi členskými státy;
- práci vykonanou v rámci sítě CSIRT, zejména při posilování operativní spolupráce členských států, budování důvěry při sdílení informací ohledně řešení kybernetických incidentů velkého rozsahu a poskytování informací pro sdílenou situační informovanost na evropské úrovni na základě závěrů z jednotlivých členských států;
- práci vykonanou v rámci smluvního partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost.

---

[12] Aniž je dotčena pravomoc členských států při provádění směrnice o bezpečnosti sítí a informací, zejména s ohledem na provozovatele základních služeb.

17. VÍTÁ potvrzení obsažené ve společném sdělení, podle něhož má silné a důvěryhodné šifrování zásadní význam pro řádné zajištění dodržování lidských práv a základních svobod v EU a pro důvěru veřejnosti v jednotný digitální trh, s přihlédnutím k tomu, že donucovací orgány potřebují přístup k údajům nezbytným pro vyšetřování, která vedou; dále vítá potvrzení, že bezpečná digitální identifikace i komunikace hrají klíčovou úlohu při zajišťování účinné kybernetické bezpečnosti v EU;

18. VÍTÁ ve společném sdělení obsažený plán zvýšit ambice při pravidelném provádění celoevropských cvičení v oblasti kybernetické bezpečnosti, vycházet při tom ze zkušeností cvičení CyberEurope a zahrnovat reakce na různých úrovních, neboť se jedná o prvek, jenž bude důležitý při zvyšování připravenosti členských států a institucí EU v reakci na kybernetické incidenty velkého rozsahu;

19. VYZÝVÁ EU a její členské státy, aby v různých složeních Rady prováděly pravidelná strategická cvičení se zaměřením na kybernetickou bezpečnost a vycházely přitom ze zkušeností získaných během cvičení nazvaného EU CYBRID 2017, a

20. aniž je dotčen výsledek legislativního procesu:

- VÍTÁ návrh na vytvoření silného a trvalého mandátu pro Evropskou agenturu pro bezpečnost sítí a informací (ENISA), jehož hlavním cílem by bylo podporovat a rozvíjet užší spolupráci mezi členskými státy, zvyšovat jejich kapacity a posilovat důvěru v digitální Evropu;

- OPĚTOVNĚ POTVRZUJE, že agentura ENISA by se v budoucnu měla opírat o zkušenosti a odborné znalosti členských států a EU a podporovat soustavný rozvoj a provádění stávajících i budoucích politik a právních předpisů, přičemž by současně mělo být zajištěno, že veškeré pravomoci agentury ENISA budou rozvíjeny tak, aby doplňovaly činnosti členských států;

- OPĚTOVNĚ POTVRZUJE cíl v podobě zvýšení důvěry v digitální Evropu, jehož má být dosaženo zvyšováním důvěry v digitální řešení a inovace včetně internetu věcí, elektronického obchodu a elektronické správy, zejména pokud jde o prvotřídní evropský rámec pro certifikaci kybernetické bezpečnosti[13]; Toto je klíčový požadavek pro posílení důvěry a bezpečnosti v oblasti digitálních výrobků a služeb, pro ochranu kritické infrastruktury, vládních, občanských a obchodní údajů a zásadní podmínka pro přijetí přístupu „bezpečnost již od fáze návrhu“ pro výrobky, služby a procesy na jednotném digitálním trhu;

- ZDŮRAZŇUJE, že legislativní práce k posílení certifikace kybernetické bezpečnosti na úrovni EU bude muset odpovídat potřebám trhu a uživatelů, vycházet ze zkušeností stávajících certifikačních kapacit a postupů v EU (například v rámci Poradního výboru pro bezpečnost informačních systémů) a měla by zajistit, aby bylo možné rychle se přizpůsobovat technické úrovni budoucího vývoje v digitální oblasti;

- ZDŮRAZŇUJE, že posílením certifikace kybernetické bezpečnosti v EU by mělo být pokryto celé spektrum bezpečnostních požadavků až po ty nejvyšší, u nichž je nutné prokázat odolnost vůči kapacitám útočníků. Mezi klíčové faktory úspěchu by patřilo zajištění spolehlivého a nezávislého procesu pro certifikaci bezpečnosti, díky němuž by byla podpořena dostupnost spolehlivých a bezpečných zařízení, softwaru a služeb v rámci jednotného trhu i mimo něj, uznávání příslušných specializací evropských průmyslových, vládních a hodnotících odborníků prostřednictvím evropských a celosvětových norem[14] a uznání úlohy členských států v procesu certifikace, zejména pokud jde o hodnocení na vyšších úrovních bezpečnosti, a zvláště s ohledem na posouzení základních potřeb a dovedností v oblasti bezpečnosti. Tento certifikační rámec by měl rovněž zajistit, aby byl jakýkoli celounijní systém certifikace úměrný úrovni zabezpečení potřebné k používání produktů, služeb nebo systémů informačních a komunikačních technologií a aby umožnil přeshraniční obchodování podnikům všech velikostí tak, aby mohly rozvíjet a prodávat nové výrobky jak na trzích EU, tak i mimo ně.

---

[13] Prostřednictvím celosvětových norem vypracovaných v souladu s duchem kodexu osvědčených postupů v oblasti technických překážek obchodu WTO.

[14] Prostřednictvím evropských a celosvětových norem vypracovaných v souladu s duchem kodexu osvědčených postupů v oblasti technických překážek obchodu WTO.

21. VÍTÁ záměr vytvořit síť center kompetencí pro kybernetickou bezpečnost za účelem stimulace vývoje a zavádění technologií v oblasti kybernetické bezpečnosti a s cílem poskytnout další impuls průmyslu EU v celosvětovém kontextu, pokud jde o inovace v rozvoji technologií příští generace a průlomových technologií, jako jsou umělá inteligence, kvantová výpočetní technika, technologie blockchain a bezpečné digitální identity;

22. ZDŮRAZŇUJE, že síť center kompetencí pro kybernetickou bezpečnost musí být inkluzivní ve vztahu ke všem členským státům a jejich stávajícím centrům excelence a kompetencí a že musí věnovat zvláštní pozornost doplňkovosti; a se zřetelem na výše uvedené BERE NA VĚDOMÍ plánované evropské centrum pro kybernetickou bezpečnost a výzkum, jehož hlavní úloha by se měla zaměřit na zajištění doplňkovosti a zamezení zdvojování v rámci sítě center kompetencí a s jinými agenturami EU;

23. ZDŮRAZŇUJE, že síť center kompetencí pro kybernetickou bezpečnost by se měla zaměřit na škálu oblastí od výzkumu po průmysl, a měla by tak přispět mimo jiné k dosažení cíle v podobě strategické nezávislosti Evropy;

24. S ohledem na vytvoření navrhované sítě center kompetencí pro kybernetickou bezpečnost OPĚTOVNĚ POTVRZUJE, že EU musí prostřednictvím svých členských států vyvinout evropskou kapacitu pro hodnocení úrovně šifrování používaného ve výrobcích a službách, které jsou občanům, podnikům a vládám k dispozici na jednotném digitálním trhu, a současně uznává, že politiky týkající se šifrování jsou klíčovým aspektem bezpečnosti státu, a spadají tudíž do pravomoci členských států;

25. VYZÝVÁ všechny příslušné zúčastněné strany, aby zvýšily investice do aplikací nových technologií v oblasti kybernetické bezpečnosti, a přispěly tím k zajištění kybernetické bezpečnosti ve všech odvětvích evropského hospodářství;

26. ZDŮRAZŇUJE, že služby v oblasti kybernetické bezpečnosti určené pro orgány EU musejí být poskytovány spolehlivým, důvěryhodným a koordinovaným způsobem, a VYBÍZÍ KOMISI a další orgány EU, aby v souladu s těmito cíli pokračovaly v dalším rozvoji činnosti CERT-EU a zajistily pro tyto účely rovněž dostatečné zdroje;

27. VÍTÁ výzvu, podle níž je třeba uznat důležitou úlohu nezávislých výzkumných pracovníků v oblasti bezpečnosti při zjišťování zranitelností existujících produktů a služeb, a VYBÍZÍ členské státy, aby sdílely osvědčené postupy koordinovaného zveřejňovaní informací o zranitelnosti;

28. ZDŮRAZŇUJE, že kybernetická bezpečnost je odpovědností všech, a vybízí EU i její členské státy, aby podporovaly digitální dovednosti a mediální gramotnost, díky nimž mohou uživatelé snáze chránit své digitální informace online a zvyšovat své povědomí o rizicích, jež se pojí k umísťování osobních údajů na internet.

29. VÍTÁ důraz, jejž společné sdělení klade na vzdělávání, kybernetickou hygienu a informovanost v členských státech i v EU;

30. VYZÝVÁ KOMISI, aby urychleně zajistila hodnocení dopadů týkající se provádění iniciativy, jejímž cílem je zřízení odborné sítě pro kybernetickou bezpečnost a Evropského výzkumného a odborného střediska, a aby do poloviny roku 2018 předložila příslušné právní nástroje pro její provádění;

31. VYZÝVÁ členské státy, aby:

- kladly důraz na povědomí o kybernetické bezpečnosti v informačních kampaních a pobízely k zahrnutí kybernetické bezpečnosti do vzdělávacích programů na akademické úrovni, jakož i do programů vzdělávání a odborné přípravy. Zvláštní pozornost by měla být věnována vzdělávání mladých lidí a rozvoji jejich digitálních dovedností, aby se z nich stali odborníci připravení na budoucnost a její výzvy v oblasti bezpečnosti, hospodářství a služeb;

- pokročily v přípravě specializovaných vzdělávacích programů na vysoké úrovni, jež budou zaměřeny na oblast kybernetické bezpečnosti a díky nimž bude možno odstranit nedostatek odborníků na kybernetickou bezpečnost, který v EU v současné době panuje;

- pod záštitou agentury ENISA vytvořily síť pro účinnou spolupráci kontaktních míst v oblasti vzdělávání. Tato kontaktní místa by měla usilovat o posílení spolupráce a výměn osvědčených postupů mezi členskými státy, pokud jde o vzdělávání a informovanost v oblasti kybernetické bezpečnosti, jakož i o odbornou přípravu, cvičení a budování kapacit;

- zvážily možnost uplatňovat pravidla směrnice o bezpečnosti sítí a informací i na orgány veřejné správy, jež se účastní sociálních nebo ekonomických činností kritického významu, nevztahují-li se na tyto orgány již odpovídající vnitrostátní právní předpisy a budou-li to členské státy považovat za vhodné, a aby s přihlédnutím k úloze, již orgány veřejné správy v naší společnosti a hospodářství plní, poskytovaly odbornou přípravu zaměřenou kybernetickou bezpečnost i jim.

Kapitola II

BUDOVÁNÍ KAPACITY EU V OBLASTI PŘEDCHÁZENÍ NEPŘÁTELSKÝM ČINNOSTEM V KYBERPROSTORU, ODRAZOVÁNÍ OD NICH, JEJICH ODHALOVÁNÍ A REAKCE NA NĚ

32. ZDŮRAZŇUJE, ŽE mimořádně závažný kybernetický incident nebo krize by mohly danému členskému státu zavdat dostatečný důvod k uplatnění doložky solidarity EU[15] nebo doložky o vzájemné pomoci[16];

33. VÍTÁ přijetí „rámce pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru“, jenž je přispěním k předcházení konfliktům a ke spolupráci a stabilitě v kyberprostoru, neboť vymezuje opatření v rámci SZBP včetně opatření omezujících, k nimž lze v zájmu předcházení nepřátelské činnosti a reakce na ni přistoupit, a VYBÍZÍ ESVČ i členské státy, aby v souvislosti s uvedeným rámcem realizovaly pravidelná cvičení;

---

15 Článek 222 SFEU.
16 Článek 42 odst. 7 SEU.

34. ZDŮRAZŇUJE, že aniž by byly dotčeny pravomoci členských států, na kybernetické incidenty a krize velkého rozsahu je třeba účinně reagovat na úrovni EU a že kybernetická bezpečnost by měla být začleněna do existujících mechanismů pro řešení krizí na úrovni EU[17]. VYZÝVÁ za tímto účelem k pravidelným cvičením v oblasti reakce EU na kybernetické incidenty velkého rozsahu, od reakcí diplomaticko-strategické povahy až po reakce technického rázu, přičemž tato cvičení by měla být založena na relevantních rámcích a postupech, jež by měla v případě potřeby zdokonalovat[18];

35. VYZDVIHUJE význam řádně integrovaných mechanismů reakce a výměny informací mezi různými komunitami, neboť takové mechanismy jsou pro zajištění kybernetické bezpečnosti v Evropě klíčové, a to i pokud jde o interakci mezi příslušnými subjekty EU a orgány členských států. Tyto mechanismy je nutno testovat a ověřovat v rámci cvičení v oblasti kybernetické bezpečnosti na úrovni EU a v případě potřeby je formalizovat vhodnými dohodami;

36. POUKAZUJE na možnost prověřit návrh – pokud by jej Komise předložila – na zřízení fondu pro reakci při mimořádných událostech v oblasti kybernetické bezpečnosti, jenž by fungoval souběžně se stávajícími činnostmi členských států a při zohlednění dostupných zdrojů (zejména v mezích víceletého finančního rámce EU), a to s cílem pomoci členským státům v reakcích na kybernetické incidenty velkého rozsahu za předpokladu, že dotčený členský stát již před daným incidentem disponuje obezřetnostním systémem kybernetické bezpečnosti zahrnujícím mimo jiné plné provedení směrnice o bezpečnosti sítí a informací a vyspělé rámce řízení rizik a dohledu na vnitrostátní úrovni;

37. UZNÁVÁ, že se prohlubuje propojenost kybernetické bezpečnosti a obrany, a VYBÍZÍ k intenzivnější spolupráci v oblasti kybernetické obrany, mimo jiné k podpoře spolupráce mezi civilními a vojenskými pracovníky činnými na poli reakce na incidenty, a dále k pokračujícímu posilování kybernetické bezpečnosti misí a operací SBOP;

---

17 Dokument C/2017/6100 final.
18 Dokumenty 9916/17 a C/2017/6100 final.

38. ZDŮRAZŇUJE, že je třeba pokud možno v plné míře využít potenciál navrhovaných obranných iniciativ v zájmu rychlejšího rozvoje adekvátních evropských schopností v oblasti kybernetiky, UZNÁVÁ příležitosti pojící se k možnosti vývoje projektů kybernetické obrany prostřednictvím stálé strukturované spolupráce, budou-li to členské státy účastnící se stálé strukturované spolupráce považovat za nezbytné, a UZNÁVÁ úlohu evropské obranné technologické a průmyslové základny, jakož i širší civilní základny odvětví kybernetické bezpečnosti, neboť obě poskytují členským státům prostředky k zajištění zájmů v oblasti kybernetické bezpečnosti a obrany;

39. BERE NA VĚDOMÍ návrh Komise, podle něhož by měla být do konce roku 2018 zavedena platforma pro vzdělávání a odbornou přípravu v oblasti kybernetické obrany, a ZDŮRAZŇUJE, že tato platforma by měla rozšířit příležitosti ke vzdělávání a odborné přípravě v členských státech a zajistit doplňkovost s dalšími činnostmi a iniciativami EU, především s Evropskou bezpečnostní a obrannou školou a s Evropskou obrannou agenturou;

40. VYBÍZÍ EU a její členské státy k připravenosti, pokud jde o hrozbu krádeží duševního vlastnictví za využití informačních a komunikačních technologií, mimo jiné co se týče obchodních tajemství nebo dalších důvěrných obchodních informací, a to s cílem získat konkurenční výhodu pro určité společnosti nebo obchodní odvětví;

41. UZNÁVÁ, že je třeba bojovat proti trestné činnosti páchané v kyberprostoru včetně temného webu (dark web), proti pohlavnímu zneužívání dětí prostřednictvím internetu a proti podvodným a padělaným bezhotovostním platebním prostředkům, a že je třeba se v tomto ohledu zejména zaměřit na utváření kvalitnějšího zpravodajského obrazu, vedení společného vyšetřování a sdílení operační podpory;

42. VÍTÁ činnost EU a jejích členských států zaměřenou na řešení výzev v podobě systémů, díky nimž jsou pachatelé trestné činnosti a teroristé schopni komunikovat způsoby vymykajícími se možnosti přístupu ze strany příslušných orgánů, a ZDŮRAZŇUJE, že tato činnost musí brát zřetel na silné a důvěryhodné šifrování, které má zásadní význam pro kybernetickou bezpečnost, důvěru v jednotný digitální trh a zajištění dodržování lidských práv a základních svobod;

43. ZDŮRAZŇUJE, že je důležité poskytnout donucovacím orgánům nástroje, jejichž prostřednictvím budou schopny kyberkriminalitu odhalovat, vyšetřovat a stíhat, a zajistit tak, že trestné činy páchané v kyberprostoru nezůstanou bez povšimnutí nebo bez trestu, a VÍTÁ přínos evropské justiční sítě pro boj proti kyberkriminalitě, která v boji proti trestné činnosti napomáhá na základě spolupráce justičních orgánů;

44. ZDŮRAZŇUJE, že je důležité zajistit koordinovaný postoj EU, aby bylo možno v rámci společenství mnoha zúčastněných stran účinně formulovat rozhodnutí týkající se správy internetu na evropské i světové úrovni, přičemž se jedná například o zajištění rychle přístupných a přesných databází WHOIS obsahujících IP adresy a doménová jména, a to s cílem zabezpečit schopnosti donucovacích orgánů a veřejné zájmy;

45. ZDŮRAZŇUJE, že je důležité zavést internetový protokol IPv6, který má zásadní význam pro náležitý vývoj internetu věcí, jakož i pro lepší přisuzování trestných činů v kyberprostoru jejich pachatelům;

46. VYSLOVUJE PODPORU probíhající činnosti zaměřené na přeshraniční přístup k elektronickým důkazům, na vyřešení otázky uchovávání údajů a na výzvy, jež pro trestní řízení představují systémy, díky nimž jsou pachatelé trestné činnosti a teroristé schopni komunikovat způsoby vymykajícími se možnosti přístupu ze strany příslušných orgánů, a to se zřetelem na skutečnost, že je nutno respektovat lidská práva, základní svobody a ochranu údajů;

47. VYZÝVÁ Komisi, aby:

- do prosince roku 2017 předložila zprávu o pokroku v provádění praktických opatření pro zlepšení přeshraničního přístupu k elektronickým důkazům;
- na počátku roku 2018 předložila legislativní návrh na zlepšení přeshraničního přístupu k elektronickým důkazům;

48. VYZÝVÁ Europol, agenturu ENISA a Eurojust, aby:

- nadále posilovaly svou spolupráci v boji proti kyberkriminalitě, jak mezi sebou navzájem, tak i s dalšími příslušnými zúčastněnými stranami včetně pracovníků sítě skupin CSIRT, Interpolu, soukromého sektoru a akademické obce, a aby zajišťovaly součinnost a komplementaritu v souladu s mandáty a pravomocemi všech stran;

- spolu s členskými státy přispívaly ke koordinovanému přístupu v oblasti reakce donucovacích orgánů EU na kybernetické incidenty a krize velkého rozsahu, a doplňovaly tak postupy vymezené v příslušných rámcích[19];

49. VYZÝVÁ EU a její členské státy, aby pokračovaly v činnosti s cílem:

- odstranit překážky, jež brání vyšetřování trestné činnosti a účinnému uskutečňování trestního soudnictví v kyberprostoru, a posílit v oblasti boje proti trestné činnosti v kyberprostoru mezinárodní spolupráci a koordinaci;

- řešit výzvy, které vyvstávají v souvislosti s technologiemi umožňujícími anonymizaci, a to se zřetelem ke skutečnosti, že zásadní význam pro kybernetickou bezpečnost a důvěru v jednotný digitální trh má silné a důvěryhodné šifrování;

- formulovat rozhodnutí týkající se správy internetu, která mají dopad na schopnost donucovacích orgánů bojovat proti trestné činnosti v kyberprostoru.

[19] Dokumenty 9916/17 a C/2017/6100 final.

Kapitola III

POSILOVÁNÍ MEZINÁRODNÍ SPOLUPRÁCE V ZÁJMU ZAJIŠTĚNÍ OTEVŘENÉHO, SVOBODNÉHO, POKOJNÉHO A BEZPEČNÉHO GLOBÁLNÍHO KYBERPROSTORU

50. UZNÁVÁ, že zajištění kybernetické bezpečnosti je globální výzvou, která vyžaduje účinnou globální spolupráci mezi všemi aktéry, a UZNÁVÁ, že zvláštní důraz musí být kladen na zachovávání demokratických hodnot a zásad otevřeného, svobodného, pokojného a bezpečného kyberprostoru v celosvětovém měřítku, a v této souvislosti

51. VYZÝVÁ EU a její členské státy, aby se zasazovaly o zřízení strategického rámce pro předcházení konfliktům, spolupráci a stabilitu v kyberprostoru, jenž bude založen na uplatňování stávajícího mezinárodního práva, zejména pak Charty OSN v plném rozsahu, a dále o vypracování a provádění všeobecných norem odpovědného chování států a opatření pro budování důvěry mezi státy na úrovni regionů;

52. UZNÁVÁ úlohu Organizace spojených národů v dalším vývoji norem pro odpovědné chování státu v kyberprostoru a připomíná, že ve výstupech jednání skupiny vládních odborníků OSN za několik let byl formulován konsensuální soubor norem a doporučení, který Valné shromáždění OSN opakovaně potvrdilo a který by státy měly považovat za základ odpovědného chování státu v kyberprostoru;

53. UZNÁVÁ, že mezi tyto normy odpovědného chování státu patří zásada, podle níž by státy neměly vědomě umožňovat, aby jejich území bylo využíváno pro páchání činů v rozporu s mezinárodním právem, měly by reagovat na přiměřené žádosti o pomoc ze strany jiného státu, jehož kritická infrastruktura se stala předmětem nepřátelské kybernetické činnosti páchané z jejich území, a měly by přijmout vhodná opatření k ochraně vlastní kritické infrastruktury před kybernetickými hrozbami;

54. UZNÁVÁ, že EU, NATO a jejich členské státy čelí sdíleným kybernetickým hrozbám a rizikům, a OPĚTOVNĚ VYZDVIHUJE význam pokračující spolupráce EU a NATO v oblastech kybernetické bezpečnosti a obrany, při plném zachování zásad inkluzivnosti, reciprocity a rozhodovací autonomie EU a v souladu se svými závěry ze dne 6. prosince 2016 o provádění společného prohlášení předsedy Evropské rady, předsedy Evropské komise a generálního tajemníka Severoatlantické aliance[20];

55. VYZÝVÁ EU a její členské státy, aby poskytovaly podporu a motivaci rozvoji regionálních opatření pro budování důvěry, neboť taková opatření jsou klíčovým prvkem pro posilování spolupráce a transparentnosti a snižují riziko střetu zájmů. Uplatňování opatření k budování důvěry v oblasti kybernetické bezpečnosti na úrovni OBSE i v jiných regionálních kontextech povede k vyšší předvídatelnosti chování států a dále přispěje ke stabilizaci kyberprostoru;

56. OPĚTOVNĚ POTVRZUJE, že v návaznosti na obecné zásady EU v oblasti lidských práv ohledně svobody na internetu bude EU i nadále prosazovat své klíčové hodnoty, pokud jde o ochranu lidských práv a základních svobod. Kromě toho EU zdůrazňuje význam zapojení všech zúčastněných stran do správy internetu, a to včetně akademické obce, občanské společnosti a soukromého sektoru;

57. VYZÝVÁ EU a její členské státy, aby podporovaly budování kybernetických kapacit ve třetích zemích, se zvláštním důrazem na země sousedící s EU a na rozvojové země, v nichž dochází k rychlému nárůstu připojení, a to v zájmu boje proti kyberkriminalitě a posilování kybernetické odolnosti v souladu se základními hodnotami EU. Na podporu úsilí EU v této oblasti by měla být vytvořena síť EU pro budování kybernetických kapacit spolu s pokyny EU pro budování kybernetických kapacit, jimiž by měly být doplněny stávající mechanismy s struktury;

---

[20] Dokument 15283/16.

58. VYZDVIHUJE pokrok, jehož bylo ve spolupráci EU a NATO v oblasti kybernetické obrany a bezpečnosti dosaženo, rozvoj této spolupráce na rovině odborné přípravy, vzdělávání a koncepcí, aniž by docházelo ke zdvojování činností v oblastech, kde se překrývají požadavky, jakož i rozvíjení interoperability prostřednictvím požadavků na kybernetickou obranu a norem, a VYBÍZÍ k další spolupráci, pokud jde o cvičení v oblasti kybernetické obrany (na úrovni personálu), a ke sdílení osvědčených postupů v řízení krizí, aniž by docházelo ke zdvojování činností v oblastech, kde se překrývají požadavky, za plného dodržení politiky EU v oblasti cvičení a zásad inkluzivnosti, reciprocity a rozhodovací autonomie EU;

59. UZNÁVÁ, že Úmluva Rady Evropy o počítačové trestné činnosti (Budapešťská úmluva) nabízí efektivní právní standard, z nějž mohou vycházet vnitrostátní právní předpisy o kyberkriminalitě; VYZÝVÁ všechny země, aby vypracovaly vhodné vnitrostátní právní rámce a pokračovaly ve spolupráci v existujícím mezinárodním rámci, jejž Budapešťská úmluva poskytuje;

60. PŘIPOMÍNÁ úspěchy dosažené v rámci dvoustranných dialogů EU o kyberprostoru a vybízí k dalšímu úsilí, jímž by byla usnadněna spolupráce v oblasti kybernetické bezpečnosti se třetími zeměmi;

61. PŘIPOMÍNÁ, že EU disponuje spolehlivým a právně závazným mechanismem kontroly vývozu, jenž vychází z rozhodnutí a osvědčených postupů vypracovaných v rámci mezinárodních režimech pro nešíření, BERE NA VĚDOMÍ probíhající jednání v Radě, jejichž účelem je identifikovat nejlepší způsoby, jak fungování uvedených kontrol dále zkvalitnit, a VYBÍZÍ členské státy, aby v rámci příslušných mezinárodních režim*ů* pro kontrolu vývozu (např. Wassenaarské ujednání) pokračovaly v činnosti zaměřené na aplikace nových technologií vyžadující kybernetickou bezpečnost nejvyšší úrovně, a to v zájmu zajištění účinné kontroly nových technologií vyžadujících kybernetickou bezpečnost nejvyšší úrovně v nejbližší budoucnosti;

62. V návaznosti na závěry Evropské rady ze dne 19. října 2017[21] budou tyto závěry prováděny prostřednictvím akčního plánu, který má Rada přijmout do konce roku 2017. Tento akční plán bude otevřeným dokumentem, pravidelně revidovaným a aktualizovaným Radou.

---

[21] Dokument EUCO 14/17.