Rada
Európskej únie

V Bruseli 20. novembra 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

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	20. novembra 2017
Komu:	Delegations
Č. predch. dok.:	13943/17 + COR 1
Č. dok. Kom.:	12210/17, 12211/17
Predmet:	Závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ – závery Rady (20. novembra 2017)

Delegáciám v prílohe zasielame závery Rady o spoločnom oznámení Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ, ktoré prijala Rada pre všeobecné záležitosti 20. novembra 2017.

PRÍLOHA

Návrh záverov Rady o spoločnom oznámení EP a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ

Rada Európskej únie,

1. UZNÁVAJÚC význam kybernetickej bezpečnosti pre prosperitu, rast a bezpečnosť EÚ a integritu našich slobodných a demokratických spoločností a ich východiskové procesy v digitálnom veku, a to prostredníctvom ochrany právneho štátu a ľudských práv a základných slobôd každého jednotlivca;

2. ZDÔRAZŇUJÚC potrebu koherentného prístupu ku kybernetickej bezpečnosti na vnútroštátnej, európskej a celosvetovej úrovni, keďže kybernetické hrozby môžu mať vplyv na našu demokraciu, prosperitu, stabilitu a bezpečnosť;

3. KONŠTATUJÚC, že vysoká úroveň kybernetickej odolnosti v celej EÚ je takisto dôležitá na dosiahnutie dôvery v digitálny jednotný trh a pre ďalší rozvoj digitálnej Európy;

4. POTVRDZUJÚC, že EÚ bude naďalej podporovať otvorený, globálny, slobodný, pokojný a bezpečný kybernetický priestor, v ktorom sa v rámci EÚ aj v celosvetovom meradle plne uplatňujú a dodržiavajú ľudské práva a základné slobody, najmä právo na slobodu prejavu, prístup k informáciám, ochranu údajov, súkromie a bezpečnosť, ako aj kľúčové hodnoty a zásady EÚ, a ZDÔRAZŇUJÚC, že je veľmi dôležité zabezpečiť primeranú rovnováhu medzi ľudskými právami a základnými slobodami a splniť požiadavky politiky vnútornej bezpečnosti EÚ[1],

5. UZNÁVAJÚC, že v kybernetickom priestore platí medzinárodné právo vrátane Charty OSN v jej plnom rozsahu, medzinárodného humanitárneho práva a práva v oblasti ľudských práv, a ZDÔRAZŇUJÚC, že je potrebné pokračovať v úsilí o zabezpečenie toho, aby sa medzinárodné právo v kybernetickom priestore dodržiavalo;

[1] 12650/17.

6. PRIPOMÍNAJÚC svoje závery o stratégii kybernetickej bezpečnosti EÚ[2], o správe internetu[3], o posilnení kybernetickej odolnosti EÚ[4], o kybernetickej diplomacii[5] a o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti[6], o zlepšení trestnej justície v kybernetickom priestore[7]; o bezpečnosti a obrane v rámci globálnej stratégie EÚ[8], spoločnom rámci pre boj proti hybridným hrozbám[9] a o preskúmaní obnovenej stratégie vnútornej bezpečnosti Európskej únie na roky 2015 – 2020 v polovici jej trvania[10];

7. UZNÁVAJÚC, že rámec, ktorý poskytuje Dohovor Rady Európy o počítačovej kriminalite (Budapeštiansky dohovor), zabezpečuje pevný základ pre rôznorodú skupinu krajín na to, aby využívali účinnú právnu normu pre rôzne vnútroštátne právne predpisy a na medzinárodnú spoluprácu v boji proti počítačovej kriminalite;

8. UZNÁVAJÚC potrebu obnoviť dôraz na vykonávanie politického rámca EÚ pre kybernetickú obranu z roku 2014 a aktualizovať ho s cieľom ďalšej integrácie kybernetickej bezpečnosti a obrany do spoločnej bezpečnostnej a obrannej politiky (SBOP) a širšieho programu v oblasti bezpečnosti a obrany;

9. UZNÁVAJÚC, že globálne konkurencieschopný európsky priemysel je dôležitým prvkom na dosiahnutie vysokej úrovne kybernetickej bezpečnosti na vnútroštátnej úrovni a v celej EÚ;

10. PRIPOMÍNAJÚC, že podľa článku 4 ods. 2 ZEÚ je národná bezpečnosť vo výlučnej zodpovednosti každého členského štátu.

---

2 12109/13 a 6225/13 (spoločné oznámenie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Stratégia kybernetickej bezpečnosti Európskej únie: otvorený, bezpečný a chránený kybernetický priestor (COM JOIN(2013) 1 final)).

3 16200/14 a 6460/14 (oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Politika a riadenie v oblasti internetu – Úloha Európy pri formovaní budúcnosti riadenia internetu (COM(2014) 72 final)).

4 14540/16 a 11013/16 (oznámenie Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov: Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe (COM 2016(410) final)).

5 6122/15.

6 9916/17.

7 10007/16.

8 9178/17.

9 7688/16 (spoločné oznámenie Európskemu parlamentu a Rade: Spoločný rámec pre boj proti hybridným hrozbám: reakcia Európskej únie).

10 12650/17.

TÝMTO:

11. VÍTA spoločné oznámenie Európskemu parlamentu a Rade s názvom Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ, pretože sa v ňom predkladá ambiciózny cieľ, ktorým je posilnenie kybernetickej bezpečnosti v EÚ. Takisto sa ním prispieva k strategickej autonómii EÚ, ako sa uvádza v záveroch Rady o Globálnej stratégii pre zahraničnú a bezpečnostnú politiku Európskej únie[11], tým, že sa zameriava na vybudovanie digitálnej Európy, ktorá bude bezpečnejšia, dôveryhodná, vedomá si svojich silných stránok, konkurencieschopná, otvorená svetu, rešpektujúca spoločné hodnoty EÚ týkajúce sa otvoreného, slobodného, pokojného a bezpečného globálneho internetu – a preto dosahujúca vyššiu úroveň odolnosti pri predchádzaní kybernetickým hrozbám, odrádzaní od nich, ich odhaľovaní a pri reakcii na ne a ktorá tiež bude schopná spoločne reagovať na kybernetické hrozby v celej EÚ, a

12. VYZÝVA členské štáty a inštitúcie, agentúry a orgány EÚ aby spolupracovali, rešpektujúc vzájomne svoje právomoci a zásady subsidiarity a proporcionality, a reagovali tak na strategické ciele uvedené v týchto záveroch, a

13. ZDÔRAZŇUJE, že je potrebné, aby EÚ, jej členské štáty a súkromný sektor zabezpečili dostatočné financovanie – pri rešpektovaní dostupných zdrojov – na podporu budovania kybernetickej odolnosti a na výskumné a vývojové činnosti v oblasti kybernetickej bezpečnosti v celej EÚ, ako aj na posilnenie spolupráce s cieľom predchádzať kybernetickým hrozbám, odrádzať od nich, odhaľovať ich a reagovať na ne a na zabezpečenie schopnosti reagovať spoločne na rozsiahle kybernetické incidenty a škodlivé kybernetické činnosti v celej EÚ;

---

[11] 13202/16.

Kapitola I

ZABEZPEČENIE ÚČINNEJ KYBERNETICKEJ ODOLNOSTI EÚ A DÔVERY V DIGITÁLNY JEDNOTNÝ TRH

14. ZDÔRAZŇUJE, že každý členský štát nesie hlavnú zodpovednosť za posilnenie vlastnej kybernetickej bezpečnosti a zabezpečenie svojej reakcie na kybernetické incidenty a krízy, zatiaľ čo EÚ môže poskytnúť výraznú pridanú hodnotu podporou spolupráce medzi členskými štátmi. V tomto kontexte ZDÔRAZŇUJE, že je potrebné, aby všetky členské štáty dali vnútroštátnym orgánom zodpovedným za kybernetickú bezpečnosť k dispozícii potrebné zdroje na zaistenie predchádzania kybernetickým incidentom a krízam v celej EÚ, ich odhaľovania a reakcie na ne;

15. ZDÔRAZŇUJE potrebu podľa možností využívať existujúce mechanizmy, štruktúry a organizácie na úrovni EÚ;

16. OCEŇUJE:

- pokrok, ktorý dosiahli členské štáty pri transpozícii smernice NIS a ZDÔRAZŇUJE potrebu dosiahnuť jej úplné a účinné vykonávanie do mája 2018, ako sa stanovuje v danej smernici[12];
- prácu vykonanú v rámci skupiny pre spoluprácu v oblasti kybernetickej bezpečnosti pri posilňovaní strategickej spolupráce a výmeny informácií medzi členskými štátmi;
- prácu vykonanú v rámci siete jednotiek CSIRT, najmä pokiaľ ide o posilňovanie operačnej spolupráce členských štátov, budovanie dôvery pri výmene informácií pri riešení rozsiahlych kybernetických incidentov a – na základe vnútroštátnych záverov v členských štátov – pri poskytovaní prvkov pre spoločné situačné povedomie na európskej úrovni;
- prácu vykonanú v rámci zmluvného verejno-súkromného partnerstva (cPPP) v oblasti kybernetickej bezpečnosti.

[12] Bez toho, aby boli dotknuté právomoci členských štátov, pokiaľ ide o transpozíciu smernice NIS, najmä pokiaľ ide o prevádzkovateľov základných služieb.

17. VÍTA potvrdenie v spoločnom oznámení, že silné a dôveryhodné šifrovanie je veľmi dôležité pre riadne zaručenie ľudských práv a základných slobôd v EÚ a pre dôveru verejnosti v digitálny jednotný trh, pričom treba zohľadniť aj potrebu orgánov presadzovania práva na prístup k údajom potrebným na vyšetrovanie, ako aj potvrdenie, že bezpečná digitálna identifikácia a komunikácia zohrávajú kľúčovú úlohu pri zabezpečovaní účinnej kybernetickej bezpečnosti v EÚ;

18. VÍTA plán v spoločnom oznámení na zvýšenie ambícií pravidelnými celoeurópskymi cvičeniami v oblasti kybernetickej bezpečnosti, pričom sa bude vychádzať zo skúseností z cvičení Cyber Europe a spájať reakcia na rôznych úrovniach, keďže to bude dôležitým prvkom pri zlepšovaní pripravenosti členských štátov a inštitúcií EÚ pri reagovaní na rozsiahle kybernetické incidenty;

19. VYZÝVA EÚ a jej členské štáty, aby vykonávali pravidelné strategické cvičenia v oblasti kybernetickej bezpečnosti v rôznych zloženiach Rady, a to na základe skúseností získaných počas cvičenia ministrov obrany EU CYBRID 2017, a

20. Bez toho, aby bol dotknutý výsledok legislatívneho procesu:

- VÍTA návrh na udelenie pevného a trvalého mandátu agentúre ENISA s hlavným cieľom podporovať a rozvíjať užšiu spoluprácu medzi členskými štátmi, zvyšovať ich kapacity a zvyšovať dôveru v digitálnu Európu;

- OPÄTOVNE POTVRDZUJE, že budúca agentúra ENISA by mala využívať skúsenosti a odbornosť v rámci členských štátov a EÚ a podporovať konzistentný vývoj a vykonávanie existujúcich a budúcich politík a právnych predpisov EÚ v oblasti kybernetickej bezpečnosti, pričom by sa malo zabezpečiť, aby sa všetky spôsobilosti agentúry ENISA rozvíjali ako doplnok spôsobilostí členských štátov;

- OPÄTOVNE POTVRDZUJE cieľ, ktorým je rastúca dôvera v digitálnu Európu zvýšením dôvery v digitálne riešenia a inovácie vrátane internetu vecí, elektronického obchodu a elektronickej správy vecí verejných, a to najmä pokiaľ ide o európsky rámec certifikácie kybernetickej bezpečnosti[13] na svetovej úrovni. Toto je kľúčová požiadavka pre posilnenie dôvery a bezpečnosti v oblasti digitálnych produktov a služieb, pre ochranu kritickej infraštruktúry, vládnych, občianskych a podnikových údajov, pričom je zásadná pri prijímaní prístupu založeného na bezpečnosti už v štádiu návrhu (security-by-design) pre produkty, služby a procesy v rámci digitálneho jednotného trhu;

- ZDÔRAZŇUJE, že legislatívne úsilie s cieľom posilniť certifikáciu kybernetickej bezpečnosti na úrovni EÚ bude musieť zodpovedať potrebám trhu a používateľov, stavať na skúsenostiach s certifikačnými kapacitami a postupmi existujúcimi v EÚ (napríklad na rámci SOG-IS) a muselo by poskytnúť rámec schopný rýchlo sa prispôsobiť najnovšiemu vývoju v oblasti digitálnych technológií v budúcnosti;

- ZDÔRAZŇUJE, že pri skvalitňovaní certifikácie kybernetickej bezpečnosti v EÚ by sa malo pokryť celé spektrum bezpečnostných požiadaviek, a to až po tie najprísnejšie, kde treba preukázať odolnosť proti schopnostiam útočníkov. Kľúčovými faktormi pre úspech by bolo zabezpečenie spoľahlivého, transparentného a nezávislého procesu certifikácie bezpečnosti s cieľom podporovať dostupnosť dôveryhodných a bezpečných zariadení, softvéru a služieb v rámci jednotného trhu aj mimo neho; uznávanie príslušných odborných znalostí špecialistov z európskeho priemyslu, vládnych špecialistov a špecialistov na hodnotenie prostredníctvom európskych a globálnych noriem[14]; rešpektovanie úlohy členských štátov v procese certifikácie, najmä pokiaľ ide o hodnotenie na vyšších úrovniach bezpečnosti, a predovšetkým v súvislosti so základnými bezpečnostnými potrebami a hodnotením zručností. Takýmto rámcom certifikácie by sa tiež malo zabezpečiť, aby bol každý celoúnijný certifikačný systém primeraný úrovni bezpečnosti, ktorá je potrebná na využívanie príslušných IKT produktov, služieb a/alebo systémov, a aby umožňoval podnikom všetkých veľkostí pri cezhraničnom obchode vyvíjať a predávať nové produkty, a to v rámci trhov EÚ aj mimo nich.

---

[13] Prostredníctvom globálnych noriem vypracovaných v duchu kódexu osvedčených postupov WTO v oblasti technických prekážok obchodu.

[14] Prostredníctvom európskych a globálnych noriem vypracovaných v duchu kódexu osvedčených postupov WTO v oblasti technických prekážok obchodu.

21. VÍTA zámer vytvoriť sieť stredísk pre spôsobilosti v oblasti kybernetickej bezpečnosti s cieľom podnietiť vývoj a zavádzanie technológií kybernetickej bezpečnosti a poskytnúť ďalší impulz pre priemysel EÚ na inováciu vo svetovom meradle pri rozvoji technológií novej generácie a prelomových technológií, ako je napríklad umelá inteligencia, kvantová informatika, technológia blockchain a bezpečné digitálne identity;

22. ZDÔRAZŇUJE, že je potrebné, aby bola sieť stredísk pre spôsobilosti v oblasti kybernetickej bezpečnosti inkluzívna pre všetky členské štáty a ich existujúce centrá excelentnosti a spôsobilostí a aby venovala osobitnú pozornosť komplementarite, a vzhľadom na túto skutočnosť BERIE NA VEDOMIE plánované Európske stredisko výskumu a kompetencií pre kybernetickú bezpečnosť, ktorého kľúčovou úlohou by malo byť zamerať sa na zabezpečenie komplementárnosti a predchádzanie zdvojovaniu v rámci siete stredísk pre spôsobilosti v oblasti kybernetickej bezpečnosti a s inými agentúrami EÚ;

23. ZDÔRAZŇUJE, že sieť stredísk pre spôsobilosti v oblasti kybernetickej bezpečnosti by sa mala zaoberať širokou škálou otázok od výskumu k priemyslu, a preto by mala okrem iného prispieť k dosiahnutiu cieľa, ktorým je európska strategická autonómia;

24. Vzhľadom na navrhovanú sieť stredísk pre spôsobilosti v oblasti kybernetickej bezpečnosti, OPÄTOVNE POTVRDZUJE, že treba, aby EÚ prostredníctvom svojich členských štátov vytvorila európsku kapacitu na hodnotenie sily kryptografie používanej v produktoch a službách dostupných pre občanov, podniky a vlády v rámci digitálneho jednotného trhu, pričom uznáva, že politika v oblasti kryptografie je kľúčovým aspektom národnej bezpečnosti, a teda patrí do právomoci členských štátov;

25. VYZÝVA všetky relevantné zainteresované strany, aby zvýšili investície do aplikácií kybernetickej bezpečnosti v rámci nových technológií s cieľom prispieť k zabezpečeniu kybernetickej bezpečnosti vo všetkých odvetviach európskeho hospodárstva;

26. ZDÔRAZŇUJE význam spoľahlivého, dôveryhodného a koordinovaného poskytovania služieb kybernetickej bezpečnosti pre inštitúcie EÚ a VYZÝVA KOMISIU a ostatné inštitúcie EÚ, aby ďalej rozvíjali tím CERT-EU podľa týchto cieľov a zabezpečili na to aj primerané zdroje;

27. VÍTA výzvu na uznanie dôležitej úlohy výskumných pracovníkov z tretích strán pri objavovaní slabých miest existujúcich produktov a služieb a VYZÝVA členské štáty, aby si vymieňali najlepšie postupy týkajúce sa koordinácie odhaľovania zraniteľnosti;

28. ZDÔRAZŇUJE, že za kybernetickú bezpečnosť sme zodpovední všetci, a VYZÝVA EÚ a jej členské štáty, aby presadzovali digitálne zručnosti a mediálnu gramotnosť, a tak pomáhali používateľom pri ochrane ich online digitálnych informácií a zvyšovali ich informovanosť o rizikách pri ukladaní osobných údajov na internete;

29. VÍTA dôraz, ktorý sa v spoločnom oznámení kladie na vzdelávanie, počítačovú hygienu a informovanosť v členských štátoch a EÚ;

30. Vyzýva KOMISIU, aby urýchlene poskytla hodnotenie vplyvu iniciatívy, ktorou sa zriaďuje sieť stredísk pre spôsobilosti v oblasti kybernetickej bezpečnosti a Európske stredisko výskumu a kompetencií pre kybernetickú bezpečnosť, a do polovice roka 2018 navrhla príslušné právne nástroje na jej vykonávanie;

31. VYZÝVA členské štáty, aby:

- priorizovali informovanosť o kybernetickej bezpečnosti v rámci informačných kampaní a zahŕňali kybernetickú bezpečnosť do akademických a vzdelávacích programov, ako aj programov odbornej prípravy. Osobitný dôraz by sa mal klásť na vzdelávanie mládeže a podporu digitálnych zručností s cieľom vychovať odborníkov pre budúcnosť pripravených na výzvy v oblasti bezpečnosti, hospodárstva a služieb;

- pokročili v úsilí zameranom na otvorenie špecializovaných programov v oblasti kybernetickej bezpečnosti na vysokej úrovni s cieľom zaplniť súčasný nedostatok odborníkov na oblasť kybernetickej bezpečnosti v EÚ;

- vytvorili účinnú sieť pre spoluprácu kontaktných miest v oblasti vzdelávania pod záštitou agentúry ENISA. Cieľom tejto siete kontaktných miest by malo byť posilnenie koordinácie a výmeny najlepších postupov medzi členskými štátmi v oblasti vzdelávania a informovanosti o kybernetickej bezpečnosti, ako aj odbornej prípravy, cvičení a budovania kapacít v tejto oblasti;

- zvážili uplatňovanie pravidiel smernice NIS aj na orgány verejnej správy, ktoré sa zúčastňujú na rozhodujúcich spoločenských alebo hospodárskych činnostiach, ak to už nie je zachytené vo vnútroštátnych právnych predpisoch a ak sa to považuje za vhodné, a aby poskytovali odbornú prípravu týkajúcu sa kybernetickej bezpečnosti aj vo verejnej správe, vzhľadom na úlohu, ktorú zohráva v našej spoločnosti a hospodárstve.

Kapitola II

BUDOVANIE KAPACITY EÚ NA PREDCHÁDZANIE ŠKODLIVÝM KYBERNETICKÝM ČINNOSTIAM, ODRÁDZANIE PRED NIMI, ICH ODHAĽOVANIE A REAGOVANIE NA NE

32. ZDÔRAZŇUJE, že obzvlášť závažný kybernetický incident alebo kríza by pre členský štát mohli predstavovať dostatočný dôvod na uplatnenie doložky o solidarite EÚ[15] a/alebo doložky o vzájomnej pomoci[16].

33. VÍTA prijatie „rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti“, ktorý prispieva k prevencii konfliktov, spolupráci a stabilite v kybernetickom priestore, keďže sa v ňom stanovujú opatrenia v rámci SZBP vrátane reštriktívnych opatrení, ktoré možno použiť na predchádzanie úmyselným kybernetickým činnostiam a reakciu na ne, a VYZÝVA ESVČ a členské štáty, aby pravidelne vykonávali cvičenia týkajúce sa tohto rámca;

---

15 článok 222 ZFEÚ.
16 článok 42,7 ZFEÚ.

34. ZDÔRAZŇUJE potrebu účinnej reakcie na úrovni EÚ na rozsiahle kybernetické incidenty a krízy, a to pri rešpektovaní právomocí členských štátov, a potrebu, aby sa kybernetická bezpečnosť začlenila do existujúcich mechanizmov krízového riadenia na úrovni EÚ[17]. V záujme dosiahnutia tohto cieľa VYZÝVA na to, aby sa konali pravidelné cvičenia reakcie na úrovni EÚ na rozsiahle kybernetické incidenty – a to od diplomaticko-strategickej až po technickú reakciu – vychádzajúce podľa potreby z príslušných rámcov a postupov a podľa potreby aj upravujúce tieto rámce a postupy[18];

35. ZDÔRAZŇUJE význam dobre integrovaných mechanizmov reakcie a výmeny informácií medzi rôznymi komunitami, ktoré sú rozhodujúce pre zaistenie kybernetickej bezpečnosti v Európe, a to aj medzi príslušnými orgánmi EÚ a orgánmi členských štátov. Takéto mechanizmy sa musia testovať a overovať ako súčasť cvičení v oblasti kybernetickej bezpečnosti na úrovni EÚ a v prípade potreby formalizovať prostredníctvom príslušných dohôd;

36. POZNAMENÁVA, že existuje možnosť preskúmania, ak by Komisia popri existujúcom úsilí členských štátov a pri rešpektovaní dostupných zdrojov (najmä v medziach viacročného finančného rámca EÚ) s cieľom pomôcť členským štátom reagovať na rozsiahle kybernetické incidenty a zmierňovať ich predložila návrh na zriadenie núdzového fondu kybernetickej bezpečnostnej reakcie, a to za predpokladu, že daný členský štát už pred príslušnou udalosťou zaviedol obozretný systém kybernetickej bezpečnosti vrátane úplného vykonávania smernice NIS a vyspelých rámcov riadenia rizika a dohľadu na vnútroštátnej úrovni;

37. UZNÁVA rastúce prepojenia medzi kybernetickou bezpečnosťou a obranou a VYZÝVA na zintenzívnenie spolupráce v oblasti kybernetickej obrany, a to aj podporovaním spolupráce medzi komunitami civilnej a vojenskej reakcie na incidenty a na pokračovanie posilňovania kybernetickej bezpečnosti misií a operácií v rámci SBOP;

---

17 C/2017/6100 final

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

38. ZDÔRAZŇUJE, že je možno potrebné plne využívať navrhované iniciatívy v oblasti obrany s cieľom urýchliť rozvoj primeraných kybernetických spôsobilostí v Európe a UZNÁVA možnosti potenciálneho rozvíjania projektov kybernetickej obrany prostredníctvom stálej štruktúrovanej spolupráce, ak to za potrebné považujú členské štáty zapojené do takejto spolupráce, a taktiež UZNÁVA úlohu Európskej obrannej technologickej a priemyselnej základne (EDTIB) a širšej civilnej základne v odvetví kybernetickej bezpečnosti pri poskytovaní prostriedkov členským štátom na zabezpečenie ich bezpečnostných a obranných záujmov v kybernetickej oblasti;

39. BERIE NA VEDOMIE návrh Komisie na zavedenie platformy odbornej prípravy a vzdelávania v oblasti kybernetickej obrany do konca roku 2018 a ZDÔRAZŇUJE, že táto platforma by mala rozšíriť príležitosti na vzdelávanie a odbornú prípravu v členských štátoch a zároveň by mala zabezpečiť doplnkovosť s ďalším úsilím a iniciatívami EÚ, najmä s EABO a EDA;

40. VYZÝVA EÚ a jej členské štáty, aby reagovali na hrozbu, ktorú predstavuje krádež duševného vlastníctva – vrátane obchodných tajomstiev alebo iných dôverných obchodných informácií – prostredníctvom IKT so zámerom poskytnúť konkurenčnú výhodu spoločnostiam alebo obchodným odvetviam;

41. UZNÁVA potrebu zaoberať sa trestnou činnosťou v kybernetickom priestore vrátane tej na temnom webe, sexuálneho vykorisťovania detí online, ako aj vrátane podvodov a falšovania bezhotovostných platobných prostriedkov, a to najmä zameraním sa na vytvorenie lepšieho spravodajského prehľadu, vykonávaním spoločných vyšetrovaní a operačnou podporou;

42. VÍTA prácu, ktorú EÚ a jej členské štáty vykonali pri riešení problémov, ktoré prinášajú systémy, ktoré umožňujú zločincom a teroristom komunikovať spôsobom neprístupným pre príslušné orgány, ZDÔRAZŇUJE, že pri tejto práci treba mať na pamäti, že pre kybernetickú bezpečnosť a dôveru v digitálny jednotný trh a zabezpečenie dodržiavania ľudských práv a základných slobôd je veľmi dôležité silné a dôveryhodné šifrovanie;

43. ZDÔRAZŇUJE, že je dôležité poskytnúť orgánom presadzovania práva nástroje, ktoré umožňujú odhaľovať, vyšetrovať a stíhať počítačovú kriminalitu, aby trestné činy spáchané v kybernetickom priestore neostali bez povšimnutia alebo nepotrestané, a VÍTA príspevok Európskej justičnej siete na boj proti počítačovej kriminalite v rámci boja proti trestnej činnosti prostredníctvom spolupráce justičných orgánov;

44. ZDÔRAZŇUJE dôležitosť zabezpečenia koordinovanej pozície EÚ s cieľom účinne formovať európske a celosvetové rozhodnutia komunity viacerých zainteresovaných strán týkajúce sa riadenia internetu, ako je napríklad zabezpečenie rýchlo dostupných a presných databáz WHOIS s IP adresami a názvami domén, aby sa chránili spôsobilosti na presadzovanie práva a verejné záujmy;

45. ZDÔRAZŇUJE význam zavedenia internetového protokolu IPv6, ktorý je zásadný pre rozvoj internetu vecí v potrebnom rozsahu, ako aj na zlepšenie prisudzovania trestnej činnosti v kybernetickom priestore;

46. PODPORUJE prebiehajúcu činnosť v oblasti cezhraničného prístupu k elektronickým dôkazom, uchovávania údajov a problémov pre trestné konanie, ktoré predstavujú systémy, ktoré umožňujú zločincom a teroristom komunikovať spôsobom neprístupným pre príslušné orgány, majúc na pamäti potrebu dodržiavať ľudské práva a základné slobody, ako aj ochranu údajov;

47. VYZÝVA Komisiu, aby:

- do decembra 2017 predložila správu o pokroku pri vykonávaní praktických opatrení na zlepšenie cezhraničného prístupu k elektronickým dôkazom;
- začiatkom roka 2018 predložila legislatívny návrh na zlepšenie cezhraničného prístupu k elektronickým dôkazom;

48. Vyzýva Europol, agentúru ENISA a Eurojust, aby:

- pokračovali v posilňovaní spolupráce v boji proti počítačovej kriminalite, a to aj medzi sebou navzájom, ako aj s inými príslušnými zainteresovanými stranami vrátane komunity jednotiek CSIRT, Interpolu, súkromného sektora a akademickej obce, pri zabezpečení synergií a vzájomného dopĺňania sa a v súlade s ich príslušnými úlohami a právomocami;

- spoločne s členskými štátmi prispievali ku koordinovanému prístupu k reakcii orgánov presadzovania práva EÚ na rozsiahle kybernetické incidenty a krízy, ktorý dopĺňa postupy stanovené v príslušných rámcoch[19];

49. VYZÝVA EÚ a jej členské štáty, aby pokračovali v práci s cieľom:

- odstrániť prekážky, ktoré bránia vyšetrovaniu trestnej činnosti a účinnej trestnej justícii v kybernetickom priestore, ako aj posilňovať medzinárodnú spoluprácu a koordináciu v boji proti trestnej činnosti v kybernetickom priestore;

- reagovať na výzvy, ktoré predstavujú technológie anonymizácie, majúc na pamäti, že pre kybernetickú bezpečnosť a dôveru v digitálny jednotný trh je veľmi dôležité silné a dôveryhodné šifrovanie;

- formovať rozhodnutia, ktoré sa týkajú riadenia internetu, ktoré majú vplyv na schopnosť orgánov presadzovania práva bojovať proti trestnej činnosti v kybernetickom priestore

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

Kapitola III

POSILNENIE MEDZINÁRODNEJ SPOLUPRÁCE V ZÁUJME OTVORENÉHO, SLOBODNÉHO, POKOJNÉHO A BEZPEČNÉHO GLOBÁLNEHO KYBERNETICKÉHO PRIESTORU

50. UZNÁVA, že zaistenie kybernetickej bezpečnosti je globálnou výzvou, ktorá si vyžaduje účinnú globálnu spoluprácu medzi všetkými aktérmi, a UZNÁVA, že osobitný dôraz treba venovať dodržiavaniu demokratických hodnôt a zásad otvoreného, slobodného, pokojného a bezpečného globálneho kybernetického priestoru, pričom v tejto súvislosti

51. VYZÝVA EÚ a jej členské štáty, aby podporovali vytvorenie strategického rámca na predchádzanie konfliktom, spoluprácu a pre stabilitu v kybernetickom priestore, ktorý bude vychádzať z uplatňovania platného medzinárodného práva, a najmä Charty OSN v celom jej rozsahu, z vývoja a vykonávania všeobecných noriem zodpovedného správania sa štátov a z regionálnych opatrení na budovanie dôvery medzi štátmi;

52. UZNÁVA úlohu Organizácie Spojených národov pri ďalšom vývoji noriem zodpovedného správania sa štátov v kybernetickom priestore a pripomína, že výsledky dlhoročných rokovaní skupiny vládnych expertov OSN priniesli dohodu na súbore noriem a odporúčaní[20], ktoré opakovane podporilo Valné zhromaždenie a ktoré by štáty mali prijať ako základ pre zodpovedné správanie sa štátov v kybernetickom priestore;

53. UZNÁVA, že tieto normy zodpovedného správania sa štátov zahŕňajú skutočnosť, že štáty by na svojom území nemali povoliť medzinárodne protiprávne konanie, mali by reagovať na primerané žiadosti o pomoc od iného štátu, ktorého kritická infraštruktúra je vystavená útoku škodlivých IKT z ich územia, a mali by prijímať primerané opatrenia na ochranu svojej kritickej infraštruktúry pred hrozbami v oblasti IKT;

54. UZNÁVA zdieľané kybernetické hrozby a riziká, ktorým čelí EÚ, NATO a ich príslušné členské štáty, a POTVRDZUJE, že je dôležité pokračovať v spolupráci medzi EÚ a NATO v oblasti kybernetickej bezpečnosti a obrany, a to pri plnom rešpektovaní zásad inkluzívnosti, reciprocity a autonómie rozhodovania EÚ a v súlade so závermi Rady zo 6. decembra 2016 o vykonávaní spoločného vyhlásenia predsedu Európskej rady, predsedu Európskej komisie a generálneho tajomníka Organizácie Severoatlantickej zmluvy[20];

55. VYZÝVA EÚ a jej členské štáty, aby podporovali a podnecovali vypracúvanie regionálnych opatrení na budovanie dôvery, ktoré sú základným predpokladom na prehĺbenie spolupráce a transparentnosti a zníženie rizika konfliktu. Vykonávanie opatrení na budovanie dôvery v oblasti kybernetickej bezpečnosti v rámci OBSE a v iných regionálnych rámcoch zvýši predvídateľnosť správania štátov a prispeje k ďalšej stabilizácii v kybernetickom priestore;

56. OPÄTOVNE POTVRDZUJE, že EÚ bude naďalej presadzovať svoje základné hodnoty v oblasti ochrany ľudských práv a základných slobôd na základe usmernení EÚ v oblasti ľudských práv týkajúcich sa slobody prejavu online. EÚ tiež zdôrazňuje význam zapojenia sa všetkých zainteresovaných strán do riadenia internetu, a to aj predstaviteľov akademickej obce, občianskej spoločnosti a súkromného sektora;

57. VYZÝVA EÚ a jej členské štáty, aby podporovali budovanie kybernetických kapacít v tretích krajinách, s osobitným dôrazom na susedné krajiny EÚ a rozvojové krajiny s rýchlo rastúcou pripojiteľnosťou, s cieľom bojovať proti počítačovej kriminalite a budovať odolnosť proti kybernetickým útokom, a to v súlade so základnými hodnotami EÚ. Na podporu úsilia EÚ v tejto oblasti by sa mala vybudovať sieť EÚ zameraná na budovanie kybernetických kapacít a vypracovať usmernenia EÚ pre budovanie kybernetických kapacít, ktoré by mali dopĺňať existujúce mechanizmy a štruktúry;

---

[20] 15283/16.

58. ZDÔRAZŇUJE pokrok, ktorý sa dosiahol pri spolupráci medzi EÚ a NATO v oblasti kybernetickej obrany a bezpečnosti, a jej rozvoj v oblasti odbornej prípravy, vzdelávania a koncepcií, pričom sa zároveň zabránilo zbytočnému zdvojovaniu úsilia v oblastiach, v ktorých dochádza k prekrývaniu požiadaviek, ako aj podporu interoperability prostredníctvom požiadaviek a noriem v oblasti kybernetickej obrany a VYZÝVA na pokračovanie spolupráce pri cvičeniach v oblasti kybernetickej obrany (zamestnanci) a na výmenu osvedčených postupov v oblasti krízového riadenia pri súčasnom zamedzení zbytočnému zdvojovaniu úsilia v oblastiach, v ktorých dochádza k prekrývaniu požiadaviek, v plnom súlade s politikou EÚ v oblasti cvičení a so zásadami inkluzívnosti, reciprocity a autonómie rozhodovania EÚ;

59. UZNÁVA, že Dohovor Rady Európy o počítačovej kriminalite, tzv. Budapeštiansky dohovor, je efektívna právna norma poskytujúca usmernenia pre zavedenie ustanovení o počítačovej trestnej činnosti do vnútroštátnych právnych predpisov. ŽIADA všetky krajiny, aby vypracovali vhodné vnútroštátne právne rámce a nadviazali spoluprácu v medziach existujúceho medzinárodného rámca, ktorý ponúka Budapeštiansky dohovor;

60. PRIPOMÍNA úspechy pri vykonávaní dvojstranných dialógov EÚ o počítačovej bezpečnosti a vyzýva na ďalšie úsilie na uľahčenie spolupráce s tretími krajinami v oblasti kybernetickej bezpečnosti;

61. PRIPOMÍNA, že EÚ prijala pevný a právne záväzný mechanizmus kontroly vývozu vychádzajúci z rozhodnutí a najlepších postupov vyvinutých v rámci medzinárodných režimov nešírenia, a BERIE NA VEDOMIE prebiehajúcu diskusiu v Rade s cieľom nájsť najlepšie spôsoby, ako ďalej zlepšiť fungovanie týchto kontrol, pričom VYZÝVA členské štáty, aby sa naďalej zaoberali v rámci príslušných medzinárodných režimov kontroly vývozu (napr. Wassenaarského usporiadania), kritickými kybernetickobezpečnostnými aplikáciami nových technológií, a to s cieľom zabezpečiť účinnú kontrolu kritických kybernetickobezpečnostných technológií budúcnosti.

62. V nadväznosti na závery Európskej rady z 19. októbra 2017[21] sa tieto závery budú vykonávať prostredníctvom akčného plánu, ktorý má Rada prijať pred koncom roku 2017. Tento akčný plán by mala Rada ako živý dokument pravidelne preskúmavať a aktualizovať.

---

[21] EUCO 14/17.