Stanovisko Európskeho hospodárskeho a sociálneho výboru – Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa zriaďuje Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti a sieť národných koordinačných centier

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Spravodajca: **Antonio LONGO**

Pomocný spravodajca: **Alberto MAZZOLA**

Konzultácia	Európska rada, 5.10.2018 Európsky parlament, 1.10.2018
Právny základ	článok 173 ods. 3 a články 188 a 304 Zmluvy o fungovaní Európskej únie
Príslušná sekcia	sekcia pre dopravu, energetiku, infraštruktúru a informačnú spoločnosť
Prijaté v sekcii	9.1.2019
Prijatie v pléne	23.1.2019
Plenárne zasadnutie č.	540
Výsledok hlasovania (za/proti/zdržalo sa)	143/5/2

1. Závery a odporúčania

1.1. Európsky hospodársky a sociálny výbor (EHSV) víta iniciatívu Komisie a považuje ju za pomoc pri vytváraní priemyselnej stratégie kybernetickej bezpečnosti, ktorá má strategický význam na dosiahnutie silnej a širokej digitálnej autonómie. Tieto faktory sú nevyhnutné na posilnenie európskych obranných mechanizmov v súvislosti s prebiehajúcou kybernetickou vojnou, ktorá môže ohroziť politické, hospodárske a sociálne systémy.

1.2. Výbor poznamenáva, že žiadnu stratégiu v oblasti kybernetickej bezpečnosti nemožno oddeliť od širokého povedomia a bezpečného správania všetkých používateľov.

1.3. Výbor súhlasí so všeobecnými cieľmi návrhu a uvedomuje si, že špecifické aspekty fungovania budú predmetom neskoršej analýzy. No keďže ide o nariadenie, sa domnieva, že citlivé aspekty týkajúce sa riadenia, financovania a dosiahnutia stanovených cieľov by sa mali stanoviť vopred. Je dôležité, aby budúca sieť a budúce centrum v čo možno najväčšej miere vychádzali z kybernetických schopností a odborných znalostí jednotlivých členských štátov, a aby sa v centre, ktoré sa má zriadiť, nesústredili všetky právomoci. Takisto treba zabrániť prekrývaniu oblastí pôsobnosti budúcej siete a centra s existujúcimi mechanizmami spolupráce a inštitúciami.

1.4. EHSV podporuje rozšírenie spolupráce na sféru priemyslu – zahrnutím ho v budúcnosti do správnej rady – na základe pevných záväzkov v oblasti vedy a investícií. V prípade trojstrannej spolupráce medzi Európskou komisiou, členskými štátmi a priemyslom by sa mala prítomnosť spoločností z krajín mimo EÚ obmedziť na tie, ktoré sú už dlhodobo usadené na európskej pôde a plne sa podieľajú na európskej technologickej a priemyselnej základni za predpokladu, že sa podrobia primeraným detekčným a kontrolným mechanizmom a budú dodržiavať zásadu reciprocity a povinnosť zachovávať dôvernosť.

1.5. Kybernetická bezpečnosť musí byť spoločným záväzkom všetkých členských štátov, ktoré sa preto musia zúčastňovať na správnej rade, pričom treba stanoviť podmienky tejto účasti. Pokiaľ ide o finančný príspevok členských štátov, mohlo by sa čerpať z pridelených finančných prostriedkov EÚ pre každý z nich.

1.6. V návrhu by sa malo lepšie objasniť, ako bude centrum schopné zasahovať do koordinácie financovania programov Digitálna Európa a Horizont Európa a predovšetkým akými usmerneniami sa bude riadiť prípadné verejné obstarávanie a zadávanie verejných zákaziek. Tento aspekt je nevyhnutný, aby sa zabránilo duplicite alebo prekrývaniu. Okrem toho sa na zvýšenie finančného krytia odporúča rozšíriť súčinnosť s ostatnými finančnými nástrojmi EÚ (napr. regionálne fondy, štrukturálne fondy, NPE, ERF, InvestEU...).

1.7. EHSV považuje za nevyhnutné definovať spôsoby spolupráce a vzťahy medzi európskym centrom a národnými centrami. Okrem toho je dôležité, aby národné centrá financovala EÚ, aspoň pokiaľ ide o administratívne náklady, čím sa uľahčí administratívna harmonizácia a harmonizácia kompetencií s cieľom znížiť rozdiely medzi členskými štátmi EÚ.

1.8. Výbor opätovne zdôrazňuje význam ľudského kapitálu a dúfa, že kompetenčné centrum bude môcť v spolupráci s univerzitami, výskumnými centrami a centrami vysokoškolského vzdelávania podporovať vzdelávanie a odbornú prípravu založenú na excelentnosti, a to aj prostredníctvom špecifických vzdelávacích odborov na vysokých i stredných školách. Podobne je nevyhnutné poskytnúť osobitnú podporu startupom a MSP.

1.9. EHSV sa domnieva, že je nevyhnutné lepšie objasniť príslušné oblasti právomocí a rozlišovanie medzi mandátom centra a Agentúry Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), pričom treba jasne vymedziť aj spôsoby spolupráce a vzájomnej podpory a zabrániť prekrývaniu kompetencií a zdvojovaniu úsilia. Podobné problémy vznikajú aj v súvislosti s inými orgánmi v oblasti kybernetickej bezpečnosti, ako sú EDA, EUROPOL a CERT-EU, a odporúča sa vytvoriť viaceré mechanizmy štruktúrovaného dialógu medzi rôznymi orgánmi.

2. **Súčasný rámec kybernetickej bezpečnosti**

2.1. Kybernetická bezpečnosť je jednou z najdôležitejších tém v EÚ, pretože je nevyhnutným faktorom obrany inštitúcií, spoločností a občanov, ako aj nevyhnutným nástrojom pre samotnú stabilitu demokracií. Jedným z najznepokojujúcejších javov je exponenciálny nárast malvéru šíreného v sieti prostredníctvom automatických systémov, pričom počet útokov sa zvýšil zo 130 tisíc v roku 2007 na 8 miliónov v roku 2017. Okrem toho je Únia čistým dovozcom produktov a riešení v oblasti kybernetickej bezpečnosti, čo je problémom pre hospodársku konkurencieschopnosť a civilnú a vojenskú bezpečnosť.

2.2. Hoci EÚ disponuje značnými kompetenciami a skúsenosťami v oblasti kybernetickej bezpečnosti, priemysel v tomto odvetví, vysoké školy a výskumné centrá sa javia stále roztrieštené, nezosúladené a neviazané žiadnou spoločnou rozvojovou stratégiou. Je to spôsobené tým, že nie sú dostatočne podporované odvetvia, ktorých sa kybernetická bezpečnosť týka (napr. energia, vesmír, obrana a doprava), ani nie sú náležite rozvíjané synergie medzi civilnou a obrannou kybernetickou bezpečnosťou.

2.3. S cieľom riešiť rastúce výzvy stanovila EÚ v roku 2013 stratégiu kybernetickej bezpečnosti na podporu spoľahlivého, bezpečného a otvoreného kybernetického ekosystému ([1]). Následne boli v roku 2016 prijaté prvé konkrétne opatrenia pre bezpečnosť sietí a informačných systémov ([2]). Tento vývoj viedol k vytvoreniu verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti („cPPP“).

2.4. V roku 2017 sa v oznámení s názvom „Odolnosť, odrádzanie a obrana: Budovanie silnej kybernetickej bezpečnosti v Európe“ ([3]) poukázalo na potrebu zabezpečiť zachovanie a rozvoj základných technologických kapacít v oblasti informačnej bezpečnosti na ochranu digitálneho jednotného trhu, a najmä na ochranu kritických informačných sietí a systémov a na poskytovanie základných služieb v oblasti kybernetickej bezpečnosti.

([1]) JOIN(2013) 1 final.

([2]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

([3]) JOIN(2017) 450 final.

2.5. Únia preto musí byť schopná chrániť svoje digitálne zdroje a postupy a súťažiť na globálnom trhu kybernetickej bezpečnosti, kým nedosiahne stabilnú a rozsiahlu digitálnu autonómiu ([4]).

3. Návrhy Komisie

3.1. Kompetenčné centrum (ďalej „centrum“) bude mať za cieľ podporovať prácu siete národných centier a pomáhať ju koordinovať, ako aj byť referenčným bodom pre komunitu pre kompetencie v oblasti kybernetickej bezpečnosti, pričom bude stáť na čele technologického programu v tejto oblasti a uľahčovať prístup k takto získaným odborným poznatkom.

3.2. Kompetenčné centrum to bude dosahovať predovšetkým implementáciou príslušných častí programov Digitálna Európa a Horizont Európa – udeľovaním grantov a vykonávaním obstarávaní. Vzhľadom na značné investície do kybernetickej bezpečnosti v iných častiach sveta a na potrebu koordinovať a združovať príslušné zdroje v Európe sa kompetenčné centrum navrhuje ako európske partnerstvo s dvojitým právnym základom, ktoré umožní spoločné investície Únie, členských štátov a/alebo príslušného priemyselného odvetvia.

3.3. Návrh si preto od členských štátov vyžaduje úmerný príspevok na akcie kompetenčného centra a siete. Finančné krytie poskytnuté EÚ predstavuje približne 2 miliardy EUR z programu Digitálna Európa; suma z programu Horizont Európa sa má určiť; celkový príspevok členských štátov sa rovná aspoň príspevku Únie.

3.4. Hlavným rozhodovacím orgánom je správna rada, v ktorej budú zastúpené všetky členské štáty, no hlasovacie práva budú mať len tie, ktoré finančne prispievajú. Hlasovací mechanizmus v správnej rade sa riadi zásadou dvojitej väčšiny, čo znamená, že sa vyžaduje zastúpenie 75 % finančného príspevku a 75 % hlasov. Komisia má 50 % hlasovacích práv. Správnej rade pomáha odvetvová a vedecká poradná rada s cieľom zabezpečiť pravidelný dialóg s podnikmi, spotrebiteľmi a inými príslušnými zainteresovanými stranami.

3.5. Centrum by bolo hlavným vykonávacím orgánom pre finančné zdroje EÚ vyčlenené na kybernetickú bezpečnosť v rámci navrhovaného programu Digitálna Európa a programu Horizont Európa, v úzkej spolupráci so sieťou národných koordinačných centier a komunitou pre kompetencie v oblasti kybernetickej bezpečnosti.

3.6. Národné koordinačné centrá budú vybrané členskými štátmi. Musia mať technologické kompetencie v oblasti kybernetickej bezpečnosti alebo mať k nim prístup priamo, najmä v oblastiach, ako je kryptografia, bezpečnostné služby IKT, automatické detekcie narušení, bezpečnosť systémov, sietí, softvéru a aplikácií a ľudské a sociálne aspekty bezpečnosti a súkromia. Musia byť tiež schopné účinne komunikovať a koordinovať svoju činnosť s priemyslom a verejným sektorom vrátane orgánov určených podľa smernice (EÚ) 2016/1148.

4. Všeobecné pripomienky

4.1. EHSV víta iniciatívu Komisie a považuje ju za strategickú pre rozvoj kybernetickej bezpečnosti pri vykonávaní rozhodnutí prijatých na summite v Talline v septembri 2017. Pri tej príležitosti hlavy štátov a predsedovia vlád vyzvali EÚ, aby sa do roku 2025 stala „globálnym lídrom v oblasti kybernetickej bezpečnosti s cieľom zabezpečiť dôveru, spoľahlivosť a ochranu našich občanov, spotrebiteľov a podnikov online a umožniť bezplatný a zákonný internet“.

4.2. EHSV opätovne zdôrazňuje, že v súčasnosti prebieha skutočná kybernetická vojna, ktorá ohrozuje politické, hospodárske a sociálne systémy útokom na informačné systémy inštitúcií, kritických infraštruktúr (energetika, doprava, banky a finančné inštitúcie...) a podnikov, a prostredníctvom falošných správ ovplyvňuje volebné a demokratické procesy vo všeobecnosti ([5]). Preto je potrebné silné povedomie a rozhodná a včasná reakcia. Z týchto dôvodov je potrebné vytvoriť jasnú a dobre podporovanú odvetvovú stratégiu kybernetickej bezpečnosti ako predpoklad pre dosiahnutie digitálnej autonómie. EHSV sa domnieva, že v pracovnom programe by sa mali uprednostniť oblasti určené smernicou (EÚ) 2016/1148 o kybernetickej bezpečnosti, ktorá sa vzťahuje na spoločnosti poskytujúce základné služby, či už verejné alebo súkromné, z dôvodu ich významu pre spoločnosť ([6]).

([4]) Ú. v. EÚ C 227, 28.6.2018, s. 86.

([5]) Informačná správa na tému Využívanie médií na ovplyvnenie sociálnych a politických procesov v EÚ a východných susedných krajinách, Vareikytė, 2014.

([6]) Ú. v. EÚ C 227, 28.6.2018, s. 86.

4.3. Výbor poznamenáva, že žiadnu stratégiu v oblasti kybernetickej bezpečnosti nemožno oddeliť od širokého povedomia a bezpečného správania všetkých používateľov. Z tohto dôvodu musí byť každá technologická iniciatíva sprevádzaná zodpovedajúcimi informačnými a osvetovými kampaňami s cieľom vytvoriť „kultúru digitálnej bezpečnosti“ ([7]).

4.4. Výbor súhlasí so všeobecnými cieľmi návrhu a uvedomuje si, že špecifické aspekty fungovania budú predmetom neskoršej analýzy. No keďže ide o nariadenie, sa domnieva, že citlivé aspekty týkajúce sa riadenia, financovania a dosiahnutia vopred stanovených cieľov by sa mali stanoviť vopred. Je dôležité, aby budúca sieť a budúce centrum v čo možno najväčšej miere vychádzali z kybernetických schopností a odborných znalostí jednotlivých členských štátov, a aby sa v centre, ktoré sa má zriadiť, nesústredili všetky právomoci. Takisto treba zabrániť prekrývaniu oblastí pôsobnosti budúcej siete a centra s existujúcimi mechanizmami spolupráce a inštitúciami.

4.5. EHSV pripomína, že vo svojom stanovisku TEN/646 k aktu o kybernetickej bezpečnosti ([8]) navrhuje trojstrannú spoluprácu medzi Európskou komisiou, členskými štátmi a odvetvím v rámci verejno-súkromného partnerstva, so zapojením MSP, zatiaľ čo súčasná štruktúra, ktorej právna forma sa musí dôkladnejšie preskúmať, v podstate zabezpečuje verejno-verejné partnerstvo medzi Európskou komisiou a členskými štátmi.

4.6. EHSV podporuje rozšírenie spolupráce na sféru priemyslu – zahrnutím ho v budúcnosti do správnej rady – na základe pevných záväzkov v oblasti vedy a investícií. Vytvorenie odvetvovej a vedeckej poradnej rady nemôže zaručiť stály dialóg s podnikmi, spotrebiteľmi a inými zainteresovanými stranami. Okrem toho v novom kontexte, ktorý vypracovala Komisia, nie je jasné, akú úlohu bude mať Európska organizácia pre kybernetickú bezpečnosť (ECSO), ktorá bola vytvorená v júni 2016 na podnet Komisie ako jej protiváha a ktorej sieťový kapitál a znalosti by nemali byť rozptýlené.

4.6.1. V prípade trojstrannej spolupráce je dôležité venovať pozornosť spoločnostiam pochádzajúcim z tretích krajín. EHSV predovšetkým zdôrazňuje, že táto spolupráca by sa mala zakladať na prísnom mechanizme na zabránenie prítomnosti podnikov z krajín mimo EÚ, ktoré by mohli predstavovať prekážku pre bezpečnosť a autonómiu Únie. V tejto súvislosti by sa mali uplatňovať aj súvisiace ustanovenia EDIDP ([9]).

4.6.2. EHSV zároveň uznáva, že niektoré podniky, ktoré síce pochádzajú z krajín mimo EÚ, avšak sú už dlhodobo usadené na európskej pôde a plne sa podieľajú na európskej technologickej a priemyselnej základni, by mohli byť pre projekty Únie veľmi užitočné a mali by mať k nim prístup za predpokladu, že členské štáty zavedú primerané detekčné a kontrolné mechanizmy a že sa bude dodržiavať zásada reciprocity a povinnosť zachovávať dôvernosť.

4.7. Kybernetická bezpečnosť musí byť spoločným záväzkom všetkých členských štátov, ktoré sa preto musia zúčastňovať na správnej rade, pričom treba stanoviť podmienky tejto účasti. Je tiež dôležité, aby všetky štáty finančne a primeraným spôsobom prispeli k iniciatíve Komisie. Pokiaľ ide o finančný príspevok členských štátov, mohlo by sa čerpať z pridelených finančných prostriedkov EÚ pre každý z nich.

4.8. EHSV súhlasí s tým, že každý členský štát môže vymenovať svojho vlastného zástupcu do správnej rady európskeho kompetenčného centra. Výbor odporúča, aby sa v životopisných profiloch národných zástupcov jednoznačne uvádzali strategické a technologické kompetencie spolu s kompetenciami v oblasti riadenia, administratívy a rozpočtu.

4.9. V návrhu by sa malo lepšie objasniť, akým spôsobom bude centrum schopné zasahovať do koordinácie financovania programov Digitálna Európa a Horizont Európa, čo je stále predmetom rokovaní, a predovšetkým to, akými usmerneniami sa bude riadiť prípadné verejné obstarávanie a zadávanie verejných zákaziek. Tento aspekt je nevyhnutný, aby sa zabránilo duplicite alebo prekrývaniu. Okrem toho sa na zvýšenie finančného krytia odporúča rozšíriť súčinnosť s ostatnými finančnými nástrojmi EÚ (napr. regionálne fondy, štrukturálne fondy, NPE, ERF, InvestEU...). Výbor dúfa, že sieť národných centier bude zapojená do riadenia a koordinácie fondov.

([7]) Ú. v. EÚ C 227, 28.6.2018, s. 86.
([8]) Ú. v. EÚ C 227, 28.6.2018, s. 86.
([9]) COM(2017) 294.

4.10. EHSV konštatuje, že poradná rada by mala byť zložená zo 16 členov a že sa neobjasňujú mechanizmy, ktoré by mali zaistiť vstupy podnikateľskej sféry, akademickej obce, výskumu a spotrebiteľov. Výbor sa domnieva, že by bolo užitočné a vhodné, aby sa členovia tejto rady vyznačovali rozsiahlymi znalosťami danej problematiky a vyváženým spôsobom zastupovali rôzne zainteresované sektory.

4.11. EHSV považuje za nevyhnutné definovať spôsoby spolupráce a vzťahy medzi európskym centrom a národnými centrami. Okrem toho je dôležité, aby národné centrá financovala EÚ, aspoň pokiaľ ide o administratívne náklady, čím sa uľahčí administratívna harmonizácia a harmonizácia kompetencií s cieľom znížiť rozdiely medzi členskými štátmi EÚ.

4.12. V súlade so svojimi predchádzajúcimi stanoviskami ([10]) EHSV zdôrazňuje význam vzdelávania a odbornej prípravy založenej na excelentnosti v oblasti ľudských zdrojov v odvetví kybernetickej bezpečnosti, a to aj prostredníctvom špecifických školských, vysokoškolských a postgraduálnych odborov. Je tiež dôležité poskytnúť primeranú finančnú podporu MSP a startupom v tomto odvetví ([11]), ktoré sú nevyhnutné pre rozvoj špičkového výskumu.

4.13. EHSV sa domnieva, že je nevyhnutné lepšie objasniť príslušné oblasti právomocí a rozlišovanie medzi mandátom centra a agentúry ENISA, pričom treba jasne vymedziť aj spôsoby spolupráce a vzájomnej podpory a zabrániť prekrývaniu kompetencií a zdvojovaniu úsilia ([12]). V návrhu nariadenia sa stanovuje prítomnosť delegáta agentúry ENISA ako stáleho pozorovateľa v správnej rade, ale táto prítomnosť nie je zárukou štruktúrovaného dialógu medzi týmito dvoma orgánmi. Podobné problémy vznikajú aj v súvislosti s inými orgánmi v oblasti kybernetickej bezpečnosti, ako sú EDA, EUROPOL a CERT-EU. Z tohto hľadiska je zaujímavé memorandum o porozumení, ktoré v máji 2018 podpísali agentúry ENISA, EDA, Europol a CERT-EU.

V Bruseli 23. januára 2019

Predseda
Európskeho hospodárskeho a sociálneho výboru
Luca JAHIER

([10]) Ú. v. EÚ C 451, 16.12.2014, s. 64.
([11]) Ú. v. EÚ C 227, 28.6.2018, s. 86.
([12]) Ú. v. EÚ C 227, 28.6.2018, s. 86.