Stanovisko Evropského hospodářského a sociálního výboru k návrhu nařízení Evropského parlamentu a Rady, kterým se mění nařízení (EU) 2019/881, pokud jde o řízené bezpečnostní služby

(COM(2023) 208 final) — 2023/0108 (COD)

a k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně

(COM(2023) 209 final) — 2023/0109 (COD)

(2023/C 349/25)

Zpravodaj: **Dumitru FORNEA**

Spoluzpravodaj: **Alberto MAZZOLA**

Žádost o vypracování stanoviska	Evropský parlament, 1. 6. 2023
	Rada Evropské unie, 7. 6. 2023
Právní základ	*Článek 114*, čl. 173 odst. 3 a článek 304 Smlouvy o fungování Evropské unie
Odpovědný orgán	Poradní komise pro průmyslové změny
Přijato na plenárním zasedání	13. 7. 2023
Plenární zasedání č.	580
Výsledek hlasování	
(pro/proti/zdrželi se hlasování)	174/0/1

1. **Závěry a doporučení**

1.1 Evropský hospodářský a sociální výbor (EHSV) vítá předložený návrh nařízení ([1]) a domnívá se, že je naprosto nezbytné zajistit koordinaci na úrovni EU, aby bylo možné překonat stávající roztříštěnost trhu a zlepšit spolupráci mezi soukromými a veřejnými subjekty v EU s cílem posílit schopnost předcházet kybernetickým hrozbám, odhalovat tyto hrozby a reagovat na ně. Doporučuje věnovat v návrhu větší pozornost respektování zásady subsidiarity a zásady proporcionality v souladu s čl. 4 odst. 2 Smlouvy o Evropské unii (SEU).

1.2 EHSV oceňuje úsilí, které Evropská komise v oblasti kybernetické bezpečnosti vyvíjí, a zdůrazňuje, že komplexní reakce na kybernetické incidenty by měla zahrnovat nejenom kapacity a procesy, ale také hardwarové a softwarové prvky. Nesouhlasí však s udělením četných prováděcích pravomocí, které je v nařízení navrženo, a to zejména z toho důvodu, že kybernetická bezpečnost je v kompetenci členských států.

1.3 Je nutné vypracovat střednědobou strategii pro dosažení strategické autonomie v klíčových technologiích a kritických odvětvích, v jejímž rámci bude podnikům sídlícím v EU poskytována podpora při zřizování výzkumných a výrobních zařízení. EHSV zdůrazňuje, že je nesmírně důležité, aby špičkové technologie, jimiž mají být vybavována národní bezpečnostní operační střediska, pocházely výhradně z EU.

1.4 EHSV vyjadřuje znepokojení nad tím, že zatím nebyl zaveden žádný systém kybernetické bezpečnosti a že z tohoto hlediska zatím nebyl certifikován žádný produkt, ačkoli jsou to již čtyři roky, co byl přijat akt EU o kybernetické bezpečnosti ([2]). Doporučuje, aby byly do vytváření systémů kybernetické bezpečnosti zapojeny odvětvové agentury EU ([3]) a aby byl ve spolupráci s Evropským výborem pro normalizaci (CEN), Evropským výborem pro normalizaci v elektrotechnice (CENELEC) a Evropským ústavem pro telekomunikační normy (ETSI) přijat minimální standard EU, mj. i ve vztahu k zařízením „internetu lidí“ a k internetu věcí.

([1]) Návrh nařízení, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).

([3]) Například Agentura Evropské unie pro bezpečnost letectví (EASA), Agentura Evropské unie pro železnice (ERA), Evropská agentura pro léčivé přípravky (EMA) a další.

1.5 EHSV oceňuje návrh posílit úlohu Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) a žádá, aby jí byly na veškeré dodatečné aktivity poskytnuty potřebné lidské zdroje a také odpovídající finanční prostředky, a tato agentura tak mohla plnit svou významnou strategickou úlohu v souladu s cíli EU v oblasti kybernetické bezpečnosti.

1.6 Členské státy by se měly dohodnout na přijetí komplexního přístupu ke kybernetické bezpečnosti, který bude zahrnovat kvalifikované pracovníky, jednotně prováděné postupy a vhodné nejmodernější technologie, přičemž je třeba klást zvláštní důraz na lepší spolupráci se soukromým sektorem. Tato spolupráce a posílení vazeb mezi soukromým sektorem a odvětvím obrany mají totiž zcela zásadní význam.

1.7 Technické specifikace pro budoucí infrastrukturu IT by měly zaručit plnou interoperabilitu mezi vnitrostátními systémy a kybernetickým štítem EU. Národní bezpečnostní operační střediska musí být také připravena realizovat zátěžové testy kritické infrastruktury v dané zemi a informovat o výsledcích těchto testů v rámci kybernetického štítu EU.

1.8 EHSV navrhuje, aby koordinující bezpečnostní operační středisko v rámci určitého konsorcia tuto funkci vykonávalo po dobu jednoho roku na základě společného rotačního systému. Finanční prostředky, které EU poskytne hostitelskému konsorciu, by měly pokrýt 100 % nákladů na pořízení nástrojů a infrastruktury a 50 % nákladů na provoz (a nikoli 75 % a 50 %, jak je uvedeno v návrhu).

1.9 Vzhledem k tomu, že se v posledních letech prohloubil nedostatek kvalifikovaných pracovníků v oblasti kybernetické bezpečnosti, EHSV vítá iniciativu týkající se Akademie kybernetických dovedností a domnívá se, že je nutné stanovit ukazatele pro měření pokroku při napravování tohoto nedostatku.

1.10 EHSV poukazuje na to, že Evropská komise neuvedla přesný odhad nákladů na potřebné programy, technologie analýzy dat a projekty rozvoje infrastruktury. Domnívá se, že navrhovaná výše prostředků, jež mají být v této souvislosti vyčleněny na úrovni EU, je nedostatečná. Naléhavě proto žádá, aby byly prozkoumány další zdroje, včetně kombinace různých soukromých zdrojů.

1.11 Stanovený postup podání žádosti o podporu z rezervy EU pro kybernetickou bezpečnost se zdá být příliš zdlouhavý a nebyly v něm jasně stanoveny lhůty pro vyřízení žádosti. EHSV zdůrazňuje, že v případě kybernetického incidentu je nutné reagovat bleskurychle.

1.12 EHSV vyzývá Evropskou komisi, aby upřesnila, co se rozumí „významným množstvím údajů“, které je zmíněno v čl. 6 odst. 2 písm. a) nařízení, a jaké „cíle“ má na mysli v písmenu c) téhož odstavce.

1.13 EHSV pokládá za mimořádně důležité, aby se EU zapojila do celosvětových jednání o zavedení mezinárodní strategie v oblasti kybernetické bezpečnosti. Je naprosto zásadní, aby byly kybernetické útoky co nejrychleji vyšetřeny a jejich pachatelé byli pohnáni k odpovědnosti, a to i diplomatickou cestou, jestliže se nacházejí mimo EU.

1.14 EHSV je zklamán tím, že dokument neobsahuje žádnou zmínku o sociálních partnerech ani o organizacích občanské společnosti, a upozorňuje, že organizovaná občanská společnost v EU musí být plně zapojena, jinak totiž nebude možné zlepšit spolupráci mezi veřejnými a soukromými subjekty.

1.15 EHSV navrhuje, aby byla zpráva Evropskému parlamentu a Radě předložena dva roky od vstupu nařízení v platnost (a nikoli čtyři, jak navrhuje Komise), a to spolu s posouzením dopadů, které by mělo být k nařízení připojeno. EHSV zdůrazňuje, že je nutné zavést konkrétní opatření v oblasti výkonnosti, která budou zaměřena na dosažení výsledků, a klíčové ukazatele výkonnosti, pomocí nichž bude možné tyto výsledky vyhodnotit.

2. **Úvodní připomínky**

2.1 Kyberprostor se vyznačuje neustálými změnami, anonymitou a absencí hranic, což s sebou z hlediska fungování informační společnosti na individuální, státní a nadnárodní úrovni nese jak příležitosti, tak i rizika.

2.2 Je zcela zřejmé, že se kybernetické incidenty mohou rychle rozšířit z jednoho členského státu do druhého. EU se tedy v oblasti kybernetické bezpečnosti potýká s narůstajícími riziky a se spletitým spektrem hrozeb. Je naprosto nezbytné zajistit koordinaci na úrovni EU, aby bylo možné překonat stávající roztříštěnost a podpořit rozsáhlejší spolupráci mezi členskými státy.

2.3 Z hlediska jednotného trhu EU je nutné zajistit, aby byla pravidla týkající se kybernetické bezpečnosti vykládána a uplatňována jednotně, byť je rovněž zapotřebí stanovit různé přístupy pro jednotlivá odvětví v závislosti na tom, jakým způsobem fungují.

2.4 Aby bylo možné reagovat na kybernetické bezpečnostní incidenty okamžitě a účinně, je nezbytné zavést rychlý systém výměny informací mezi všemi důležitými zúčastněnými stranami na vnitrostátní úrovni a na úrovni EU. A to zase vyžaduje jasné pochopení toho, jakou úlohu jednotlivé subjekty plní a jaké mají kompetence.

2.5 EHSV oceňuje úsilí, které Evropská komise v oblasti kybernetické bezpečnosti vyvíjí, a také velké množství předložených sdělení a návrhů, jejichž cílem je vytvořit silnější rámec EU, zlepšit spolupráci a docílit odolnosti a odrazujícího účinku. Evropa potřebuje špičkové kybernetické technologie, přičemž je třeba posílit vazby mezi odvětvím obrany a soukromým sektorem, aby bylo možné mobilizovat prostředky určené na obranu a vyvinout kybernetické produkty pro vojenské i civilní využití. EHSV upozorňuje na to, že reakce nezbytná v případě kybernetických incidentů musí zahrnovat nejenom kapacity a procesy, ale také hardwarové a softwarové prvky.

2.6 Tímto návrhem nařízení je rovněž realizována Strategie kybernetické bezpečnosti EU, která byla přijata v prosinci 2020 a v níž byl oznámen záměr vytvořit evropský kybernetický štít s cílem posílit v celé EU kapacity pro odhalování kybernetických hrozeb a sdílení informací v této oblasti.

2.7 V souvislosti s budováním evropského kybernetického štítu Evropská komise navrhuje, aby byla v budoucnu v úzké spolupráci s vysokým představitelem postupně rozvíjena spolupráce se sítěmi a platformami, které se zabývají sdílením informací v rámci komunity v oblasti kybernetické obrany.

2.8 Ruská vojenská agrese vůči Ukrajině jasně ukázala, že útočné kybernetické operace mohou být využívány jako stěžejní součást hybridní taktiky spočívající v nátlaku, destabilizaci a narušení hospodářského života.

3. **Obecné připomínky**

3.1 EHSV vítá navrhované nařízení, které má za cíl překonat stávající roztříštěnost trhu a urychlit spolupráci mezi evropskými subjekty ze soukromého a veřejného sektoru, aby bylo možné lépe předcházet kybernetickým hrozbám, odhalovat je a reagovat na ně. Toto nařízení by po svém provedení mohlo pomoci zvýšit odolnost evropských systémů.

3.2 Je ovšem třeba poukázat na to, že cíle vytyčené v předloženém návrhu byly zdůrazněny již v návrhu na zřízení Společné kybernetické jednotky ([4]) – jde o zajištění rozsáhlejší spolupráce, připravenosti a odolnosti kybernetických systémů v EU. Tato kybernetická jednotka sice měla začít fungovat koncem roku 2022, v návrhu Komise však není vůbec zmíněna.

3.3 Jednotlivé technologie či nástroje nejsou samy o sobě s to zaručit plnou ochranu před kybernetickými hrozbami. Členské státy by se proto měly dohodnout na komplexním přístupu, který bude zahrnovat kvalifikované pracovníky, jednotně prováděné postupy a vhodné nejmodernější technologie. Je nutné klást důraz na lepší spolupráci se soukromým sektorem.

3.4 EHSV je zklamán tím, že dokument neobsahuje žádnou zmínku o sociálních partnerech ani o organizacích občanské společnosti. Organizovaná občanská společnost v EU však musí být plně zapojena, jinak totiž nebude možné zlepšit spolupráci mezi veřejnými a soukromými organizacemi.

3.5 EU by měla přijmout střednědobou strategii pro dosažení strategické autonomie v klíčových technologiích a kritických odvětvích. EHSV doporučuje, aby byla podnikům sídlícím v EU poskytována podpora při zřizování výzkumných a výrobních zařízení s cílem pomoci vytvořit autonomní kybernetický ekosystém. EHSV již v minulosti upozornil, že EU musí snížit „svoji závislost na technologických gigantech ze zemí mimo EU (…) dvojnásobným úsilím o rozvíjení bezpečné, inkluzivní a na hodnotách založené digitální ekonomiky“ ([5]).

([4]) Komise navrhuje zřízení Společné kybernetické jednotky, která umožní efektivnější reakci na kyberneticko-bezpečnostní incidenty velkého rozsahu.

([5]) Stanovisko Evropského hospodářského a sociálního výboru k tématu Digitální suverenita – pilíř digitalizace a růstu (stanovisko z vlastní iniciativy (Úř. věst. C 75, 28.2.2023, s. 8).

3.6 Velmi pozitivním prvkem je návrh na zřízení evropského kybernetického štítu, který bude sestávat z národních bezpečnostních operačních středisek a přeshraničních bezpečnostních operačních středisek a bude vybaven nejmodernějšími technologiemi. V zájmu zajištění odolnosti celého dodavatelského řetězce musí řešení bezpečnostních operačních středisek nejen chránit vnitřní organizační zdroje, ale také podporovat bezpečnou výměnu a rozsáhlejší spolupráci v rámci tohoto ekosystému. Technické specifikace pro budoucí infrastrukturu IT musí zaručit plnou interoperabilitu mezi vnitrostátními systémy a kybernetickým štítem EU.

3.7 EHSV zdůrazňuje, že je nesmírně důležité, aby špičkové technologie, jimiž mají být vybavovány subjekty tvořící kybernetický štít EU, pocházely výhradně z Evropy. EU si nemůže dovolit riskovat a pořizovat kritické kybernetické technologie od zahraničních podniků, neboť „je ve strategickém zájmu EU zajistit, aby si Unie zachovala a rozvíjela základní kapacity pro zabezpečení své digitální ekonomiky, společnosti a demokracie, aby dosáhla plné digitální suverenity jako jediného způsobu, jak chránit kritické technologie a poskytovat účinné klíčové služby v oblasti kybernetické bezpečnosti“ ([6]).

3.8 EHSV se domnívá, že navrhovaný poměr financování nákupu vybavení národních bezpečnostních operačních středisek (50 % z prostředků daného členského státu a 50 % z prostředků EU) je přiměřený, neboť členské státy a EU tak budou přispívat rovným dílem. Je nutné společnými silami zajistit, aby byla síť bezpečnostních operačních středisek náležitě vybavena špičkovými technologiemi a fungovala koordinovaným způsobem.

3.9 Národní bezpečnostní operační střediska se musí zaměřit na vypracování komplexních protokolů pro posuzování a testování bezpečnosti a měla by pravidelně provádět vyhodnocení. V rámci posuzování a zvyšování odolnosti vůči případným kybernetickým útokům by měla být také připravena realizovat zátěžové testy kritické infrastruktury v dané zemi, o jejichž výsledcích je pak nutné informovat v rámci evropského kybernetického štítu. Je rovněž zapotřebí společně vyhodnotit existující problémy, aktualizovat pokyny ohledně jejich oznamování a patřičně je také řešit.

3.10 EHSV vyjadřuje znepokojení nad tím, že Evropská komise zatím prostřednictvím prováděcích aktů nezavedla žádný systém kybernetické bezpečnosti a že z tohoto hlediska zatím nebyl certifikován žádný produkt, ačkoli jsou to již čtyři roky, co byl přijat akt o kybernetické bezpečnosti. Do vytváření systémů kybernetické bezpečnosti by měly být zapojeny odvětvové agentury EU a ve spolupráci s Evropským výborem pro normalizaci (CEN), Evropským výborem pro normalizaci v elektrotechnice (CENELEC) a Evropským ústavem pro telekomunikační normy (ETSI) by měl být přijat minimální evropský standard, mj. i ve vztahu k zařízením „internetu lidí“ a k internetu věcí.

3.11 Je nezbytné, aby byla informatika a kybernetická bezpečnost ve všech členských státech zařazena do vzdělávacích programů základních a středních škol. Podle EHSV je zapotřebí zvážit případné pobídky na podporu této iniciativy, a to vzhledem k tomu, že se posledních letech prohloubil nedostatek kvalifikovaných pracovníků v oblasti kybernetické bezpečnosti. EHSV vítá iniciativu týkající se Akademie kybernetických dovedností a domnívá se, že je nutné stanovit ukazatele pro měření pokroku při napravování tohoto nedostatku.

3.12 Digitální ekonomika čelí po celém světě stále větší hrozbě kybernetických útoků, která si žádá, aby jednotlivé země, průmysl a odborníci navázali rozsáhlejší spolupráci na mezinárodní úrovni a navrhli pro oblast kybernetické bezpečnosti společné definice a společná řešení. Mezinárodní spolupráce má zcela zásadní význam, aby bylo možné pochopit kybernetická rizika a měnící se charakter globálních kybernetických útoků, a připravit se tak na jejich překonávání. EU se musí zapojit do celosvětových jednání o zavedení mezinárodní strategie v oblasti kybernetické bezpečnosti, která bude založena na společném mezinárodním úsilí a rozsáhlejší spolupráci.

3.13 V zájmu dosažení skutečného odrazujícího účinku je nezbytné zlepšit reakci EU v oblasti prosazování práva a klást při tom důraz na odhalování pachatelů kybernetické kriminality, schopnost vysledovat je a na jejich stíhání. Je naprosto zásadní, aby byly kybernetické útoky co nejrychleji vyšetřeny a jejich pachatelé byli postaveni před soud, a to i diplomatickou cestou, jestliže se nacházejí mimo EU.

([6]) Stanovisko Evropského hospodářského a sociálního výboru ke společnému sdělení Evropskému parlamentu a Radě: Politika kybernetické obrany EU (stanovisko z vlastní iniciativy) (Úř. věst. C 293, 18.8.2023, s. 21).

4. **Konkrétní připomínky**

4.1 EHSV poukazuje na to, že panují odlišné názory, co se týče centralizovanějšího přijímání opatření na úrovni EU a pravomocí a jurisdikce členských států, a klade si otázku, zda se podaří dosáhnout konečné dohody o tomto návrhu, obzvláště s ohledem na to, že členské státy v závěrech Rady z roku 2021 ([7]) jasně uvedly, že jsou to ony, kdo nese odpovědnost za reakci na rozsáhlé kybernetické bezpečnostní incidenty a krize, které se jich týkají.

4.2 EHSV oceňuje, že po přijetí nařízení by měla být posílena úloha agentury ENISA a měly by jí být svěřeny další úkoly. Upozorňuje však, že na veškeré dodatečné aktivity jí musí být poskytnuty potřebné lidské zdroje, které budou tyto úkoly plnit, a také odpovídající finanční prostředky. V opačném případě nebude agentura ENISA moci plnit svou významnou strategickou úlohu v souladu s cíli EU v oblasti kybernetické bezpečnosti.

4.3 EHSV se domnívá, že z návrhu Komise není patrné, zda se může národní bezpečnostní operační středisko zapojit do více než jednoho přeshraničního bezpečnostního operačního střediska. Mimoto není jasné, zda se budou národní bezpečnostní operační střediska sdružovat na základě zeměpisných kritérií nebo pouze na základě vlastního rozhodnutí členských států.

4.4 EHSV žádá, aby bylo upřesněno, co se rozumí „významným množstvím údajů“, které je zmíněno v čl. 6 odst. 2 písm. a) nařízení, a jaké „cíle“ má Komise na mysli v písmenu c) téhož odstavce.

4.5 Pokud členské státy návrh na zřízení přeshraničních bezpečnostních operačních středisek přijmou, pak by koordinující bezpečnostní operační středisko v rámci určitého konsorcia mělo tuto funkci vykonávat po dobu jednoho roku a všechna bezpečnostní operační střediska by měla mít možnost se této role střídavě ujmout. Umožní to rovněž zajistit plné zapojení národních bezpečnostních operačních středisek a sdílené řízení s přeshraničními bezpečnostními operačními středisky.

4.6 EHSV se domnívá, že finanční prostředky, které EU poskytne hostitelskému konsorciu, by měly pokrýt 100 % nákladů na pořízení nástrojů a infrastruktury a 50 % nákladů na provoz (a nikoli 75 % a 50 %, jak je uvedeno v návrhu), aby tak byl urychlen proces zřizování konsorcií. Je třeba zaručit koordinaci zadávání zakázek.

4.7 EHSV se domnívá, že má-li kybernetický štít EU členským státům účinně pomoci připravit se na kybernetické incidenty a reagovat na ně, pak je nutné zavést konkrétní opatření v oblasti výkonnosti, která budou zaměřena na dosažení viditelných výsledků, a klíčové ukazatele výkonnosti, pomocí nichž bude možné tyto výsledky vyhodnotit. EHSV doporučuje, aby byly případy narušení kybernetické bezpečnosti systematicky zaznamenávány a informace o nich byly předávány subjektům, které je důvodně potřebují. Díky tomu bude možné posoudit situaci, zavést vhodná preventivní opatření a zamezit případným ztrátám.

4.8 EHSV bere na vědomí návrh, aby bylo členským státům umožněno požádat o úhradu nákladů spojených s vysláním týmů odborníků v rámci vzájemné pomoci, a souhlasí s ním. Vzájemnou pomoc je nepochybně třeba podpořit, zároveň je však zapotřebí celý mechanismus solidarity náležitě a postupně otestovat, a prověřit tak jeho účinnost, než bude plně zaveden.

4.9 EHSV vyjadřuje znepokojení nad tím, že stále více předních osobností zabývajících se umělou inteligencí na mezinárodní úrovni (například Elon Musk, Geoffrey Hinton a další) varuje před existenční hrozbou, kterou s sebou nese rozvoj umělé inteligence v neregulovaném prostředí. Umělá inteligence musí být regulována rozsáhlejším způsobem, než jak je tomu v aktu o umělé inteligenci ([8]). EHSV vyzývá k odpovědnému využívání technologií umělé inteligence ve všech projektech EU, včetně těch v oblasti kybernetické bezpečnosti. Je nutné neprodleně v této věci zahájit další jednání a posílit regulační rámec.

4.10 EHSV již v minulosti uvedl: „EU by měla zaujmout pevný postoj proti jakémukoliv systému sociálního hodnocení namířenému proti občanům. EHSV jasně uvádí, že skutečná demokracie nemůže existovat bez účinné ochrany osobních údajů“ ([9]). Základním pravidlem, kterým je třeba se při rozvoji posílených systémů kybernetické bezpečnosti v EU řídit, tedy musí být ochrana lidských práv a práva občanů na soukromí.

([7]) Závěry Rady ze dne 19. října 2021 o prozkoumání potenciálu iniciativy ke zřízení společné kybernetické jednotky.

([8]) Akt EU o umělé inteligenci.

([9]) Stanovisko Evropského hospodářského a sociálního výboru ke společnému sdělení Evropskému parlamentu a Radě: Politika kybernetické obrany EU (stanovisko z vlastní iniciativy) (Úř. věst. C 293, 18.8.2023, s. 21).

4.11 Evropští občané hrají důležitou roli, co se týče oznamování kybernetických hrozeb příslušným orgánům. EHSV se domnívá, že je naprosto nezbytné zavést patřičné mechanismy pro komunikaci s veřejností a s organizacemi občanské společnosti, a vyzývá ke zřízení speciální platformy pro shromažďování informací o kybernetických hrozbách. Dále pak žádá, aby byly v souvislosti s vytvářením nástrojů pro interakci s veřejností realizovány informační a propagační kampaně s cílem poukázat na dostupné nástroje.

4.12 EU a NATO by měly společně provést harmonizaci norem týkajících se kybernetické bezpečnosti a dalších technických norem v odvětví obrany, aby se tak v co největší míře odstranily administrativní překážky a omezila byrokratická zátěž. Kromě toho by měly EU a NATO spolupracovat i na definování norem pro zadávání zakázek a vytvoření účinného a transparentního rámce v této oblasti, který by podnikům – zejména pak podnikům malým a středním – umožnil účastnit se zadávacích řízení v podmínkách spravedlivé hospodářské soutěže.

4.13 EHSV se domnívá, že navrhovaná výše prostředků, jež mají být v této souvislosti vyčleněny na úrovni EU, je nedostatečná, a žádá, aby byly prozkoumány další zdroje, včetně kombinace různých soukromých zdrojů. Poukazuje na to, že Komise neuvedla přesný odhad nákladů na programy umělé inteligence, technologie analýzy dat a projekty rozvoje infrastruktury, jež bude v souvislosti s prováděním opatření stanovených v tomto nařízení nutné realizovat ve všech členských státech a na úrovni EU.

4.14 Komise navrhuje, aby jí byly svěřeny prováděcí pravomoci pro zajištění jednotných podmínek k provedení tohoto nařízení, zejména co se týče upřesnění podmínek interoperability mezi přeshraničními bezpečnostními operačními středisky, určení procesního režimu pro sdílení informací v případě kybernetických bezpečnostních incidentů, stanovení technických požadavků na bezpečnost evropského kybernetického štítu atd. EHSV je toho názoru, že všechny tyto aspekty měly být vyjasněny před předložením návrhu nařízení a měly do něj být zahrnuty, poněvadž kybernetická bezpečnost je v kompetenci členských států. Pokud by byly Komise svěřeny příliš rozsáhlé prováděcí pravomoci, mohlo by to navíc vyvolat zbytečné napětí z důvodu obcházení demokratického systému EU.

4.15 Akt o kybernetické bezpečnosti obsahuje průmyslovou složku, jejímž účelem je zřídit rezervu pro kybernetickou bezpečnost, a vytvořit tak jednotný trh pro řešení v oblasti kybernetické bezpečnosti. Postup podání žádosti o podporu z rezervy EU pro kybernetickou bezpečnost se však zdá být příliš zdlouhavý a nebyly v něm jasně stanoveny lhůty pro vyřízení žádosti. EHSV zdůrazňuje, že v případě kybernetického incidentu je nutné reagovat bleskurychle, což při nutnosti učinit nejprve celou řadu kroků zjevně nebude možné.

4.16 Evropská komise uvedla, že kvůli naléhavosti návrhu nebylo provedeno posouzení dopadů. Navrhla rovněž, že po uplynutí čtyř let od vstupu nařízení v platnost předloží Evropskému parlamentu a Radě podrobnou zprávu. EHSV se domnívá, že vzhledem k rychlému vývoji v oblasti kybernetické bezpečnosti by tato zpráva měla být předložena již po dvou letech, a to spolu s posouzením dopadů, které k nařízení nebylo připojeno. Mimoto důrazně doporučuje, aby byla v návrhu věnována větší pozornost respektování zásady subsidiarity a zásady proporcionality v souladu s čl. 4 odst. 2 SEU. Má to zásadní význam z hlediska zamezení vzniku napětí mezi centralizovanými opatřeními na úrovni EU a pravomocemi a jurisdikcí členských států.

4.17 Závěrem EHSV zdůrazňuje, že je důležité, aby byly otázky týkající se kybernetické bezpečnosti zohledňovány ve všech politikách EU.

V Bruselu dne 13. července 2023.

předseda
Evropského hospodářského a sociálního výboru
Oliver RÖPKE