Stanovisko Evropského hospodářského a sociálního výboru ke společnému sdělení Evropskému parlamentu a Radě: Politika kybernetické obrany EU

(stanovisko z vlastní iniciativy)

(2023/C 293/04)

Zpravodaj: **Anastasis YIAPANIS**

Spoluzpravodaj: **Alberto MAZZOLA**

Rozhodnutí plenárního shromáždění	20. 9. 2022
Právní základ	čl. 52 odst. 2 jednacího řádu
	stanovisko z vlastní iniciativy
Odpovědný orgán	Poradní komise pro průmyslové změny (CCMI)
Přijato v CCMI	27. 3. 2023
Přijato na plenárním zasedání	14. 6. 2023
Plenární zasedání č.	579
Výsledek hlasování	
(pro/proti/zdrželi se hlasování)	208/1/2

1. Závěry a doporučení

1.1 Evropský hospodářský a sociální výbor (EHSV) podporuje navrhovanou politiku EU v oblasti kybernetické obrany, ale očekával by, že se na vypracovávání těchto návrhů bude více podílet organizovaná občanská společnost. Výbor považuje v tomto okamžiku za obtížné posoudit, zda budou budoucí iniciativy uvedené ve společném sdělení provedeny a zda bude dosaženo jejich zamýšlených výsledků. Naléhavě vyzývá orgány EU a členské státy, aby ohlášené iniciativy označily za prioritní a urychleně u nich dosáhly pokroku.

1.2 EHSV zdůrazňuje, že jsou zapotřebí další opatření ke zvýšení schopnosti EU odhalovat kybernetické hrozby, a vyzývá k tomu, aby byly prostředky na výzkum a vývoj investovány do rozvoje špičkových schopností EU. Zásadní význam má spolupráce mezi soukromým a veřejným sektorem, která nesmí být jednosměrná. EHSV se domnívá, že koordinace na úrovni EU je nezbytná k řešení roztříštěnosti a k zajištění spolupráce a společných investic členských států.

1.3 EHSV podporuje vytvoření koordinačního střediska EU pro kybernetickou obranu a doporučuje, aby se členské státy zavázaly k zajištění nepřetržité rychlé reakce a posoudily kybernetickou připravenost a výkonnost mechanismů EU pro reakci na kybernetické krize se zaměřením jak na vojenské schopnosti, tak na kritická odvětví stanovená ve směrnici Evropského parlamentu a Rady (EU) 2022/2555 ([1]) (směrnice NIS 2). Výbor podporuje rozšíření mandátu Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC) o podporu činnosti koordinačního střediska EU pro kybernetickou obranu.

1.4 V zájmu posílení strategické autonomie a suverenity Unie v oblasti kybernetické bezpečnosti se EHSV domnívá, že by měla být vytvořena nebo ze soukromého sektoru převzata dynamická platforma pro testování a sdílení informací v reálném čase s cílem odhalit současné nedostatky ve stávajících schopnostech. Lze ji rovněž využít ke sdílení osvědčených postupů, oznamování kybernetických incidentů a k vytvoření seznamu EU týkajícího se všech pachatelů kybernetické kriminality.

([1]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

1.5 EHSV zdůrazňuje, že je třeba se lépe připravit na kybernetické útoky, jako jsou ruské útoky na Ukrajině, zaměřené zejména na kritickou infrastrukturu. Spolupráce mezi civilními a vojenskými systémy má zásadní význam pro účinné řešení krizí, interoperabilitu a zamezení zdvojování úsilí a investic, mimo jiné prostřednictvím simulovaných testovacích kybernetických útoků.

1.6 EHSV se domnívá, že investice do kybernetické obrany by měly být zaměřeny v prvé řadě na ochranu občanů a kritické infrastruktury EU, mj. díky využívání důvěryhodných dodavatelů hardwaru a softwaru. Důrazně požaduje včasné aktualizace priorit a investic, na nichž se EU a členské státy dohodnou za účasti příslušných soukromých zainteresovaných stran.

1.7 EU si musí zachovat a rozvíjet nezbytné kapacity k zabezpečení své digitální ekonomiky, společnosti, demokracie a kritických technologií a k poskytování klíčových služeb v oblasti kybernetické bezpečnosti. Pro zajištění strategické autonomie EU je zásadní snížit závislost na třetích zemích. EHSV považuje za zásadní, aby se EU ve střednědobém horizontu zaměřila na autonomii, pokud jde o klíčové technologie, a důrazně se zasazuje o to, aby výzkumná a výrobní zařízení byla zřizována podniky se sídlem v EU v mezích náležité evropské průmyslové politiky zaměřené na autonomní kybernetický systém.

1.8 Malé a střední podniky by měly obdržet cílenou podporu a mít přístup k programům financování, které zvýší jejich odolnost vůči kybernetickým útokům, jakož i k možnostem pomoci, odborné přípravy a vzdělávání v oblasti kybernetických rizik a toho, jak se proti nim zabezpečit. EU by měla vytvořit pobídkový mechanismus, který by malé a střední podniky podpořil v postupném obeznamování se s touto problematikou a v rozvoji jejich inovačních činností.

1.9 EHSV podporuje plán zřídit akademii v oblasti kybernetických dovedností a žádá Komisi, aby koordinovala a financovala rozsáhlé programy odborné přípravy a odborného vzdělávání, které zahrnou všechny členské státy a jejichž cílem bude vyškolit kvalifikovanou pracovní sílu pro všechny orgány a organizace zapojené do kybernetické obrany, jakož i pro soukromé civilní sítě.

1.10 Výbor považuje zvyšování povědomí občanů o kybernetické bezpečnosti za zásadní pro snížení vystavení kybernetickým útokům a požaduje vzdělávací osnovy v oblasti kybernetické bezpečnosti a programy celoživotního vzdělávání, které se zaměří na zlepšování kybernetických dovedností a znalostí. EHSV podporuje začlenění kybernetické bezpečnosti do všech budoucích veřejných politik EU a informování široké veřejnosti o kybernetických hrozbách.

1.11 EHSV se domnívá, že úzká spolupráce se spojenci NATO ve vojenských oblastech se musí zaměřit na plnou koordinaci a vzájemnost, společné projekty v oblasti výzkumu, vývoje a inovací, sdílení osvědčených postupů, rozsáhlé programy odborné přípravy a simulace kybernetických útoků, přičemž hlavním cílem je rozšířit společnou schopnost reakce.

1.12 Výbor vyzývá vysokého představitele, aby přezkoumal stávající dvoustranné dialogy v oblasti kybernetiky a zapojil se do dalších diskusí s dalšími zeměmi a příslušnými mezinárodními organizacemi s cílem vytvořit celosvětový rámec pro dodržování mezinárodního práva v kyberprostoru se silným důrazem na vzájemnost. Výbor se domnívá, že EU má předpoklady pro to, aby se ujala vedení v mezinárodních diskusích o budoucnosti kybernetické bezpečnosti, zejména v rámci Organizace spojených národů, neboť má pevný základ v oblasti základních demokratických svobod.

1.13 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, a domnívá se, že pro přeměnu hyperkonektivity v konkurenční výhodu je nezbytná odpovědná a účinná správa dat.

2. **Úvod a obecné připomínky**

2.1 Digitální expanze společností je spojena s velkým počtem hrozeb v oblasti kybernetické bezpečnosti, které vznikají v důsledku technologických modernizací. Počet kybernetických útoků a jejich sofistikovanost v posledních několika letech výrazně vzrostly, což oslabilo bezpečnost veřejných i soukromých subjektů. Ať už jde o ransomware, malware, e-mailové útoky, porušení zabezpečení údajů, dezinformace, útoky distribuovaným odmítnutím služby (DDoS) nebo jiné formy útoků, všechny představují stálou a nepřetržitou hrozbu pro bezpečnost celé EU.

2.2 EHSV vítá společné sdělení *Politika kybernetické obrany EU* ([2]) a domnívá se, že nyní nastala doba jednat, a to s naléhavostí a koordinovaně na úrovni EU, přičemž je třeba zahrnout civilní i vojenské systémy kyberprostoru a zajistit řádný investiční rámec pro schopnost kybernetické obrany. Výbor však konstatuje, že sdělení je pouhým prohlášením o odhodlání jednat a seznamem budoucích iniciativ EU, které by měly splnit cíle, a má za to, že není možné posoudit, zda budou tyto budoucí závazky skutečně přijaty, neboť budoucí jednání mezi spolunormotvůrci přirozeně ovlivní konečný výsledek akčního plánu EU pro kybernetickou bezpečnost.

2.3 Ruský útok na satelitní síť KA-SAT, který narušil komunikaci mezi ukrajinskými vojenskými silami, a nedávný skandál ohledně Érica Léandriho, který byl najat několika společnostmi v oblasti obrany za účelem kybernetické špionáže jejich jménem, staví kybernetickou bezpečnost na přední místo na seznamu bezpečnostních hrozeb v EU. Ačkoli je obecné nařízení o ochraně osobních údajů spolehlivým právním předpisem EU a je v platnosti již několik let, je zřejmé, že zranitelné je stále větší množství dostupných údajů a že se každým dnem zvyšuje riziko, že třetí strany překročí hranici zákonnosti.

2.4 Vzhledem k nadnárodní povaze kybernetických útoků je koordinace na úrovni EU nezbytná ke snížení stávající roztříštěnosti a k zajištění připravenosti členských států spolupracovat a společně investovat. To je obzvláště důležité pro budoucí případy, kdy by se jeden členský stát mohl stát cílem a všechny ostatní by měly mít možnost poskytnout okamžitou podporu.

3. **Společné úsilí o silnější kybernetickou obranu**

3.1 Výbor bere na vědomí ohlášené ambiciózní iniciativy týkající se zřízení koordinačního střediska EU pro kybernetickou obranu, vypracování projektu CyDEf-X, vytvoření týmů rychlé kybernetické reakce, vytvoření iniciativy EU pro kybernetickou solidaritu a prozkoumání vývoje systémů certifikace v oblasti kybernetické bezpečnosti pro produkty, služby a procesy IKT. EHSV doporučuje, aby se všechny členské státy zavázaly, že budou připraveny zajistit nepřetržitou rychlou reakci, přičemž koordinační středisko EU se zapojí do posuzování a vypracovávání pravidelných zpráv o kybernetické připravenosti členských států a o účinnosti evropského mechanismu pro reakci na kybernetické krize se zaměřením jak na vojenské schopnosti, tak na kritická odvětví stanovená ve směrnici NIS 2. Každý členský stát by měl mít odborníky speciálně vyškolené k zásahu v případě kybernetických incidentů a měl by pravidelně testovat jejich schopnost zasáhnout v jiných členských státech.

3.2 Sdělení sice obsahuje dlouhý seznam postupných zlepšení, EHSV by však uvítal jasný plán provádění těchto iniciativ s jasnou správou a lhůtami pro předložení a přijetí. Výbor by dále očekával, že organizovaná občanská společnost získá při vypracovávání těchto návrhů významnější úlohu.

3.3 EHSV se domnívá, že členské státy musí posílit svou vnitřní kapacitu pro boj proti kybernetickým hrozbám a zároveň se zapojit do projektů spolupráce a sdílet informace a osvědčené postupy se svými protějšky v ostatních členských státech. Je třeba rychle investovat do kapacit kybernetické obrany a rychleji zavádět technologie ([3]) ve všech členských státech a do společné připravenosti odhalovat kybernetické útoky, zotavit se z nich a bránit se proti nim. Za účelem podpory autonomie Unie v oblasti kybernetické bezpečnosti se Výbor domnívá, že by měla být vytvořena nebo ze soukromého sektoru převzata dynamická platforma pro testování a sdílení informací v reálném čase, která bude zaměřena na odhalení schopností, jež v současnosti chybějí.

3.4 EHSV sdílí názor, že vojenské operace v kyberprostoru by v této fázi měly zůstat výhradně v pravomoci členských států. Výbor podporuje ohlášenou spolupráci mezi vojenskými týmy EU pro reakci na počítačové hrozby (vojenské týmy CERT), týmy pro reakci na počítačové bezpečnostní incidenty (týmy CSIRT) a týmem pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT-EU).

3.5 Nedávno přijatá směrnice NIS 2 a směrnice o odolnosti kritických subjektů ([4]) již zavedly specifické vnitrostátní a odvětvové povinnosti pro rámec EU pro kybernetickou obranu. Je třeba přijmout další opatření ke zlepšení kolektivní detekční kapacity EU a EHSV vyzývá k investicím do výzkumu a vývoje pro rozvoj špičkových schopností EU.

([2]) Sdělení Komise Politika kybernetické obrany EU.
([3]) Například Akcelerátor obranných inovací pro severní Atlantik (DIANA).
([4]) Směrnice o odolnosti kritických subjektů.

4. **Zabezpečení obranného systému EU**

4.1 EHSV se domnívá, že inherentní složitost a rychle se vyvíjející technologické výzvy změnily obranný systém a že se kybernetická bezpečnost stala společným tématem jak pro vojenský, tak pro civilní sektor i pro občany EU. Spolupráce mezi civilními a vojenskými systémy je nyní důležitější než kdy jindy a měla by přinést výhody, pokud jde o účinnější řešení krizí, jakož i trvalý pokrok a interoperabilitu, aby se zabránilo zdvojování nebo násobení stejného úsilí a investic. Členské státy by měly být připraveny provést vnitrostátní zátěžové testy kritické infrastruktury s cílem posoudit a zvýšit odolnost vůči budoucím kybernetickým útokům.

4.2 EHSV se domnívá, že investice do kybernetické obrany musí být zaměřeny především na ochranu občanů a kritické infrastruktury EU. Vzhledem k rychlému tempu digitální transformace a rychlému vývoji prostředí hrozeb Výbor důrazně vyzývá k tomu, aby se EU a členské státy dohodly na včasných aktualizacích priorit a investic, a to za důkladné konzultace s příslušnými soukromými zainteresovanými stranami. Zařízení internetu věcí často nejsou chráněna tak dobře jako tradiční zařízení a EHSV požaduje, aby byla prostřednictvím platforem pro správu identit a přístupu (IDAM) zajištěna minimální úroveň bezpečnosti. Vzhledem k tomu, že klíčovou metodou k zajištění vyšší úrovně bezpečnosti je certifikace, Výbor rovněž požaduje, aby nový přístup EU k certifikaci kladl větší důraz na bezpečnost internetu věcí.

4.3 EU si musí vybudovat odolnost vůči kybernetickým útokům a efektivně je odvracet. Kritická infrastruktura musí být chráněna před kybernetickými útoky všeho druhu, a to i prostřednictvím obranných systémů EU. Výbor se domnívá, že 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. Pro strategickou autonomii EU má rovněž zásadní význam snížení závislosti na třetích zemích. EHSV se domnívá, že by do tohoto procesu měly být zapojeny odvětvové agentury EU (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA atd.) a že by měly poskytovat pokyny pro vývoj systémů v oblasti kybernetické bezpečnosti.

4.4 Pandemie COVID-19 urychlila digitální transformaci a přeměnila tradiční pracovní sílu na hybridní a/nebo pracující na dálku, čímž vytvořila nové pracovní vztahy a očekávání, jakož i novou třídu digitálních nomádů, jejichž počet roste. EHSV bere na vědomí rychlé změny na trhu práce, které vedly podniky k přijetí architektury na bázi „nulové důvěry“ prostřednictvím řešení IAM (správa identit a přístupů) a PAM (řízení privilegovaného přístupu). Výbor se domnívá, že tento typ řízení zdrojů podniků je spojen s novými řešeními v oblasti kybernetických hrozeb, a má za to, že je třeba podpořit soukromý sektor při zvyšování míry bezpečnosti svých inovativních digitálních řešení.

4.5 EHSV je poněkud zklamán tvrzením Komise, že „ve spolupráci s členskými státy by mohl být stanoven prováděcí plán“, a považuje takový prováděcí plán za povinný. Domnívá se, že by měl být vypracován společně s členskými státy a proveden co nejdříve. Výbor je znepokojen nedůrazným přístupem Komise a naléhavě vyzývá orgány EU a členské státy, aby usnadnily rychlý pokrok při provádění oznámených iniciativ.

5. **Investice do schopností v oblasti kybernetické obrany**

5.1 Díky rychlému technologickému vývoji se kyberprostor stal nejnovější operační oblastí, a to po zemi, moři, vzduchu a vesmíru. Vytvořil také velké příležitosti k trestné činnosti pro nepřátelské subjekty v kyberprostoru sahající od nezávislých hackerů až k profesionálním pachatelům kriminality, a dokonce i státním subjektům.

5.2 Investice do výzkumu a vývoje mají zásadní význam a EHSV vítá stávající specializované finanční prostředky v rámci programu Digitální Evropa, Evropského obranného fondu, programu Horizont Evropa a národních plánů pro oživení a odolnost. Výbor by však ocenil více nadnárodních projektů zaměřených na spolupráci a interoperabilitu mezi systémy kybernetické obrany ve všech členských státech, jakož i větší součinnost mezi nástroji financování, zejména nástrojů určených na podporu inovativních malých a středních podniků.

5.3 Jak bylo oznámeno ve Strategii kybernetické bezpečnosti EU již v roce 2020, Výbor konstatuje, že lhůtou pro vytvoření Společné kybernetické jednotky je letošní rok, a očekává zprávy o dokončení tohoto procesu a připravenosti EU reagovat na rozsáhlé kybernetické incidenty. EHSV předpokládá, že zlepší informovanost EU o situaci a celkovou schopnost reagovat a zotavit se.

5.4 Výbor podporuje rozšíření mandátu ECCC o podporu činnosti koordinačního střediska EU pro kybernetickou obranu. Kromě toho by tato síť mohla podpořit digitální suverenitu Evropy vytvořením konkurenceschopné evropské průmyslové základny pro klíčové technologické schopnosti, která by byla částečně založena na práci vyvíjené v rámci smluvních partnerství veřejného a soukromého sektoru (PPP). PPP se ukázala být nejúčinnějším přístupem ke zlepšení kybernetické bezpečnosti celého digitálního systému, nemohou však být jednosměrná: veřejné instituce musí rovněž sdílet své operativní informace se soukromým sektorem.

5.5 EHSV konstatuje, že má-li EU řešit budoucí pokusy o hackerské útoky z kvantových počítačů, musí okamžitě investovat do špičkových technologií, jako je postkvantová kryptografie. Domnívá se, že je nezbytné, aby se Evropa ve střednědobém horizontu zaměřila na autonomii, a důrazně se zasazuje o to, aby výzkumná a výrobní zařízení byla zřizována podniky se sídlem v EU. EHSV považuje za důležité navýšit zdroje EU v oblasti digitálního výzkumu a inovací a podpořit investice provozovatelů a dodavatelů do nových technických bezpečnostních prvků, mj. i v souvislosti s novými trendy, jako je rozšířená realita a metaverzum. Zejména je nezbytné vybudovat evropskou distribuovanou cloudovou infrastrukturu založenou na evropských pravidlech týkajících se témat, jako je ukládání a zpracování dat ([5]).

5.6 Malé a střední podniky by měly být středem konkrétní pozornosti a měly by mít přístup k programům financování, které zvýší jejich připravenost na kybernetické útoky, jakož i k možnostem pomoci, odborné přípravy a vzdělávání, které jim pomohou pochopit kybernetická rizika a to, jak se proti nim zabezpečit. EU by měla vytvořit pobídkový mechanismus, který by malé a střední podniky podpořil v postupném obeznamování se s touto problematikou.

5.7 Komise odhaduje stávající nedostatek dovedností v oblasti kybernetické bezpečnosti na půl milionu lidí a EHSV oceňuje návrh na vytvoření akademie v oblasti kybernetických dovedností. Je zřejmé, že ke snížení nedostatku dovedností nestačí úsilí na úrovni členských států, a proto Výbor navrhuje, aby se Komise spolu se zahájením činnosti akademie chopila příležitosti, kterou nabízí Evropský rok dovedností, a koordinovala a financovala rozsáhlé programy odborné přípravy a programy OVP na úrovni EU, do nichž budou zapojeny všechny členské státy a jež se zaměří na vyškolení kvalifikované pracovní síly pro všechny orgány a subjekty zapojené do kybernetické obrany, jakož i pro soukromé civilní sítě. Zvláštní důraz musí být kladen na odbornou přípravu pracovní síly, zejména v oblasti přírodních věd, technologií, inženýrství a matematiky (STEM).

5.8 EHSV se dále domnívá, že je nezbytné zvýšit povědomí občanů o kybernetické bezpečnosti, aby se snížilo vystavení kybernetickým útokům, zejména pokud jde o základní kybernetickou trestnou činnost namířenou proti obyvatelstvu jako celku. Výbor požaduje vzdělávací osnovy v oblasti kybernetické bezpečnosti a programy celoživotního vzdělávání v téže oblasti, které se zaměří na zlepšení kybernetických dovedností a zvýší povědomí o kybernetické bezpečnosti a její atraktivitu pro občany, zejména pro mladší generaci. EHSV podporuje začlenění úvah o kybernetické bezpečnosti do všech budoucích veřejných politik EU a informování široké veřejnosti o kybernetických hrozbách, mj. prostřednictvím bezplatné odborné přípravy pro širokou veřejnost, bezplatných aplikací pro mobilní telefony nebo televizní reklamy v hlavním vysílacím čase. Souběžně s těmito opatřeními je třeba podporovat rozsáhlý kulturní rozvoj na všech úrovních společnosti směrem k přístupu zaměřenému na kybernetickou bezpečnost.

5.9 EHSV je přesvědčen, že je nezbytné zaručit posouzení rizikového profilu dodavatelů a uplatnit příslušná omezení vůči dodavatelům považovaným za vysoce rizikové, včetně nezbytných zákazů, pokud jde o klíčová aktiva a aplikace definované v rámci koordinovaného posouzení rizik na úrovni EU jako kritické a citlivé, a certifikovat důvěryhodné dodavatele hardwaru a softwaru.

6. **Partner pro řešení společných výzev**

6.1 Míra připravenosti na budoucí kybernetické útoky se v jednotlivých členských státech značně liší. EHSV se domnívá, že bezprostředním prvním krokem je zřízení komunikační platformy pro výměnu osvědčených postupů v rámci EU, v jejímž rámci budou moci členské státy, které dosáhly největšího pokroku v kybernetické oblasti, sdílet své znalosti s ostatními zeměmi a usnadnit jejich okamžité využití. To by pomohlo zlepšit vzájemnou důvěru mezi vnitrostátními subjekty. Za druhé se Výbor domnívá, že je zapotřebí užší spolupráce mezi státními a nestátními subjekty v celé EU, aby se zlepšila kybernetická bezpečnost produktů a služeb v rámci vnitřního trhu. EHSV rovněž navrhuje vytvoření společné platformy EU pro hlášení kybernetických incidentů, včetně černé listiny EU všech aktivistů v oblasti kybernetické trestné činnosti.

([5]) Například Gaia-X, francouzsko-německá iniciativa.

6.2 EHSV je toho názoru, že úzká spolupráce s našimi vojenskými spojenci v NATO musí být zaměřena nejen na budování kapacit a včasné odhalování, ale také na společné projekty v oblasti výzkumu, vývoje a inovací, sdílení osvědčených postupů a výměny mezi odborníky, rozsáhlé programy odborné přípravy a simulace kybernetických útoků. Hlavním cílem by mělo být rozšířit společnou schopnost reakce a vytvořit součinnost pro boj proti budoucím hybridním hrozbám v návaznosti na společná prohlášení z Varšavy z roku 2016 a z Bruselu z roku 2018. Spolupráce mezi EU a NATO nabízí ještě řadu možností, které lze využít, a okamžitý pokrok může přinést skutečnou změnu, pokud jde o zajištění bezpečnosti našich občanů a společností.

6.3 Výbor se domnívá, že diskuse na celosvětové úrovni a s našimi mezinárodními partnery by měly vytvořit podmínky pro podporu globálního a otevřeného kyberprostoru, který chrání lidská práva, základní svobody a právní stát a zaměřuje se na vypracování závazných mezinárodních norem v odvětvích s rychlým digitálním vývojem. Výbor doporučuje vysokému představiteli, aby přezkoumal stávající dvoustranné dialogy v oblasti kybernetiky a zapojil se do dalších jednání s dalšími zeměmi a příslušnými mezinárodními organizacemi s cílem prosazovat globální rámec pro uplatňování mezinárodního práva v kyberprostoru na základě přísné podmínky vzájemnosti.

6.4 V neposlední řadě se Výbor domnívá, že EU má nejlepší předpoklady k vedení mezinárodních diskusí o budoucnosti kybernetické bezpečnosti, zejména v rámci diskusí v OSN, a to díky svému pevnému základu v oblasti základních demokratických svobod. EU se musí rovněž zapojit do boje proti totalitním režimům, které sledují údaje týkající se občanů a porušují jejich práva a svobody, a měla by důrazně vystupovat proti jakémukoliv systému bodového hodnocení sociálního kreditu namířenému proti občanům. EHSV jasně uvádí, že skutečná demokracie nemůže existovat bez účinné ochrany osobních údajů, a domnívá se, že pro přeměnu hyperkonektivity ve výhodu je nezbytná odpovědná a účinná správa dat.

V Bruselu dne 14. června 2023.

předseda
Evropského hospodářského a sociálního výboru
Oliver RÖPKE