Stanovisko Európskeho hospodárskeho a sociálneho výboru – Spoločné oznámenie Európskemu parlamentu a Rade – Politika EÚ v oblasti kybernetickej obrany

(stanovisko z vlastnej iniciatívy)

(2023/C 293/04)

Spravodajca: **Anastasis YIAPANIS**

Spoluspravodajca: **Alberto MAZZOLA**

Rozhodnutie plenárneho zhromaždenia	20. 9. 2022
Právny základ	článok 52 ods. 2 rokovacieho poriadku
	stanovisko z vlastnej iniciatívy
Príslušná sekcia	poradná komisia pre priemyselné zmeny (CCMI)
Prijaté v sekcii	27. 3. 2023
Prijaté v pléne	14. 6. 2023
Plenárne zasadnutie č.	579
Výsledok hlasovania	
(za/proti/zdržalo sa)	208/1/2

1. **Závery a odporúčania**

1.1. Európsky hospodársky a sociálny výbor (EHSV) podporuje navrhovanú politiku EÚ v oblasti kybernetickej obrany, ale očakával by, že pri vypracúvaní týchto návrhov bude zohrávať významnejšiu úlohu organizovaná občianska spoločnosť. Výboru sa zdá v tejto chvíli ťažké posúdiť, či sa budúce iniciatívy uvedené v spoločnom oznámení zrealizujú a či sa dosiahnu zamýšľané výsledky. Naliehavo vyzýva inštitúcie EÚ a členské štáty, aby oznámené iniciatívy zaradili medzi svoje priority a urýchlene ich presadzovali.

1.2. EHSV zdôrazňuje potrebu ďalších opatrení na zvýšenie schopnosti EÚ odhaľovať kybernetické hrozby a žiada, aby sa financovanie výskumu a vývoja zameralo na rozvoj špičkových spôsobilostí v EÚ. Je nevyhnutná spolupráca medzi súkromným a verejným sektorom, ktorá nesmie byť jednosmerná. EHSV sa domnieva, že na riešenie roztrieštenosti a zabezpečenie spolupráce a spoločných investícií medzi členskými štátmi je potrebná koordinácia na úrovni EÚ.

1.3. EHSV podporuje vytvorenie Koordinačného centra kybernetickej obrany EÚ a odporúča, aby sa členské štáty zaviazali k nepretržitej rýchlej reakcii a vyhodnotili kybernetickú pripravenosť a výkonnosť mechanizmov reakcie EÚ na kybernetické krízy, a to so zameraním na vojenské spôsobilosti aj kritické odvetvia určené v smernici Európskeho parlamentu a Rady (EÚ) 2022/2555 ([1]) (smernica NIS 2). Výbor schvaľuje rozšírenie mandátu Európskeho centra priemyselných, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti (ECCC) s cieľom pomáhať pri práci Koordinačného centra kybernetickej obrany EÚ.

1.4. EHSV sa domnieva, že na posilnenie strategickej autonómie a suverenity Únie v oblasti kybernetickej bezpečnosti by sa mala vytvoriť alebo prevziať od súkromného sektora dynamická platforma na testovanie a výmenu informácií v reálnom čase, aby sa zistili súčasné nedostatky v existujúcich spôsobilostiach. Môže slúžiť aj na výmenu najlepších postupov, nahlasovanie kybernetických incidentov a vytváranie európskeho zoznamu všetkých páchateľov počítačovej kriminality.

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2) (Ú. v. EÚ L 333, 27.12.2022, s. 80).

1.5. EHSV zdôrazňuje potrebu lepšej prípravy na kybernetické útoky zamerané najmä na kritickú infraštruktúru, ako boli ruské útoky na Ukrajine. Pre krízové riadenie, interoperabilitu a zabránenie duplicite úsilia a investícií má zásadný význam spolupráca medzi civilnými a vojenskými ekosystémami, a to aj prostredníctvom simulovaných testovacích kybernetických útokov.

1.6. EHSV sa domnieva, že pri investíciách do kybernetickej obrany by mala byť prioritou ochrana občanov EÚ a jej kritickej infraštruktúry, a to aj prostredníctvom využívania dôveryhodných dodávateľov hardvéru a softvéru. Trvá na včasnej aktualizácii priorít a investícií, na ktorých sa dohodnú EÚ a členské štáty za účasti príslušných súkromných zainteresovaných strán.

1.7. EÚ si musí zachovať a rozvíjať potrebné spôsobilosti na zabezpečenie svojho digitálneho hospodárstva, spoločnosti, demokracie a kritických technológií a na poskytovanie kľúčových služieb v oblasti kybernetickej bezpečnosti. Na zabezpečenie strategickej autonómie EÚ je nevyhnutné znížiť jej závislosť od tretích krajín. EHSV považuje za nevyhnutné, aby EÚ prijala strednodobý prístup k autonómii, pokiaľ ide o kľúčové technológie, a dôrazne sa zasadzuje za to, aby výskumné a výrobné zariadenia zriaďovali spoločnosti so sídlom v EÚ a aby sa príslušná európska priemyselná politika zamerala na autonómny ekosystém kybernetickej bezpečnosti.

1.8. MSP by mali dostávať cielenú podporu a mali by mať prístup k programom financovania, ktoré im pomôžu zvýšiť ich odolnosť voči kybernetickým útokom. Mali by mať k dispozícii aj pomoc, odbornú prípravu a možnosti vzdelávania v oblasti kybernetických rizík a spôsobov ochrany pred nimi. EÚ by mala vytvoriť stimulačný mechanizmus, ktorý by podporoval postupné oboznamovanie sa MSP s touto problematikou a rozvoj inovatívnych MSP.

1.9. EHSV podporuje plán na zriadenie Akadémie zručností v oblasti kybernetickej bezpečnosti a žiada Európsku komisiu, aby koordinovala a financovala rozsiahle programy odbornej prípravy a odborného vzdelávania, ktoré by zahŕňali všetky členské štáty a ktorých cieľom by bolo zabezpečiť kvalifikovanú pracovnú silu pre všetky agentúry a organizácie zapojené do kybernetickej obrany, ako aj pre súkromné civilné siete.

1.10. Výbor považuje zvyšovanie informovanosti občanov o kybernetickej bezpečnosti za kľúčové pri znižovaní vystavenia kybernetickým útokom a vyzýva na vytvorenie učebných osnov a programov celoživotného vzdelávania v oblasti kybernetickej bezpečnosti, ktoré by boli zamerané na zlepšenie zručností a znalostí v oblasti kybernetickej bezpečnosti. EHSV podporuje začlenenie kybernetickej bezpečnosti do všetkých budúcich verejných politík EÚ a informovanie širokej verejnosti o kybernetických hrozbách.

1.11. EHSV sa domnieva, že intenzívna spolupráca so spojencami z NATO vo vojenských oblastiach sa musí zamerať na plnú koordináciu a reciprocitu, spoločné projekty v oblasti výskumu, vývoja a inovácií, výmenu najlepších postupov a rozsiahle programy odbornej prípravy a simulácie kybernetických útokov, pričom hlavným cieľom je rozšíriť spoločnú schopnosť reakcie.

1.12. Výbor vyzýva vysokého predstaviteľa, aby preskúmal súčasné dvojstranné kybernetické dialógy a zapojil sa do ďalších diskusií s inými krajinami a príslušnými medzinárodnými organizáciami s cieľom vytvoriť celosvetový rámec pre dodržiavanie medzinárodného práva v kybernetickom priestore so silným dôrazom na reciprocitu. Výbor sa domnieva, že EÚ má vhodnú pozíciu na to, aby prevzala vedúcu úlohu v medzinárodných rokovaniach o budúcnosti kybernetickej bezpečnosti, najmä v rámci Organizácie Spojených národov, keďže pevne stojí na základných demokratických slobodách.

1.13. EÚ by mala zaujať rozhodný postoj proti akémukoľvek systému sociálneho bodovania občanov. EHSV jasne zdôrazňuje, že skutočná demokracia nemôže existovať bez efektívnej ochrany osobných údajov, a domnieva sa, že na to, aby sa hyperkonektivita stala konkurenčnou výhodou, je nevyhnutná zodpovedná a účinná správa údajov.

2. **Úvod a všeobecné pripomienky**

2.1. Digitálna expanzia spoločností so sebou prináša veľké množstvo kybernetických hrozieb, ktoré vznikajú v dôsledku technologických inovácií. Počet a sofistikovanosť kybernetických útokov v posledných rokoch výrazne vzrástli, čo ohrozuje bezpečnosť verejných aj súkromných subjektov. Či už ide o ransomvér, malvér, e-mailové útoky, úniky údajov, dezinformácie, distribuované útoky na vyradenie služby (DDoS) alebo iné formy útokov, všetky predstavujú trvalú a nepretržitú hrozbu pre bezpečnosť EÚ ako celku.

2.2. EHSV víta spoločné oznámenie o *politike EÚ v oblasti kybernetickej obrany* ([2]) a domnieva sa, že teraz je čas konať, a to naliehavo a koordinovane na úrovni EÚ, pričom treba zapojiť civilné aj vojenské ekosystémy kybernetického priestoru a zabezpečiť vhodný investičný rámec pre spôsobilosti kybernetickej obrany. Výbor však konštatuje, že oznámenie je len vyhlásením o odhodlaní konať a zoznamom budúcich iniciatív EÚ, ktoré by mali priniesť výsledky, a domnieva sa, že nie je možné posúdiť, či sa tieto budúce záväzky skutočne zrealizujú, keďže na konečné výsledky akčného plánu EÚ v oblasti kybernetickej bezpečnosti prirodzene budú mať vplyv budúce rokovania medzi spoluzákonodarcami.

2.3. Ruský útok na satelitnú sieť KA-SAT, ktorý narušil komunikáciu medzi ukrajinskými vojenskými silami, a nedávny škandál okolo Érica Léandriho, ktorého niektoré spoločnosti pôsobiace v oblasti obrany poverili kybernetickou špionážou v ich mene, stavajú kybernetickú bezpečnosť na prvé miesto v zozname bezpečnostných hrozieb v EÚ. Hoci je všeobecné nariadenie o ochrane údajov (GDPR) pevnou súčasťou právnych predpisov EÚ a platí už niekoľko rokov, je zrejmé, že čoraz väčšie množstvo dostupných údajov je zraniteľné a riziko, že tretie strany prekročia hranicu zákonnosti, je každým dňom vyššie.

2.4. Vzhľadom na nadnárodnú povahu kybernetických útokov je potrebná koordinácia na úrovni EÚ, aby sa zmenšila súčasná roztrieštenosť a zabezpečila pripravenosť členských štátov na spoluprácu a spoločné investície. Je to dôležité najmä pre budúce prípady, v ktorých by sa mohol stať terčom jeden členský štát, aby mu všetky ostatné štáty mali možnosť poskytnúť okamžitú podporu.

3. **Spoločné úsilie o silnejšiu kybernetickú obranu**

3.1. Výbor berie na vedomie oznámené ambiciózne iniciatívy na zriadenie Koordinačného centra kybernetickej obrany EÚ, na rozvoj projektu CyDEf-X, na vytvorenie tímov rýchlej reakcie na kybernetické incidenty, na rozvoj iniciatívy na podporu kybernetickej solidarity EÚ a na preskúmanie možností vývoja systémov certifikácie kybernetickej bezpečnosti produktov, služieb a procesov IKT. EHSV odporúča, aby sa všetky členské štáty zaviazali, že budú nepretržite pripravené poskytnúť rýchlu reakciu, pričom koordinačné centrum EÚ by sa malo podieľať na posudzovaní kybernetickej pripravenosti členských štátov a účinnosti európskeho mechanizmu krízovej reakcie na kybernetické hrozby a na vypracúvaní pravidelných správ o nich so zameraním na vojenské spôsobilosti, ako aj na kritické odvetvia určené v smernici NIS 2. Každý členský štát by mal mať špecialistov osobitne vyškolených na zásahy v prípade kybernetických incidentov a mal by pravidelne testovať ich schopnosť zasahovať v iných členských štátoch.

3.2. Hoci oznámenie obsahuje dlhý zoznam postupných zlepšení, EHSV by si želal, aby bol k dispozícii jasný plán realizácie týchto iniciatív s jasným riadením a termínmi na ich predloženie a schválenie. Okrem toho by výbor očakával, že pri vypracúvaní týchto návrhov bude zohrávať významnejšiu úlohu organizovaná občianska spoločnosť.

3.3. EHSV sa domnieva, že členské štáty musia posilniť svoje vnútorné spôsobilosti na boj proti kybernetickým hrozbám a zároveň sa zapojiť do projektov spolupráce a výmeny informácií a najlepších postupov so svojimi partnermi v iných členských štátoch. Je potrebné rýchlo investovať jednak do spôsobilostí v oblasti kybernetickej obrany a urýchliť zavádzanie technológií ([3]) vo všetkých členských štátoch, jednak do spoločnej pripravenosti na odhaľovanie kybernetických útokov, obnovu po nich a obranu proti nim Výbor sa domnieva, že na podporu autonómie Únie v oblasti kybernetickej bezpečnosti je potrebné vytvoriť dynamickú platformu na testovanie a výmenu informácií v reálnom čase alebo ju prevziať od súkromného sektora so zameraním na identifikáciu spôsobilostí, ktoré v súčasnosti chýbajú.

3.4. EHSV sa stotožňuje s názorom, že vojenské operácie v kybernetickom priestore by v tejto fáze mali zostať výlučne v kompetencii členských štátov; výbor podporuje ohlásenú spoluprácu medzi vojenskými tímami reakcie na počítačové núdzové situácie (milCERT) EÚ, jednotkami pre riešenie počítačových bezpečnostných incidentov (CSIRT) a tímom reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach (CERT-EU).

3.5. V nedávno prijatej smernici NIS 2 a smernici o odolnosti kritických subjektov (CER) ([4]) sa už zaviedli konkrétne vnútroštátne a odvetvové povinnosti pre rámec kybernetickej obrany EÚ. Na zlepšenie kolektívnej detekčnej kapacity EÚ sú však potrebné ďalšie opatrenia a EHSV vyzýva na investície do výskumu a vývoja na rozvoj špičkových spôsobilostí EÚ.

([2]) Ú. v. EÚ – Oznámenie Komisie o politike EÚ v oblasti kybernetickej obrany.
([3]) Napríklad Severoatlantický akcelerátor pre obranné inovácie NATO (DIANA).
([4]) Smernica CER.

4. **Zabezpečenie obranného ekosystému EÚ**

4.1. EHSV sa domnieva, že prirodzená zložitosť a rýchlo sa vyvíjajúce technologické výzvy zmenili ekosystém obrany a že kybernetická bezpečnosť sa stala spoločnou témou pre vojenský aj civilný sektor, ako aj pre občanov EÚ. Spolupráca medzi civilnými a vojenskými ekosystémami je v súčasnosti dôležitejšia ako kedykoľvek predtým a mala by priniesť výhody v podobe účinnejšieho krízového riadenia, ako aj nepretržitého pokroku a interoperability, čím sa zabráni duplicite alebo znásobovaniu rovnakého úsilia a investícií. Členské štáty by mali byť pripravené vykonávať záťažové testy národnej kritickej infraštruktúry s cieľom posúdiť a zvýšiť odolnosť voči budúcim kybernetickým útokom.

4.2. EHSV sa domnieva, že investície do kybernetickej obrany musia byť prioritne zamerané na ochranu občanov EÚ a jej kritickej infraštruktúry. Vzhľadom na rýchle tempo digitálnej transformácie a rýchly vývoj v oblasti hrozieb výbor dôrazne žiada, aby sa EÚ a členské štáty dohodli na včasnej aktualizácii priorít a investícií a aby sa uskutočnili dôkladné konzultácie s príslušnými súkromnými zainteresovanými stranami. Zariadenia internetu vecí (IoT) často nie sú chránené tak dobre ako tradičné zariadenia a EHSV požaduje, aby sa prostredníctvom platforiem IDAM zabezpečila minimálna úroveň ich zabezpečenia. Keďže kľúčovou metódou na zaistenie vyššej úrovne bezpečnosti je certifikácia, výbor žiada, aby sa v novom prístupe EÚ k certifikácii kládol väčší dôraz na zabezpečenie internetu vecí.

4.3. Európa musí budovať odolnosť proti kybernetickým útokom a účinne odrádzať páchateľov. Kritická infraštruktúra musí byť chránená pred kybernetickými útokmi všetkého druhu vrátane obranných systémov EÚ. Výbor sa domnieva, že je v strategickom záujme EÚ zabezpečiť, aby si Únia zachovala a rozvíjala základné spôsobilosti na zabezpečenie svojho digitálneho hospodárstva, spoločnosti a demokracie, aby tak dosiahla úplnú technologickú suverenitu ako jediný spôsob ochrany kritických technológií a poskytovania účinných kľúčových služieb v oblasti kybernetickej bezpečnosti. Pre strategickú autonómiu EÚ je zároveň nevyhnutné zníženie závislosti od tretích krajín. EHSV sa domnieva, že do tohto procesu by mali byť zapojené odvetvové agentúry EÚ (ENISA, EASA, ERA, EMA, EBA, ESA, HADEA atď.), ktoré by mali poskytovať usmernenia pri vytváraní systémov kybernetickej bezpečnosti.

4.4. Pandémia ochorenia COVID-19 urýchlila prechod na digitálne technológie a transformovala tradičnú prácu na hybridnú a/alebo diaľkovú, čím sa vytvorili nové pracovné vzťahy a vznikli nové očakávania, ako aj nová trieda digitálnych nomádov, ktorých počet sa zvyšuje. EHSV poukazuje na rýchle zmeny na trhu práce, ktoré viedli k tomu, že podniky prijali tzv. architektúru nulovej dôvery prostredníctvom riešení IAM (riadenie identity a prístupu) a PAM (správa privilegovaného prístupu). Výbor sa domnieva, že tento typ riadenia zdrojov podnikov prináša nové riešenia súvisiace s kybernetickými hrozbami, a domnieva sa, že súkromný sektor je potrebné podporovať pri posilňovaní úrovne zabezpečenia svojich inovatívnych digitálnych riešení.

4.5. EHSV je sklamaný vyhlásením Komisie, že „v spolupráci s členskými štátmi by sa mohol stanoviť plán vykonávania“, a považuje takýto plán implementácie za nevyhnutnosť. Domnieva sa, že by sa mal vypracovať spoločne s členskými štátmi a čo najskôr začať vykonávať. Výbor je znepokojený ľahkovážnym postojom Komisie a vyzýva inštitúcie EÚ a členské štáty, aby umožnili rýchly pokrok v ohlásených iniciatívach.

5. **Investície do spôsobilostí v oblasti kybernetickej obrany**

5.1. S rýchlym technologickým vývojom sa kybernetický priestor stal po pozemnej, námornej, vzdušnej a vesmírnej vojne najnovšou doménou. Zároveň vytvoril veľké príležitosti na páchanie trestnej činnosti pre škodlivé kybernetické subjekty od nezávislých hekerov až po profesionálnych páchateľov trestnej činnosti a dokonca aj štátne subjekty.

5.2. Preto sú nevyhnutné investície do výskumu a vývoja a EHSV víta existujúce účelové fondy v rámci programu Digitálna Európa, Európskeho obranného fondu, programu Horizont Európa a národných plánov obnovy. Výbor by však ocenil viac nadnárodných projektov zameraných na spoluprácu a interoperabilitu medzi systémami kybernetickej obrany vo všetkých členských štátoch, ako aj väčšie synergie medzi nástrojmi ich financovania, ktoré by podporovali najmä inovatívne MSP.

5.3. Výbor konštatuje, že ako sa v roku 2020 oznámilo v stratégii kybernetickej bezpečnosti EÚ, lehota na vytvorenie spoločnej kybernetickej jednotky je tento rok, a očakáva správy o dokončení tohto procesu a pripravenosti EÚ reagovať na rozsiahle kybernetické incidenty. EHSV očakáva, že táto jednotka zlepší v EÚ situačné povedomie a celkovú schopnosť reakcie a obnovy.

5.4. EHSV podporuje rozšírenie mandátu ECCC o podporu činnosti Koordinačného centra kybernetickej obrany EÚ. Okrem toho by táto sieť mohla podporiť európsku technologickú suverenitu vytvorením konkurencieschopnej európskej priemyselnej základne pre kľúčové technologické spôsobilosti, ktorá by bola čiastočne založená na práci rozvinutej v rámci zmluvných verejno-súkromných partnerstiev. Verejno-súkromné partnerstvá sa ukázali ako najúčinnejší prístup k zlepšeniu kybernetickej bezpečnosti celého digitálneho ekosystému, ale nemôžu byť jednosmerné: aj verejné inštitúcie sa musia deliť o svoje informácie so súkromným sektorom.

5.5. EHSV konštatuje, že EÚ musí v záujme riešenia budúcich pokusov o hekerské útoky zo strany kvantových počítačov okamžite investovať do špičkových technológií, ako je postkvantová kryptografia. Domnieva sa, že je nevyhnutné, aby sa Európa v strednodobom horizonte zamerala na svoju autonómiu, a dôrazne sa zasadzuje za to, aby výskumné a výrobné zariadenia zriaďovali spoločnosti so sídlom v EÚ. EHSV považuje za dôležité zvýšiť objem zdrojov EÚ na digitálny výskum a inovácie a podporiť investície prevádzkovateľov a dodávateľov do nových funkcií technického zabezpečenia, ktoré súvisia aj s novými trendmi, ako je rozšírená realita a metaverzum. Predovšetkým je nevyhnutné vybudovať európsku distribuovanú cloudovú infraštruktúru založenú na európskych pravidlách týkajúcich sa napríklad ukladania a spracovania údajov ([5]).

5.6. Malým a stredným podnikom by sa mala venovať osobitná pozornosť a mali by mať prístup k programom financovania, ktoré im pomôžu zvýšiť ich pripravenosť na kybernetické útoky, ako aj k programom pomoci, odbornej prípravy a vzdelávania, ktoré im pomôžu pochopiť kybernetické riziká a spôsoby ochrany. EÚ by mala vytvoriť stimulačný mechanizmus, ktorý by podporoval postupné oboznamovanie sa MSP s touto problematikou.

5.7. Komisia odhaduje, že v súčasnosti chýba v oblasti kybernetickej bezpečnosti pol milióna ľudí, a EHSV oceňuje návrh na vytvorenie Akadémie zručností v oblasti kybernetickej bezpečnosti. Je zrejmé, že na zníženie nedostatku kvalifikovaných pracovníkov nestačí úsilie na úrovni členských štátov, a preto výbor navrhuje, aby Komisia spolu so spustením akadémie využila príležitosť, ktorú ponúka Európsky rok zručností, a koordinovala a financovala rozsiahle programy odbornej prípravy a vzdelávania na úrovni EÚ, ktoré by zahŕňali všetky členské štáty a zameriavali sa na zabezpečenie kvalifikovanej pracovnej sily pre všetky agentúry a orgány zapojené do kybernetickej obrany, ako aj pre súkromné civilné siete. Osobitný dôraz sa musí klásť na odbornú prípravu pracovnej sily, najmä v oblasti vedy, technológií, inžinierstva a matematiky (STEM).

5.8. Okrem toho sa EHSV domnieva, že je nevyhnutné zvýšiť informovanosť občanov o kybernetickej bezpečnosti, aby sa znížilo vystavenie kybernetickým útokom, najmä pokiaľ ide o základnú počítačovú trestnú činnosť zameranú na širokú verejnosť. Výbor žiada, aby sa vzdelávacie programy a programy celoživotnej odbornej prípravy v oblasti kybernetickej bezpečnosti zamerali na zlepšenie kybernetických zručností, aby sa kybernetická bezpečnosť stala pre občanov, najmä pre mladú generáciu, známejšou a atraktívnejšou témou. EHSV podporuje začlenenie problematiky kybernetickej bezpečnosti do všetkých budúcich verejných politík EÚ a informovanie širokej verejnosti o kybernetických hrozbách, a to aj prostredníctvom bezplatných vzdelávacích programov pre širokú verejnosť, bezplatných informačných aplikácií pre mobilné telefóny alebo prostredníctvom komunikácie v rámci televízneho vysielania v hlavnom vysielacom čase. Súbežne s týmito opatreniami je potrebné podporovať rozsiahly kultúrny pokrok na všetkých úrovniach spoločnosti smerom k tzv. prístupu orientovanému na kybernetickú bezpečnosť.

5.9. EHSV sa domnieva, že je nevyhnutné posudzovať rizikový profil dodávateľov a na tých, ktorí sa posúdia ako vysokorizikoví, uplatňovať príslušné obmedzenia vrátane vylúčení potrebných v súvislosti s kľúčovými aktívami a aplikáciami, ktoré sa v rámci koordinovaného hodnotenia rizika na úrovni EÚ vymedzia ako kriticky dôležité a citlivé, ako aj certifikácie dôveryhodných poskytovateľov hardvéru a softvéru.

6. **Uzatváranie partnerstiev na riešenie spoločných výziev**

6.1. Úroveň pripravenosti na budúce kybernetické útoky sa v jednotlivých členských štátoch značne líši. EHSV sa domnieva, že prvým okamžitým krokom je vytvorenie komunikačnej platformy pre najlepšie postupy v rámci EÚ, kde by sa najpokročilejšie členské štáty mohli podeliť o svoje poznatky a uľahčiť tak ich okamžité prevzatie ostatnými krajinami. To by pomohlo zlepšiť vzájomnú dôveru medzi vnútroštátnymi subjektmi. Po druhé, výbor sa domnieva, že na zlepšenie kybernetickej bezpečnosti produktov a služieb na vnútornom trhu je potrebná intenzívnejšia spolupráca medzi štátnymi a neštátnymi subjektmi v celej EÚ. EHSV takisto navrhuje vytvoriť spoločnú platformu EÚ na nahlasovanie kybernetických incidentov vrátane európskej čiernej listiny všetkých aktivistov v oblasti kybernetickej trestnej činnosti.

([5]) Napríklad Gaia-X, francúzsko-nemecká iniciatíva.

6.2. EHSV zastáva názor, že intenzívna spolupráca s našimi spojencami z NATO vo vojenskej oblasti sa musí zamerať nielen na budovanie spôsobilostí a včasné odhaľovanie hrozieb, ale aj na spoločné projekty v oblasti výskumu, vývoja a inovácií, výmenu najlepších postupov a odborníkov, rozsiahle programy odbornej prípravy a simulácie kybernetických útokov. Hlavným cieľom by malo byť rozšírenie spoločnej spôsobilosti rýchlej reakcie a vytvorenie synergií v boji proti budúcim hybridným hrozbám v nadväznosti na spoločné vyhlásenia z Varšavy z roku 2016 a z Bruselu z roku 2018. Spolupráca medzi EÚ a NATO ponúka ešte stále veľa možností, ktoré možno využiť, a okamžitý pokrok môže priniesť skutočnú zmenu z hľadiska zaistenia bezpečnosti pre našich občanov a spoločnosť.

6.3. Výbor sa domnieva, že rokovaniami na celosvetovej úrovni a s našimi medzinárodnými partnermi by sa mali vytvoriť podmienky na podporu globálneho a otvoreného kybernetického priestoru, v ktorom sa zabezpečí ochrana ľudských práv, základných slobôd a právneho štátu so zameraním na vypracovanie záväzných medzinárodných noriem v odvetviach s rýchlym digitálnym rozvojom. EHSV odporúča vysokému predstaviteľovi, aby preskúmal existujúce dvojstranné kybernetické dialógy a zapojil sa do ďalších rokovaní s inými krajinami a príslušnými medzinárodnými organizáciami s cieľom podporiť globálny rámec pre uplatňovanie medzinárodného práva v kybernetickom priestore založený na prísnej podmienke reciprocity.

6.4. Napokon sa výbor domnieva, že EÚ má najlepšie predpoklady na to, aby viedla medzinárodné rokovania o budúcnosti kybernetickej bezpečnosti, najmä v rámci OSN, a to vďaka svojmu pevnému základu v oblasti základných demokratických slobôd. EÚ sa takisto musí zapojiť do boja proti totalitným režimom, ktoré monitorujú údaje občanov a porušujú tak ich práva a slobody, a mala by sa dôrazne postaviť proti akémukoľvek systému sociálneho bodovania občanov. EHSV jasne konštatuje, že skutočná demokracia nemôže existovať bez efektívnej ochrany osobných údajov, a domnieva sa, že na to, aby sa hyperkonektivita stala prínosom, je nevyhnutná zodpovedná a účinná správa údajov.

V Bruseli 14. júna 2023

Predseda
Európskeho hospodárskeho a sociálneho výboru
Oliver RÖPKE