Rada
Európskej únie

V Bruseli 22. mája 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Komu:	Delegácie
Č. predch. dok.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Predmet:	Závery Rady o politike EÚ v oblasti kybernetickej obrany

Delegáciám v prílohe zasielame závery Rady o politike EÚ v oblasti kybernetickej obrany v znení, ktoré schválila Rada na zasadnutí 22. mája 2023.

Závery Rady o politike EÚ v oblasti kybernetickej obrany

1. Rada v nadväznosti na politický rámec pre kybernetickú obranu z roku 2014 a jeho aktualizáciu v roku 2018 víta ambiciózne spoločné oznámenie o politike EÚ v oblasti kybernetickej obrany zamerané na ďalšie investovanie do našich moderných a interoperabilných ozbrojených síl, špičkových technológií, najmodernejších spôsobilostí v oblasti kybernetickej obrany a posilnenie partnerstiev na riešenie spoločných výziev. Kybernetický priestor sa v čase rastúcej závislosti od digitálnych technológií stal oblasťou strategického súperenia. Preto je nevyhnutné zachovať otvorený, slobodný, stabilný a bezpečný kybernetický priestor. Využívanie kybernetických operácií, ktoré umožňujú a sprevádzajú nevyprovokovanú a neodôvodnenú útočnú vojnu Ruska voči Ukrajine, ovplyvňuje globálnu stabilitu a bezpečnosť, predstavuje významné riziko eskalácie a prispieva k už aj tak výraznému nárastu škodlivých kybernetických činností mimo kontextu ozbrojeného konfliktu v posledných rokoch.

2. Vojna na Ukrajine poskytla nový strategický kontext a potvrdila, že je potrebné, aby EÚ, jej členské štáty a ich partneri ďalej posilňovali odolnosť EÚ voči kybernetickým hrozbám a zvýšili našu spoločnú kybernetickú bezpečnosť a kybernetickú obranu proti zlovoľnému správaniu a aktom agresie v kybernetickom priestore. Spoločné oznámenie o politike EÚ v oblasti kybernetickej obrany vyjadruje naše odhodlanie prijať okamžité a dlhodobé opatrenia na zabezpečenie slobody konania v kybernetickom priestore a reakcie voči aktérom hrozieb, ktorí sa okrem iného snažia vniknúť do sietí a informačných systémov EÚ a jej partnerov, narušiť ich alebo zničiť. Toto spoločné oznámenie, ktoré dopĺňa stratégiu kybernetickej bezpečnosti EÚ a je v súlade so Strategickým kompasom, predstavuje významný krok smerom k celospektrálnemu prístupu EÚ k odolnosti, reakcii, predchádzaniu konfliktom, spolupráci a stabilite v kybernetickom priestore. Rada v tejto súvislosti zdôrazňuje potrebu vhodných a súdržných reakcií zo strany EÚ, jej členských štátov a ich partnerov, pričom tiež so záujmom očakáva revíziu vykonávacích usmernení súboru nástrojov kybernetickej diplomacie EÚ ako ďalší kľúčový krok vo vývoji stavu kybernetickej bezpečnosti v EÚ.

3. Rada zdôrazňuje, že nedávne kybernetické útoky na európsku kritickú infraštruktúru, rýchlo sa vyvíjajúca panoráma kybernetických hrozieb a rýchle tempo technického rozvoja tiež poukazujú na potrebu posilnenej civilno-vojenskej koordinácie a spolupráce, pričom podčiarkuje, že medzi civilnými a vojenskými komunitami neexistuje hierarchia. Politika EÚ v oblasti kybernetickej obrany umožňuje EÚ a jej členským štátom posilniť ich schopnosť chrániť, odhaľovať, brániť a odrádzať a pritom primerane využívať celú škálu obranných možností, ktoré majú civilné a vojenské komunity k dispozícii na širšiu bezpečnosť a obranu EÚ, v súlade s medzinárodným právom vrátane práva v oblasti ľudských práv a medzinárodného humanitárneho práva.

4. Národná bezpečnosť, a to aj v kybernetickej oblasti, síce ostáva vo výlučnej zodpovednosti každého členského štátu, ako sa uvádza v článku 4 ods. 2 Zmluvy o EÚ, Rada však zdôrazňuje, že je potrebné jednotlivo aj spoločne výrazne investovať do zvýšenej odolnosti a zavádzania celospektrálnych obranných spôsobilostí v oblasti kybernetickej obrany a do využívania rámcov spolupráce EÚ a finančných stimulov. Rada zdôrazňuje potrebu ďalšieho posilnenia opatrení členských štátov a inštitúcií, orgánov a agentúr EÚ s cieľom chrániť Úniu, našich občanov, inštitúcie, orgány a agentúry EÚ, ako aj misie a operácie SBOP v kybernetickom priestore. Okrem toho zdôrazňuje dôležitosť odolnosti EÚ v kybernetickom priestore prostredníctvom rozvoja spôsobilostí v oblasti kybernetickej obrany a posilnenia spolupráce s dôveryhodným súkromným ekosystémom.

I. **Spoločne sa pričiniť o silnejšiu kybernetickú obranu**

5. Rada opätovne zdôrazňuje, že na posilnenie dôvery, ktorá má zásadný význam pre ďalší rozvoj rámca EÚ pre krízové riadenie kybernetickej bezpečnosti, je nevyhnutný postupný, transparentný a inkluzívny proces, ktorý sa má uskutočniť v súlade s plánom riadenia kybernetických kríz vypracovaným v Rade. Rada opätovne zdôrazňuje potrebu ďalej posilňovať našu schopnosť chrániť, odhaľovať, brániť a odrádzať od kybernetických útokov prostredníctvom lepšieho situačného povedomia, budovania kapacít, výcviku, cvičení a zvýšenej odolnosti a rozhodnou reakciou na kybernetické útoky proti Únii, jej členským štátom, inštitúciám, orgánom a agentúram EÚ a misiám a operáciám SBOP za použitia všetkých primeraných prostriedkov. Rada pritom nabáda vysokého predstaviteľa a Komisiu, aby znížili zložitosť v oblasti kybernetickej bezpečnosti, vyhli sa zbytočnej duplicite a zabezpečili spoluprácu a synergie s existujúcimi iniciatívami. Je potrebné posilniť spoluprácu a koordináciu medzi aktérmi kybernetickej obrany v rámci EÚ a členských štátov, ako aj medzi vojenskými a civilnými kybernetickými komunitami a medzi verejným a dôveryhodným súkromným ekosystémom. V tejto súvislosti sa členské štáty vyzývajú, aby ďalej skúmali a posilňovali civilno-vojenské vnútroštátne koordinačné mechanizmy, uľahčovali spoločnú dobrovoľnú výmenu informácií, vymieňali si získané poznatky, prispievali k rozvoju interoperabilných noriem, vykonávali hodnotenia rizík a vypracúvali scenáre rizík, ako aj spoločné cvičenia, najmä na európskej úrovni, pri plnom dodržiavaní ustanovení smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS 2).

6. Rada berie na vedomie úsilie o ďalšie posilnenie odolnosti Únie prostredníctvom smernice NIS 2 a smernice o odolnosti kritických subjektov (CER) a opakuje svoje odporúčanie týkajúce sa celoeurópskeho koordinovaného prístupu k posilneniu odolnosti kritickej infraštruktúry[1]. Vyzýva na prijatie opatrení na ďalšie posilnenie odolnosti kritických subjektov, infraštruktúry, digitálnych produktov a služieb, pričom poznamenáva, že najdôležitejším krokom zostáva riadne vykonávanie smernice NIS 2. Hoci ide prevažne o civilnú zodpovednosť, aj táto prispieva k silnejšej kybernetickej obrane. V tejto súvislosti sa inštitúcie, orgány a agentúry EÚ, ako aj členské štáty nabádajú, aby podporovali ďalší rozvoj a zavádzanie nových a existujúcich koordinačných mechanizmov EÚ, posúdení rizík, hodnotení a scenárov, spoločnej dobrovoľnej výmeny informácií a cvičení spôsobom, ktorý prináša pridanú hodnotu a zabraňuje zbytočnej duplicite s existujúcimi iniciatívami.

7. S cieľom ďalej posilniť dôveru, upevniť spoluprácu a uľahčiť včasnú výmenu informácií o významných a rozsiahlych kybernetických incidentoch, ktoré majú vplyv na obranné systémy, Rada víta iniciatívu na ďalšie rozpracovanie konferencie veliteľov EÚ v oblasti kybernetickej bezpečnosti, ktorú má organizovať každé predsedníctvo Rady EÚ s podporou Európskej obrannej agentúry (EDA) a za účasti Európskej služby pre vonkajšiu činnosť (ESVČ). Rada nabáda všetky členské štáty, aby sa na týchto zasadnutiach zúčastňovali. S cieľom posilniť odolnosť EÚ voči rozsiahlym kyberneticko-bezpečnostným incidentom Rada vyzýva sieť styčných organizácií EÚ pre kybernetické krízy (EU-CyCLONe) a konferenciu veliteľov EÚ v oblasti kybernetickej bezpečnosti, aby identifikovali možné spôsoby spolupráce a využitia spoločnej vojenskej a civilnej perspektívy.

---

[1] Návrh odporúčania Rady týkajúceho sa koordinovaného prístupu Únie k posilneniu odolnosti kritickej infraštruktúry, COM/2022/551.

8. S cieľom podporiť spoľahlivejšiu a koordinovanejšiu reakciu na úrovni EÚ Rada víta zriadenie operačnej siete pre vojenské tímy reakcie na počítačové núdzové situácie (MICNET) v záujme zlepšenia výmeny technických informácií o kybernetických incidentoch ovplyvňujúcich obranné systémy medzi zúčastnenými členskými štátmi a očakáva, že sa do polovice roka 2024 dosiahne jej počiatočná operačná spôsobilosť. Rada nabáda všetky členské štáty, aby sa zapojili do siete MICNET s cieľom zabezpečiť jej účinnosť. Rada okrem toho vyzýva členské štáty, aby vychádzali z poznatkov získaných zo siete jednotiek pre riešenie počítačových bezpečnostných incidentov (CSIRT), a dôrazne nabáda na vytvorenie účinného mechanizmu spolupráce a koordinácie medzi týmito dvoma sieťami vo vhodnom čase pri plnom rešpektovaní riadiacich mechanizmov a zložiek každého subjektu.

9. Vzhľadom na nárast škodlivých kybernetických činností zo strany štátnych a neštátnych subjektov zameraných na misie a operácie EÚ v rámci SBOP Rada vyzýva EÚ a jej členské štáty, aby posilnili svoje spôsobilosti na obranu a zabezpečenie misií a operácií SBOP. Rada v tejto súvislosti víta ciele ďalej napredovať v ochrane vojenských sietí a štruktúr EÚ, okrem iného v súlade s vojenskou víziou a stratégiou EÚ pre kybernetický priestor ako operačnú oblasť[2].

[2] ESVČ(2021) 706 REV 4.

10. Rada opätovne pripomína závery Rady z mája 2022[3] a potrebu investovať do našej vzájomnej pomoci podľa článku 42 ods. 7 ZEÚ, ako aj doložky o solidarite podľa článku 222 ZFEÚ. Rada zdôrazňuje význam ďalšieho prehlbovania jednotného chápania vykonávania článku 42 ods. 7 zo strany EÚ a jej členských štátov, a to aj v rámci zložitých scenárov zahŕňajúcich kybernetický útok, v súlade s príslušnými zásadami medzinárodného práva. Víta možnosť podpory zo strany EÚ v prípade kybernetického útoku na výslovnú žiadosť dotknutých členských štátov, a to bez toho, aby bola dotknutá osobitná povaha bezpečnostnej a obrannej politiky niektorých členských štátov.

11. Rada zdôrazňuje pokrok dosiahnutý v projekte PESCO s názvom tímy rýchlej kybernetickej reakcie a vzájomnej pomoci v oblasti kybernetickej bezpečnosti (CRRT) a svoju pripravenosť konať na požiadanie ako spôsobilosť pre potreby členských štátov a EÚ na podporu misií a operácií SBOP a poskytovať pomoc partnerom EÚ. Rada víta ďalší rozvoj spôsobilosti PESCO CRRT, národných tímov kybernetickej reakcie a prípadne ďalších spôsobilostí reakcie na incidenty, ako sú budúce tímy rýchlej reakcie na hybridné hrozby, ako sa predpokladá v Strategickom kompase, a to aj prostredníctvom podpory ich koordinácie a spolupráce na úrovni EÚ.

[3] Závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, 23. mája 2022, 9364/22.

12. Rada víta činnosť v rámci projektu PESCO s názvom Koordinačné centrum pre kybernetickú a informačnú oblasť (CIDCC), ktorého cieľom je poskytnúť vojenskú spôsobilosť na zhromažďovanie a analýzu informácií relevantných pre spoločný operačný obraz o situácii v oblasti kybernetických hrozieb. Rada ďalej víta návrh na začlenenie overenia koncepcie, ak bude úspešné ako centrum na koordináciu informácií, od roku 2025 do Koordinačného centra kybernetickej obrany EÚ (EUCDCC), čím sa zlepší koordinácia a situačné povedomie, najmä pokiaľ ide o veliteľov misií a operácií EÚ v rámci SBOP, a posilní širšia štruktúra EÚ pre velenie a riadenie. Rada vyzýva vysokého predstaviteľa, aby predložil koncepciu a plán na zriadenie EUCDCC, v ktorej by čerpal ponaučenia z podobných medzinárodných subjektov, identifikoval potrebné zdroje, bránil zbytočnej duplicite a usiloval sa o komplementárnosť so širším rámcom kybernetickej bezpečnosti EÚ.

13. Rada zdôrazňuje význam strategickej spravodajskej spolupráce v oblasti kybernetických hrozieb a činností a vyzýva členské štáty, aby prostredníctvom svojich príslušných orgánov naďalej prispievali k práci Spravodajského a situačného centra EÚ (EU INTCEN), riaditeľstva spravodajskej služby VŠEÚ a členských štátov v rámci jednotnej kapacity na analýzu spravodajských informácií (SIAC). Rada ďalej zdôrazňuje, že je dôležité posilniť naše kapacity v oblasti kybernetického spravodajstva s cieľom zvýšiť našu kybernetickú odolnosť a reakcie a poskytovať účinnú podporu našim civilným a vojenským misiám a operáciám SBOP, ako aj našim ozbrojeným silám a kapacitám SIAC v kybernetickej oblasti, a to na základe dobrovoľných spravodajských príspevkov členských štátov a bez toho, aby boli dotknuté ich právomoci.

14. Rada berie na vedomie situačné a analytické centrum Európskej komisie pre kybernetický priestor, ktorého cieľom je zvýšiť situačné povedomie Komisie. Rada zdôrazňuje význam nadviazania vzájomne prospešnej spolupráce medzi týmto centrom a ostatnými inštitúciami, orgánmi a agentúrami EÚ, najmä agentúrou ENISA a tímom CERT-EU. Rada zdôrazňuje, že pri vytváraní situačného povedomia je dôležité zabezpečiť úzku spoluprácu so sieťami spolupráce EÚ, ako aj rešpektovať dôvernosť. Rada konštatuje, že je potrebné posilniť spoločné situačné povedomie na úrovni EÚ a ďalej rozvíjať rámec EÚ pre krízové riadenie kybernetickej bezpečnosti, pričom je potrebné vyhnúť sa zbytočnej duplicite úsilia.

15. Rada pripomína, že vzdelávanie, odborná príprava a cvičenia v oblasti kybernetickej bezpečnosti sú nevyhnutné na zabezpečenie pripravenosti a účinnosti, a víta vnútroštátne činnosti, ako aj činnosti, ktoré zabezpečuje EÚ prostredníctvom Európskej akadémie bezpečnosti a obrany (EABO), agentúr EDA a ENISA a prebiehajúcich projektov PESCO, ako sú Združenie národných kybernetických polygónov a Akademické a inovačné centrum EÚ pre kybernetickú oblasť (CAIH). Rada s cieľom ďalšieho posilnenia tohto úsilia so záujmom očakáva vytvorenie rámcového projektu EDA CyDef-X na synchronizáciu a podporu cvičení v oblasti kybernetickej obrany. Rada nabáda agentúru EDA, aby v úzkej spolupráci s členskými štátmi a ESVČ preskúmala, ako by CyDef-X mohol ďalej podporovať cvičenia, ako je CYBER PHALANX, a to aj pokiaľ ide o vzájomnú pomoc podľa článku 42 ods. 7 ZEÚ a doložku o solidarite podľa článku 222 ZFEÚ, ako aj s Komisiou a agentúrou ENISA, pokiaľ ide o civilné cvičenia. Rada okrem toho nabáda na využívanie a ďalší rozvoj existujúcich prostredí testovania a cvičení v oblasti kybernetickej obrany v rámci CyDef-X, ako je napríklad Združenie národných kybernetických polygónov. S cieľom zabezpečiť pružný a efektívny rozhodovací proces v súvislosti s kybernetickou krízou Rada zdôrazňuje, že je dôležité organizovať pravidelné simulačné cvičenia na úrovni rozhodovania členských štátov.

16. Rada berie na vedomie návrh aktu o kybernetickej solidarite a zámer posilniť spôsobilosti na odhaľovanie kyberneticko-bezpečnostných hrozieb a incidentov v EÚ a reakcie na ne. Rada zdôrazňuje, že návrhy v tejto oblasti môžu byť účinné len vtedy, ak sú v súlade s rámcami krízového riadenia členských štátov a ich potrebami. Rada zdôrazňuje význam testovania kritickej infraštruktúry na potenciálne zraniteľné miesta v prípadoch, v ktorých sa to považuje za prospešné, ako vnútroštátnej právomoci, pričom sa zohľadnia dostupné posúdenia rizík EÚ.

17. Rada berie na vedomie návrh Komisie zriadiť núdzový kybernetický mechanizmus, ktorý by mohol podporiť dostupnosť služieb kybernetickej bezpečnosti od dôveryhodných súkromných poskytovateľov, aby na požiadanie pomáhali členským štátom v prípade rozsiahlych kybernetických incidentov, pričom zdôrazňuje potrebu rozšíriť európske odvetvie kybernetickej bezpečnosti s podporou Európskeho centra kompetencií pre kybernetickú bezpečnosť (ECCC) ako základného piliera pre fungovanie tohto mechanizmu. Rada zdôrazňuje kľúčovú úlohu každého členského štátu pri monitorovaní a posudzovaní jeho vnútroštátnych potrieb.

II. **Zabezpečenie obranného ekosystému EÚ**

18. Rada pripomína svoju podporu členským štátom, aby ďalej rozvíjali svoje vlastné spôsobilosti na vykonávanie operácií kybernetickej obrany vrátane prípadných proaktívnych obranných opatrení na ochranu a obranu pred kybernetickými útokmi, ich odhaľovanie a odrádzanie od nich. Vzhľadom na to, že smernica NIS 2 sa nevzťahuje na subjekty verejnej správy, ktoré vykonávajú svoje činnosti v oblasti obrany, Rada vyzýva agentúru EDA, aby s prípadnou podporou Komisie a ESVČ pomáhala členským štátom pri vypracúvaní právne nezáväzných dobrovoľných odporúčaní inšpirovaných smernicou NIS 2 s cieľom zvýšiť kybernetickú bezpečnosť v obrannom spoločenstve, a vyzýva všetky členské štáty, aby sa aktívne zapojili do tohto úsilia. Tieto odporúčania by mali zohľadňovať podobné úsilie vyvíjané v iných rámcoch.

19. Ako sa uznáva v Strategickom kompase, schopnosť EÚ konať závisí od jej schopnosti znížiť svoju strategickú závislosť v rámci svojich spôsobilostí v oblasti kybernetickej obrany a dodávateľských reťazcov, ako aj od jej schopnosti vyvíjať a dokonale zvládať špičkové technológie v oblasti kybernetickej obrany. To zahŕňa posilnenie európskej obrannej technologickej a priemyselnej základne (EDTIB) v celej EÚ a jej schopnosti spolupracovať s podobne zmýšľajúcimi partnermi na celom svete na recipročnom základe s cieľom zabezpečiť vzájomné výhody. Rada preto vyzýva, aby odvetvia kybernetickej bezpečnosti a kybernetickej obrany úzko spolupracovali v záujme vytvárania synergií s cieľom rozvíjať a poskytovať celospektrálne spôsobilosti v oblasti kybernetickej obrany. Rada vyzýva Komisiu, aby v prípadnej úzkej spolupráci s ECCC ďalej podporovala rozvoj silnej, pružnej, celosvetovo konkurencieschopnej a inovačnej európskej priemyselnej a technologickej základne v oblasti kybernetickej obrany vrátane malých a stredných podnikov (MSP) prostredníctvom ďalších investícií a politických opatrení.

20. Vzhľadom na význam interoperability a spoločného charakteru spôsobilostí v oblasti kybernetickej obrany, a to aj pokiaľ ide o spoluprácu pri rozvoji spôsobilostí novej generácie v oblasti kybernetickej obrany, Rada vyzýva agentúru EDA a Vojenský štáb EÚ, aby pracovali na súbore požiadaviek EÚ na interoperabilitu v oblasti kybernetickej obrany, ktoré by vychádzali z existujúcich zásad, procesov a noriem stanovených najmä v rámci Organizácie Severoatlantickej zmluvy (NATO) a boli by s nimi zlučiteľné. Rada okrem toho vyzýva členské štáty, aby v rámci Európskeho výboru pre normalizáciu v oblasti obrany preskúmali, či by sa mohli vyžadovať osobitné dobrovoľné normy pre obranné systémy, a to v úzkej spolupráci so všetkými príslušnými zainteresovanými stranami, podľa potreby vrátane európskych normalizačných organizácií a NATO.

21. Rada víta úsilie Komisie predložiť plán na podporu využívania existujúcich noriem v oblasti civilnej kybernetickej bezpečnosti a kybernetickej obrany, ako aj vypracovania nových dobrovoľných noriem. Rada zdôrazňuje, že je potrebné zosúladiť normy kybernetickej bezpečnosti a kybernetickej obrany tam, kde je to vhodné. Rada uznáva, že takéto dobrovoľné normy by mohli byť užitočné pre odvetvia kybernetickej bezpečnosti a kybernetickej obrany EÚ, a naliehavo vyzýva na užšiu spoluprácu medzi civilnými a obrannými normalizačnými orgánmi.

22. Rada vyzýva, aby sa urýchlene vypracovali odporúčania založené na mapovaní existujúcich nástrojov bezpečnej komunikácie v kybernetickej oblasti, ktoré má vykonať Komisia a príslušné inštitúcie. Tieto odporúčania by sa mali podľa možnosti zosúladiť s existujúcimi iniciatívami v oblasti výmeny informácií a mali by sa v nich zohľadniť aj riziká, ktoré pre súčasné metódy šifrovania predstavujú vznikajúce a prelomové technológie.

23. Rada okrem toho víta počiatočnú prácu na hodnotení rizík a na scenároch, ktoré na žiadosť Rady vypracúvajú Komisia, vysoký predstaviteľ a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, a to najprv v súvislosti s odvetviami energetiky a telekomunikácií. Rada potvrdzuje, že sa pripravujú aj cielené posúdenia kyberneticko-bezpečnostných rizík pre komunikačnú infraštruktúru a siete v EÚ. Rada opätovne zdôrazňuje, že je mimoriadne dôležité, aby sa medzi členskými štátmi, ale aj inštitúciami, orgánmi a agentúrami EÚ vytvorilo spoločné chápanie možných vplyvov kybernetických incidentov. Rada preto vyzýva uvedených aktérov, aby zabezpečili, že sa pri vymedzovaní a určovaní priorít opatrení a podpory na úrovni EÚ a prípadne na vnútroštátnej úrovni zohľadnia hodnotenia rizík, scenáre a následné odporúčania. Rada okrem toho vyzýva, aby všetci príslušní aktéri zvážili scenáre rizík v rámci procesov posudzovania rizík, ako aj pri vývoji kybernetických cvičení.

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

24. Rada nabáda členské štáty, aby zvýšili svoje investície do budovania, udržiavania a ďalšieho rozvoja interoperabilných spôsobilostí v oblasti kybernetickej obrany. Rada podporuje vypracovanie súboru dobrovoľných záväzkov pre ďalší rozvoj vnútroštátnych spôsobilostí v oblasti kybernetickej obrany, pričom berie do úvahy podobné úsilie vyvíjané v iných rámcoch.

25. Rada vyzýva členské štáty a agentúru EDA, aby využili príležitosť revízie plánu rozvoja spôsobilostí na stanovenie vysokej úrovne ambícií, pokiaľ ide o rozvoj spolupráce v oblasti kybernetickej obrany na úrovni EÚ. Rada ďalej nabáda členské štáty, aby vychádzali z aktualizovaného súboru priorít a zo svojich záväzkov v rámci PESCO zvýšiť svoju úroveň zapojenia do spoločných projektov rozvoja spôsobilostí EÚ v oblasti kybernetickej obrany, pričom uznáva priamy prínos spoločných projektov na úrovni EÚ pre podporu rozvoja vnútroštátnych spôsobilostí v oblasti kybernetickej obrany.

26. Rada víta spoločné výskumné úsilie na úrovni EÚ zamerané na preskúmanie možných aplikácií v rámci vznikajúcich a prelomových technológií v systémoch súvisiacich s obranou, pričom tiež konštatuje, že je potrebné zabezpečiť, aby sa tento technologický vývoj rýchlo začlenil do existujúcich a budúcich spôsobilostí. Rada nabáda členské štáty a priemysel EÚ, aby čo najlepšie využívali možnosti spolupráce v oblasti výskumu na úrovni EÚ, napríklad v rámci agentúry EDA, prebiehajúce projekty PESCO, ako je Akademické a inovačné centrum EÚ pre kybernetickú oblasť (CAIH EÚ), Európsky obranný fond a prípadne Horizont Európa a program Digitálna Európa pre projekty s dvojakým použitím. Rada okrem toho víta využívanie špecializovaných rámcov na podporu inovácií v oblasti obrany s využitím produktov spin-in z civilnej oblasti, najmä programu EÚ pre inovácie v oblasti obrany a centra pre inovácie v oblasti európskej obrany. Rada okrem toho nabáda Európske centrum kompetencií v oblasti kybernetickej bezpečnosti (ECCC) a agentúru EDA, aby vypracovali pracovné dojednanie s cieľom uľahčiť výmenu informácií medzi ich zamestnancami o civilných prioritách, prioritách v oblasti technológií dvojakého použitia a prioritách v oblasti obranných technológií s cieľom vytvoriť synergie a zabrániť duplicite.

27. Rada víta zámer Komisie vypracovať technologický plán pre kritické kybernetické technológie v spolupráci s agentúrou EDA a ECCC v súlade s ich príslušnými mandátmi, s členskými štátmi a po konzultácii s príslušnými zainteresovanými stranami, ako je priemysel, ktorý prostredníctvom identifikácie kritických kybernetických technológií, mapovania technologického vývoja a strategických závislostí stanovuje spôsoby, ako ich znížiť, a to v záujme podpory strategickej autonómie a technologickej suverenity EÚ, pričom sa zachová otvorené hospodárstvo. Rada konštatuje, že technologický plán pre kritické kybernetické technológie môže poskytovať strategické priority pre nástroje financovania EÚ, pričom bude zároveň v súlade s príslušnými postupmi, ktoré sú pre ne zavedené. Rada pripomína, že EÚ by sa mala usilovať o ambicióznu a asertívnu európsku priemyselnú politiku s cieľom vytvoriť udržateľné, atraktívne a konkurencieschopné podnikateľské prostredie, ktoré môže tiež umožniť posilnenie európskych subjektov v kybernetickej oblasti.

28. Rada oceňuje zámer riešiť významný nedostatok zručností v oblasti kybernetickej bezpečnosti prilákaním nových odborníkov vrátane žien, zvyšovaním úrovne zručností a rekvalifikáciou, ako aj investovaním do odbornej prípravy a cvičení a ich organizovaním s cieľom vytvoriť rozmanitú a inkluzívnu pracovnú silu v oblasti kybernetickej bezpečnosti. Rada uznáva výzvy, ktorým EÚ čelí v súvislosti s ľudským kapitálom v oblasti kybernetickej bezpečnosti a kybernetickej obrany, a víta iniciatívu na zriadenie Akadémie kyberneticko-bezpečnostných zručností, ktorá môže byť prínosom aj pre pracovnú silu v oblasti kybernetickej obrany.

29. Rada vyzýva členské štáty, aby si vymieňali informácie o najlepších postupoch na vyškolenie kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti s využitím synergií medzi vojenskými a civilnými iniciatívami a iniciatívami v oblasti presadzovania práva, a vyzýva akadémiu EABO, aby s podporou agentúr EDA a ENISA a využívajúc ich odborné znalosti zvážila možnosti posilnenia výmeny najlepších postupov a ďalších synergií medzi vojenskou a civilnou oblasťou, pokiaľ ide o odbornú prípravu a rozvoj zručností v oblasti kybernetickej obrany.

30. Rada zdôrazňuje význam spoločného chápania zloženia pracovnej sily v oblasti kybernetickej bezpečnosti a súvisiacich zručností s cieľom identifikovať a riešiť nedostatky na trhu práce v oblasti kybernetickej bezpečnosti, ako aj potrebu zapojiť všetky zainteresované strany vrátane členských štátov a priemyslu. Rada uznáva, že stanovenie ukazovateľov na monitorovanie trhu práce v oblasti kybernetickej bezpečnosti by pomohlo identifikovať potreby kyberneticko-bezpečnostných zručností a primerane nasmerovať finančné prostriedky a zároveň by prispelo k plneniu politických záväzkov, najmä tých, ktoré vyplývajú zo smernice NIS 2. Rada víta návrh na vytvorenie rámca certifikácie zručností v oblasti kybernetickej obrany a vyzýva vysokého predstaviteľa, aby z titulu svojej funkcie vedúceho akadémie EABO tento rámec vypracoval v spolupráci s ESVČ, Komisiou a členskými štátmi a s využitím civilných iniciatív.

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

31. Rada vyzýva vysokého predstaviteľa a Komisiu, aby posilnili spoluprácu a pokročili v nej a aby preskúmali vzájomne prospešné a prispôsobené partnerstvá v oblasti politík kybernetickej obrany vrátane budovania kapacít v oblasti kybernetickej obrany prostredníctvom Európskeho mierového nástroja (EPF). Na tento účel by sa mala kybernetická obrana pridať ako bod v rámci dialógov a konzultácií EÚ o kybernetickej bezpečnosti a celkových konzultácií o bezpečnosti a obrane s partnermi. Okrem toho by sa mali posilniť dialógy a spolupráca so súkromným sektorom. Rada zdôrazňuje, že medzinárodná spolupráca v oblasti noriem kybernetickej bezpečnosti a certifikácie by bola pre európsky priemysel pridanou hodnotou. Preto víta záväzok Komisie, aby sa tento proces stal zásadnou súčasťou dialógov EÚ s tretími krajinami a medzinárodnými organizáciami o kybernetickej bezpečnosti.

32. Rada zdôrazňuje význam medzinárodnej spolupráce pri predchádzaní alebo znižovaní rizík konfliktov v kybernetickom priestore, najmä prostredníctvom ďalšieho rozvoja a uplatňovania opatrení na budovanie dôvery (CBM) na regionálnej a medzinárodnej úrovni vrátane OSN a ďalšej podpory využívania existujúcich kybernetických CBM, ako je to v rámci Organizácie pre bezpečnosť a spoluprácu v Európe (OBSE), a to aj v čase medzinárodného napätia. EÚ a jej členské štáty zdôrazňujú, že v kybernetickom priestore platí existujúce medzinárodné právo a že je dôležité pokračovať v úsilí o zachovanie a podporu rámca OSN pre zodpovedné správanie štátov a usilovať sa o jeho vykonávanie, a to aj prostredníctvom vytvorenia akčného programu na posilňovanie zodpovedného správania štátov v kybernetickom priestore.

33. Rada v súlade so spoločnými vyhláseniami o spolupráci medzi EÚ a NATO vyzýva Komisiu a vysokého predstaviteľa, aby aj z titulu svojej funkcie vedúceho agentúry EDA ďalej posilňovali, prehlbovali a rozširovali partnerstvo v kybernetickej oblasti s NATO pri plnom rešpektovaní zásad inkluzívnosti, reciprocity, vzájomnej otvorenosti a transparentnosti, ako aj autonómie rozhodovania oboch organizácií. Rada s ohľadom na potrebu zabezpečiť doplnkové a koordinované úsilie s čo najväčším zapojením členských štátov, ktoré nie sú súčasťou NATO, a zabrániť zbytočnej duplicite vyzýva na vytvorenie prepojení na príslušných úrovniach medzi EÚ a NATO v oblasti odbornej prípravy, vzdelávania, situačného povedomia, cvičení a platforiem výskumu a vývoja a na hľadanie potenciálnych synergií medzi príslušnými dobrovoľnými záväzkami zameranými na vytvorenie rámca vnútroštátnych spôsobilostí v oblasti kybernetickej obrany a rámca krízového riadenia, na ochranu kritickej infraštruktúry a zlepšenie výmeny situačného povedomia, koordinované reakcie na škodlivé kybernetické činnosti, ako aj na úsilie o budovanie kapacít v tretích krajinách. Súčasťou toho je technická dohoda medzi spôsobilosťou NATO pre reakciu na počítačové incidenty (NCIRC) a tímom reakcie na núdzové počítačové situácie v EÚ (CERT-EU), ako aj posilnený politický dialóg o otázkach kybernetickej obrany na všetkých úrovniach.

V. **Záver**

34. Rada na základe záverov Rady o politike EÚ v oblasti kybernetickej obrany vyzýva vysokého predstaviteľa a Komisiu, aby do druhého štvrťroka 2023 vypracovali plán vykonávania tejto politiky, ktorý majú schváliť členské štáty. Rada tiež vyzýva členské štáty, aby dobrovoľne uviedli svoje ambície a opatrenia v oblasti kybernetickej obrany v kontexte politiky EÚ v oblasti kybernetickej obrany a v plnej miere využívali právne nezáväzné dobrovoľné odporúčania a záväzky na zintenzívnenie svojho vnútroštátneho a nadnárodného úsilia v oblasti kybernetickej obrany s cieľom maximalizovať vplyv na úrovni EÚ. Vysoký predstaviteľ, Komisia a členské štáty sa vyzývajú, aby počnúc druhým štvrťrokom 2024 každoročne predkladali správy a diskutovali o pokroku pri vykonávaní prvkov spoločného oznámenia a jeho plánu vykonávania.