Rada
Evropské unie

Brusel 22. května 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

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Příjemce:	Delegace
Č. předchozího dokumentu:	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
Předmět:	Závěry Rady o politice EU pro kybernetickou obranu

Delegace naleznou v příloze závěry Rady o politice EU pro kybernetickou obranu, které schválila Rada na zasedání dne 22. května 2023.

Závěry Rady o politice EU pro kybernetickou obranu

1. V návaznosti na politický rámec pro kybernetickou obranu z roku 2014 a jeho aktualizaci v roce 2018 Rada vítá ambiciózní společné sdělení Politika kybernetické obrany EU s cílem dále investovat do našich moderních a interoperabilních ozbrojených sil, špičkových technologií, nejmodernějších schopností kybernetické obrany a posílit partnerství pro řešení společných výzev. V době rostoucí závislosti na digitálních technologiích se stal kyberprostor polem pro strategickou soutěž. Je proto nezbytné zachovat otevřený, svobodný, stabilní a bezpečný kyberprostor. Využívání kybernetických operací, které umožnily a doprovázely nevyprovokovanou a neodůvodněnou válečnou agresi Ruska proti Ukrajině, ovlivňuje globální stabilitu a bezpečnost, představuje významné riziko eskalace a přispívá k již tak významnému nárůstu nepřátelských činností v kyberprostoru v posledních letech mimo rámec ozbrojeného konfliktu.

2. Válka na Ukrajině představuje nový strategický kontext a potvrzuje, že je třeba, aby EU, její členské státy a jejich partneři dále posilovali odolnost EU vůči kybernetickým hrozbám a zvýšili naši společnou kybernetickou bezpečnost a kybernetickou obranu proti nepřátelskému chování a aktům agrese v kyberprostoru. Společné sdělení Politika kybernetické obrany EU signalizuje naše odhodlání přijmout okamžitá a dlouhodobá opatření k zajištění svobody jednání v kyberprostoru a reakce aktérům hrozeb, kteří se mimo jiné snaží proniknout do sítí a informačních systémů EU a jejích partnerů nebo je narušit či zničit. Toto společné sdělení, které doplňuje Strategii kybernetické bezpečnosti EU a je v souladu se Strategickým kompasem, představuje významný krok směrem k celospektrálnímu přístupu EU k odolnosti, reakci, předcházení konfliktům, spolupráci a stabilitě v kyberprostoru. V této souvislosti Rada zdůrazňuje potřebu vhodných a soudržných reakcí ze strany EU, jejích členských států a jejich partnerů a jako další klíčový krok vpřed ve vývoji kybernetické pozice EU rovněž se zájmem očekává revizi prováděcích pokynů k souboru nástrojů EU pro diplomacii v oblasti kybernetiky.

3. Rada zdůrazňuje, že nedávné kybernetické útoky na evropskou kritickou infrastrukturu, rychle se vyvíjející prostředí kybernetických hrozeb a rychlé tempo technologického rozvoje rovněž ukazují potřebu posílené civilně-vojenské koordinace a spolupráce, přičemž zdůrazňuje, že mezi civilním a vojenským společenstvím neexistuje hierarchie. Politika EU pro kybernetickou obranu umožňuje EU a jejím členským státům posílit jejich schopnost chránit se před kybernetickými útoky, odhalovat je, zabraňovat jim a odstrašovat od nich, přičemž mohou vhodným způsobem využívat celou škálu obranných možností, které mají civilní a vojenské komunity k dispozici pro širší bezpečnost a obranu EU, v souladu s mezinárodním právem, včetně práva v oblasti lidských práv a mezinárodního humanitárního práva.

4. I když národní bezpečnost, a to i v kybernetické oblasti, zůstává výhradní odpovědností každého členského státu, jak je uvedeno v čl. 4 odst. 2 Smlouvy o EU, Rada zdůrazňuje, že je třeba podstatně investovat, a to jednotlivě i společně, do zvyšování odolnosti a zavádění schopností v oblasti kybernetické obrany v celém spektru a posílení rámců spolupráce EU a finančních pobídek. Rada zdůrazňuje, že je třeba dále posílit opatření členských států a orgánů, institucí a jiných subjektů EU za účelem ochrany Unie, našich občanů, orgánů, institucí a jiných subjektů EU a misí a operací SBOP v kyberprostoru. Dále zdůrazňuje význam odolnosti EU v kyberprostoru prostřednictvím rozvoje schopností kybernetické obrany a posílením spolupráce s důvěryhodným soukromým ekosystémem.

I. **Společně jednat v zájmu silnější kybernetické obrany**

5. Rada znovu opakuje, že pro posílení důvěry má zásadní význam postupný, transparentní a inkluzivní proces, který je rozhodující pro další rozvoj rámce EU pro řešení krizí v oblasti kybernetické bezpečnosti, který musí probíhat v souladu s plánem pro řešení kybernetických krizí vypracovaným Radou. Rada znovu opakuje, že je třeba i nadále posilovat naši schopnost chránit se před kybernetickými útoky, odhalovat je, zabraňovat jim a odstrašovat od nich prostřednictvím větší informovanosti o situaci, budování kapacit, rozvoje schopností, školení, cvičení a zvýšení odolnosti a rozhodným způsobem na kybernetické útoky namířené proti EU, jejím členským státům a orgánům, institucím a jiným subjektům EU, misím a operacím SBOP reagovat, a to s využitím všech vhodných prostředků. Rada tímto vyzývá vysokého představitele a Komisi, aby zjednodušili oblast kybernetické bezpečnosti, zabránili zbytečnému zdvojování činností a zajistili spolupráci a synergie se stávajícími iniciativami. Je třeba posílit spolupráci a koordinaci mezi aktéry kybernetické obrany v rámci EU a členských států, mezi vojenskými a civilními kybernetickými komunitami a mezi veřejným a důvěryhodným soukromým ekosystémem. V této souvislosti se členské státy vyzývají, aby dále zkoumaly a posilovaly civilně-vojenské vnitrostátní koordinační mechanismy, usnadňovaly společné dobrovolné sdílení informací, sdílely získané poznatky, přispívaly k rozvoji interoperabilních norem, prováděly hodnocení rizik a připravovaly rizikové scénáře, jakož i společná cvičení, zejména na evropské úrovni, a to při plném dodržování ustanovení směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS2).

6. Rada uznává úsilí o další posílení odolnosti Unie prostřednictvím směrnice NIS2 a směrnice o odolnosti kritických subjektů a znovu opakuje své doporučení týkající se celounijního koordinovaného přístupu k posílení odolnosti kritické infrastruktury[1]. Vyzývá k přijetí opatření k dalšímu posílení odolnosti kritických subjektů, infrastruktury, digitálních produktů a služeb, přičemž konstatuje, že nejdůležitějším krokem zůstává řádné provádění směrnice NIS2. Ačkoli se jedná převážně o civilní odpovědnost, přispěje to rovněž k silnější kybernetické obraně. V této souvislosti se orgány, instituce a jiné subjekty EU i členské státy vyzývají, aby podporovaly další rozvoj a zavádění nových a stávajících koordinačních mechanismů EU, posouzení rizik, hodnocení a scénářů, společného dobrovolného sdílení informací a cvičení, a to způsobem, který přináší přidanou hodnotu a zabrání zbytečnému zdvojování stávajících iniciativ.

7. V zájmu dalšího posílení důvěry, upevnění spolupráce a usnadnění včasného sdílení informací o významných a rozsáhlých kybernetických incidentech, které mají dopad na obranné systémy, Rada vítá iniciativu zaměřenou na další rozvoj konference velitelů kybernetických sil EU, kterou bude pořádat každé předsednictví Rady EU za podpory Evropské obranné agentury (EDA) a za účasti Evropské služby pro vnější činnost (ESVČ). Rada vybízí všechny členské státy, aby se těchto zasedání účastnily. Pro posílení odolnosti EU vůči rozsáhlým kybernetickým bezpečnostním incidentům Rada vyzývá Evropskou síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe) a konferenci velitelů kybernetických sil EU, aby určily možné způsoby spolupráce a využití společné vojenské a civilní perspektivy.

[1] Návrh doporučení Rady o koordinovaném přístupu Unie za účelem posílení odolnosti kritické infrastruktury, COM/2022/551.

8. Rada vítá zřízení operační sítě EU pro vojenské týmy pro reakci na počítačové hrozby (MICNET), která má posílit sdílení technických informací o kybernetických incidentech, jež mají dopad na obranné systémy, mezi zúčastněnými členskými státy, a očekává, že do poloviny roku 2024 bude dosaženo její počáteční operační schopnosti, aby se podpořila důraznější a koordinovanější reakce na úrovni EU. Rada vyzývá všechny členské státy, aby se zapojily do sítě MICNET s cílem zajistit její účinnost. Dále členské státy vyzývá, aby vycházely ze zkušeností získaných z činnosti sítě týmů pro reakci na počítačové bezpečnostní incidenty (CSIRT), a důrazně vybízí k tomu, aby byl mezi oběma sítěmi ve vhodnou dobu vytvořen účinný mechanismus spolupráce a koordinace při plném respektování mechanismů správy a řízení a složek každého subjektu.

9. Vzhledem k nárůstu nepřátelských činností v kyberprostoru ze strany státních i nestátních aktérů zaměřených na mise a operace SBOP EU Rada vyzývá EU a její členské státy, aby posílily své schopnosti v oblasti obrany a zabezpečení misí a operací SBOP. V tomto ohledu Rada vítá cíle spočívající v dosažení dalšího pokroku v ochraně vojenských sítí a struktur EU, mimo jiné v souladu s vojenskou vizí a strategií EU pro kyberprostor jako oblast operací[2].

[2] ESVČ(2021) 706 REV 4.

10. Rada připomíná své závěry z května 2022[3] a potřebu investovat do naší vzájemné pomoci podle čl. 42 odst. 7 SEU, jakož i doložku solidarity podle článku 222 SFEU. Zdůrazňuje, že je důležité, aby EU a její členské státy dále prohlubovaly společné chápání provádění čl. 42 odst. 7, a to i ve složitých scénářích zahrnujících kybernetický útok, v souladu s příslušnými zásadami mezinárodního práva. Vítá možnost, aby EU na výslovnou žádost dotčeného členského státu nebo členských států poskytla v případě kybernetického útoku podporu, aniž je dotčena zvláštní povaha bezpečnostní a obranné politiky některých členských států.

11. Rada zdůrazňuje pokrok, jehož bylo dosaženo v rámci projektu stálé strukturované spolupráce týkajícího se „týmů rychlé kybernetické reakce a vzájemné pomoci v oblasti kybernetické bezpečnosti“ (CRRT), a jejich připravenost působit na požádání jako kapacita pro potřeby členských států a EU, na podporu misí a operací SBOP a pro poskytování pomoci partnerům EU. Rada vítá další rozvoj schopností týmů CRRT v rámci stálé strukturované spolupráce, vnitrostátních týmů pro kybernetickou reakci a případně dalších schopností reakce na incidenty, jako jsou budoucí týmy rychlé reakce na hybridní hrozby, jak se předpokládá ve Strategickém kompasu, mimo jiné i podporou jejich koordinace a spolupráce na úrovni EU.

[3] Závěry Rady o rozvoji kybernetické pozice Evropské unie, 23. května 2022, dokument 9364/22.

12. Rada vítá práci na projektu stálé strukturované spolupráce týkajícím se Koordinačního střediska pro kybernetický a informační prostor (CIDCC), jehož cílem je poskytnout vojenskou kapacitu pro shromažďování a analýzu informací relevantních pro společný operační kybernetický obraz. Dále vítá návrh, aby bylo ověření koncepce, bude-li úspěšná jako informační koordinační centrum, od roku 2025 začleněno do koordinačního centra EU pro kybernetickou obranu (EUCDCC), čímž se zlepší koordinace a informovanost o situaci zejména mezi veliteli misí a operací SBOP EU a dále se posílí širší velitelská a řídicí struktura EU. Rada vyzývá vysokého představitele, aby předložil koncepci a plán zřízení EUCDCC, přičemž by měl čerpat ze zkušeností z podobných mezinárodních subjektů, určit potřebné zdroje, zabránit zbytečnému zdvojování a usilovat o doplňkovost s širším rámcem EU pro kybernetickou bezpečnost.

13. Rada zdůrazňuje význam strategické zpravodajské spolupráce v oblasti kybernetických hrozeb a činností a vyzývá členské státy, aby prostřednictvím svých příslušných orgánů nadále přispívaly k práci střediska EU INTCEN, zpravodajského ředitelství Vojenského štábu EU a členských států v rámci společné zpravodajsko-analytické složky (SIAC). Dále zdůrazňuje, že je důležité posílit naše kapacity v oblasti kybernetických zpravodajských informací s cílem zlepšit naši kybernetickou odolnost a reakce a poskytovat účinnou podporu našim civilním a vojenským misím a operacím SBOP, jakož i našim ozbrojeným silám a kapacitě SIAC v kybernetické oblasti, a to na základě dobrovolných zpravodajských příspěvků členských států a aniž jsou dotčeny jejich pravomoci.

14. Rada bere na vědomí situační a analytické středisko pro kybernetické hrozby, které zřídila Evropská komise a jehož cílem je zlepšit informovanost Komise o situaci. Zdůrazňuje, že je důležité navázat vzájemně prospěšnou spolupráci mezi tímto střediskem a dalšími orgány, institucemi a jinými subjekty EU, zejména agenturou ENISA a CERT-EU. Rada zdůrazňuje, že je důležité zajistit úzkou spolupráci s unijními sítěmi spolupráce při rozvoji situačního povědomí, jakož i zachovávat důvěrnost. Bere na vědomí, že je třeba posílit společné situační povědomí na úrovni EU a dále rozvíjet rámec EU pro reakci na kybernetické bezpečnostní krize, přičemž je nezbytné zabránit zbytečnému zdvojování úsilí.

15. Rada připomíná, že vzdělávání, odborná příprava a cvičení v oblasti kybernetické bezpečnosti mají zásadní význam pro zajištění připravenosti a účinnosti, a vítá vnitrostátní činnosti, jakož i činnosti, které zajišťuje EU prostřednictvím Evropské bezpečnostní a obranné školy (EBOŠ), Evropské obranné agentury (EDA), agentury ENISA a probíhajících projektů stálé strukturované spolupráce, jako jsou Propojené kybernetické polygony a Akademické a inovační středisko EU pro kybernetickou oblast (CAIH). V zájmu dalšího posílení tohoto úsilí Rada se zájmem očekává vytvoření rámcového projektu EDA CyDef-X, jehož účelem je synchronizovat a podporovat cvičení v oblasti kybernetické obrany. Vybízí EDA, aby v úzké spolupráci s členskými státy a ESVČ prozkoumala, jak by CyDef-X mohl dále podporovat cvičení, jako je CYBER PHALANX, mimo jiné v oblasti vzájemné pomoci podle čl. 42 odst. 7 SEU a doložky solidarity podle článku 222 SFEU, jakož i s Komisí a agenturou ENISA, pokud jde o civilní cvičení. Rada dále vybízí k tomu, aby byla v rámci projektu CyDef-X využívána a dále rozvíjena stávající prostředí pro testování a cvičení v oblasti kybernetické obrany, jako jsou například Propojené kybernetické polygony. V zájmu zajištění agilního a účinného rozhodovacího procesu v případě kybernetické krize Rada zdůrazňuje, že je důležité pořádat pravidelná table-top cvičení pro rozhodovací úroveň členských států.

16. Rada bere na vědomí návrh aktu o kybernetické solidaritě a záměr posílit schopnosti odhalovat kybernetické hrozby a incidenty v EU a reagovat na ně. Rada zdůrazňuje, že návrhy v této oblasti mohou být účinné pouze tehdy, budou-li v souladu s rámci a potřebami členských států pro řešení krizí. Rada zdůrazňuje význam testování kritické infrastruktury s cílem zjistit potenciální slabá místa v případech, v nichž je to považováno za přínosné, a to v rámci vnitrostátní pravomoci a s přihlédnutím k dostupným posouzením rizik EU.

17. Rada bere na vědomí návrh Komise na zřízení mechanismu pro mimořádné situace v oblasti kybernetické bezpečnosti, který by mohl napomoci dostupnosti služeb kybernetické bezpečnosti od důvěryhodných soukromých poskytovatelů, kteří by na požádání pomáhali členským státům v případě rozsáhlých kybernetických bezpečnostních incidentů, a zároveň zdůrazňuje, že je třeba rozšířit evropské odvětví kybernetické bezpečnosti, a to s podporou Evropského centra kompetencí pro kybernetickou bezpečnost jakožto základního pilíře fungování tohoto mechanismu. Rada zdůrazňuje klíčovou úlohu každého členského státu při sledování a posuzování jeho vnitrostátních potřeb.

II. **Zabezpečení obranného ekosystému EU**

18. Rada připomíná, že vybízela členské státy, aby dále rozvíjely své vlastní schopnosti provádět operace kybernetické obrany, včetně případných proaktivních obranných opatření, jejichž cílem je chránit před kybernetickými útoky, odhalovat je, zabraňovat jim a odstrašovat od nich. Vzhledem k tomu, že se směrnice NIS2 nevztahuje na subjekty veřejné správy, které vykonávají své činnosti v oblasti obrany, Rada vyzývá agenturu EDA, aby za případné podpory Komise a ESVČ pomáhala členským státům při vypracovávání právně nezávazných dobrovolných doporučení vycházejících ze směrnice NIS2 s cílem zvýšit kybernetickou bezpečnost v obranném společenství, a vyzývá všechny členské státy, aby se do tohoto úsilí aktivně zapojily. V těchto doporučeních by mělo být zohledněno podobné úsilí vyvíjené v jiných rámcích.

19. Jak je uvedeno ve Strategickém kompasu, schopnost EU jednat závisí na její schopnosti snížit svou strategickou závislost u všech schopností a dodavatelských řetězců v oblasti kybernetické obrany, jakož i na vývoji a zvládnutí špičkových technologií v oblasti kybernetické obrany. Do této oblasti lze zahrnout posílení evropské technologické a průmyslové základny obrany (EDTIB) v celé EU a její schopnosti spolupracovat na recipročním základě s podobně smýšlejícími partnery po celém světě s cílem zajistit vzájemnou prospěšnost. Rada proto vyzývá odvětví kybernetické bezpečnosti a odvětví kybernetické obrany k úzké spolupráci s cílem vytvářet synergie za účelem rozvoje a poskytování kapacity v oblasti kybernetické obrany v plném rozsahu. Rada vyzývá Komisi, aby případně v úzké spolupráci s Evropským centrem kompetencí pro kybernetickou bezpečnost dále podporovala rozvoj silné, aktivní, celosvětově konkurenceschopné a inovativní evropské průmyslové a technologické základny kybernetické obrany, včetně malých a středních podniků, a to prostřednictvím dalších investic a politických opatření.

20. S ohledem na význam interoperability a shodnosti schopností kybernetické obrany, a to i pokud jde o společné rozvíjení schopností kybernetické obrany nové generace, Rada vyzývá agenturu EDA a Vojenský štáb EU, aby pracovaly na souboru požadavků EU na interoperabilitu kybernetické obrany, které by vycházely ze stávajících zásad, procesů a norem stanovených zejména v rámci Organizace Severoatlantické smlouvy (NATO) a byly by s nimi slučitelné. Rada dále vyzývá členské státy, aby v rámci Výboru pro evropskou normalizaci v oblasti obrany posoudily, zda by mohly být zapotřebí konkrétní dobrovolné normy pro obranné systémy, a to v úzké spolupráci se všemi příslušnými zúčastněnými stranami, případně včetně evropských normalizačních organizací a NATO.

21. Rada vítá činnost Komise směřující k předložení plánu na podporu používání stávajících norem pro použití v oblasti civilní kybernetické bezpečnosti a kybernetické obrany, jakož i vypracování nových dobrovolných norem. Rada zdůrazňuje, že ve vhodných případech je třeba sladit normy v oblasti kybernetické bezpečnosti a kybernetické obrany. Rada uznává, že tyto dobrovolné normy by mohly být užitečné pro odvětví kybernetické bezpečnosti a kybernetické obrany v EU, a naléhavě vyzývá k užší spolupráci mezi civilními a obrannými normalizačními orgány.

22. Rada vyzývá k urychlenému vypracování doporučení založených na zmapování stávajících nástrojů pro bezpečnou komunikaci v kybernetické oblasti, které provede Komise a příslušné orgány. Je-li to možné, měla by být doporučení sladěna se stávajícími iniciativami ohledně sdílení informací a měla by rovněž zohledňovat rizika, která pro stávající metody šifrování představují vznikající a přelomové technologie.

23. Rada dále vítá první kroky provedené v oblasti hodnocení rizik a scénářů, které vypracovává Komise, vysoká představitelka a skupina pro spolupráci v oblasti bezpečnosti sítí a informací, pokud jde původně o odvětví energetiky a telekomunikací, a to na žádost Rady. Rada oceňuje, že se rovněž připravují cílená posouzení rizik v oblasti kybernetické bezpečnosti pro komunikační infrastrukturu a sítě v EU. Rada znovu opakuje, že je nanejvýš důležité, aby se členské státy, ale také orgány, instituce a jiné subjekty EU, shodly na možných dopadech kybernetických incidentů. Rada proto vyzývá výše uvedené aktéry, aby zajistili, že hodnocení rizik, scénáře a následná doporučení budou zohledněny při vymezování a stanovování priorit opatření a podpory na úrovni EU a případně na vnitrostátní úrovni. Rada dále vyzývá k tomu, aby byly v rizikových scénářích zohledněny všechny příslušné subjekty podílející se na procesech posuzování rizik, jakož i při rozvíjení cvičení v oblasti kybernetické bezpečnosti.

III. **Investice do schopností kybernetické obrany**

24. Rada vyzývá členské státy, aby zvýšily své investice do budování, udržování a dalšího rozvoje interoperabilních schopností kybernetické obrany. Rada podporuje vypracování souboru dobrovolných závazků pro další rozvoj vnitrostátních schopností kybernetické obrany, a to s ohledem na podobné úsilí vyvíjené v jiných rámcích.

25. Rada vyzývá členské státy a agenturu EDA, aby využily příležitosti revize plánu rozvoje schopností a stanovily ambice na vysoké úrovni, pokud jde o rozvoj společné kybernetické obrany na úrovni EU. Rada dále vybízí členské státy, aby vycházely z aktualizovaného souboru priorit a ze svých závazků stálé strukturované spolupráce, pokud jde o zvýšení jejich zapojení do kooperativních projektů EU v oblasti rozvoje schopností kybernetické obrany, přičemž uznává přímý přínos projektů spolupráce na úrovni EU pro podporu rozvoje vnitrostátních schopností kybernetické obrany.

26. Rada vítá společné úsilí vyvíjené na úrovni EU v oblasti výzkumu, jehož cílem je prozkoumat možné využití vznikajících a přelomových technologií v systémech souvisejících s obranou, přičemž rovněž konstatuje, že je třeba zajistit, aby byly výsledky tohoto technologického vývoje rychle začleněny do stávajících a budoucích schopností. Rada vybízí členské státy a průmysl EU, aby co nejlépe využívaly možností kooperativního výzkumu na úrovni EU, například v rámci agentury EDA, probíhajících projektů stálé strukturované spolupráce, jako je Akademické a inovační středisko EU pro kybernetickou oblast (CAIH), Evropský obranný fond a v příslušných případech program Horizont Evropa a program Digitální Evropa pro projekty dvojího užití. Rada dále vítá využívání specializovaných rámců na podporu inovací v oblasti obrany s využitím produktu převzetí technologií z civilní oblasti, zejména Programu EU pro inovace v oblasti obrany a centra pro evropské inovace v oblasti obrany. Rada dále vybízí Evropské centrum kompetencí pro kybernetickou bezpečnost (ECCC) a agenturu EDA, aby vypracovaly pracovní ujednání s cílem usnadnit sdílení informací mezi příslušnými pracovníky ohledně priorit v oblasti civilních technologií, technologií dvojího užití a obranných technologií s cílem vytvářet synergie a zamezit zdvojování činností.

27. Rada vítá záměr Komise vypracovat technologický plán pro kritické kybernetické technologie, a to ve spolupráci s agenturou EDA a Evropským centrem kompetencí pro kybernetickou bezpečnost v souladu s jejich příslušnými mandáty, s členskými státy a za konzultace s příslušnými zúčastněnými stranami, jako je průmysl, který prostřednictvím identifikace kritických kybernetických technologií, mapování technologického vývoje a strategických závislostí poskytuje způsoby, jak tyto technologie omezit, a to na podporu strategické autonomie a technologické suverenity EU a při zachování otevřené ekonomiky. Rada bere na vědomí, že technologický plán pro kritické kybernetické technologie může být podkladem pro strategické priority ohledně nástrojů financování EU, přičemž musí být v souladu s příslušnými postupy platnými pro tyto nástroje. Rada připomíná, že EU by měla usilovat o ambiciózní a asertivní evropskou průmyslovou politiku s cílem vytvořit udržitelné, atraktivní a konkurenceschopné podnikatelské prostředí, jež může evropským subjektům v kybernetické oblasti také umožnit rozvoj.

28. Rada oceňuje záměr řešit významný nedostatek dovedností v oblasti kybernetické bezpečnosti přilákáním nových odborníků, včetně žen, zvyšováním kvalifikace a rekvalifikací a investováním do odborné přípravy a cvičení a jejich organizováním s cílem vybudovat rozmanitou a inkluzivní pracovní sílu v oblasti kybernetiky. Rada uznává výzvy, kterým EU čelí, pokud jde o lidský kapitál v oblasti kybernetické bezpečnosti a kybernetické obrany, a vítá iniciativu Akademie kybernetických dovedností, která může být přínosem i pro pracovníky v oblasti kybernetické obrany.

29. Rada vyzývá členské státy, aby si vyměňovaly informace o osvědčených postupech pro rozvíjení kvalifikovaných odborníků v oblasti kybernetické bezpečnosti s využitím synergií mezi vojenskými, civilními a donucovacími iniciativami, a vyzývá Evropskou bezpečnostní a obrannou školu, aby za podpory ze strany agentury EDA a agentury ENISA a za pomoci jejich odborných znalostí zvážila možnosti posílení výměny osvědčených postupů a další synergie mezi vojenskou a civilní oblastí, pokud jde o odbornou přípravu a rozvoj dovedností v oblasti kybernetické obrany.

30. Rada zdůrazňuje význam společného chápání složení pracovních sil v oblasti kybernetické bezpečnosti a souvisejících dovedností s cílem nalézt a řešit nedostatky na trhu práce v oblasti kybernetické bezpečnosti, jakož i potřebu zapojit všechny zúčastněné strany, včetně členských států a průmyslu. Rada uznává, že zavedení ukazatelů pro sledování trhu práce v oblasti kybernetické bezpečnosti by pomohlo určit potřeby ohledně dovedností v oblasti kybernetické bezpečnosti a odpovídajícím způsobem směrovat finanční prostředky a zároveň by přispělo ke splnění povinností souvisejících s politikou, zejména těch, které vyplývají ze směrnice NIS2. Rada vítá návrh na rámec pro certifikaci dovedností v oblasti kybernetické obrany a vyzývá vysokého představitele jakožto vedoucího Evropské bezpečnostní a obranné školy, aby jej ve spolupráci s ESVČ, Komisí a členskými státy prostřednictvím využití civilních iniciativ rozvíjel.

IV. **Partner při řešení společných výzev**

31. Rada vyzývá vysokého představitele a Komisi, aby posílili vzájemnou spolupráci, pokročily v ní a prozkoumali vzájemně přínosná a individuálně uzpůsobená partnerství v oblasti politik kybernetické obrany, včetně budování kapacit v oblasti kybernetické obrany prostřednictvím Evropského mírového nástroje. Za tímto účelem by měla být otázka kybernetické obrany doplněna jako bod při jednáních a konzultacích v rámci EU o kybernetických otázkách a při konzultacích s partnery o celkové bezpečnosti a obraně. Kromě toho by měl být posílen dialog a spolupráce se soukromým sektorem. Rada zdůrazňuje, že mezinárodní spolupráce ohledně norem a certifikace v oblasti kybernetické bezpečnosti by byla pro evropský průmysl přidanou hodnotou. Vítá proto závazek Komise začlenit tuto otázku jako podstatnou součást dialogů EU o kybernetické bezpečnosti se třetími zeměmi a mezinárodními organizacemi.

32. Rada zdůrazňuje význam mezinárodní spolupráce pro předcházení rizikům konfliktů v kyberprostoru nebo pro jejich omezování, zejména prostřednictvím dalšího rozvoje a zavedení opatření na budování důvěry na regionální a mezinárodní úrovni, mimo jiné i v rámci OSN, a další podpory využívání stávajících kybernetických opatření pro budování důvěry, jako je tomu v rámci Organizace pro bezpečnost a spolupráci v Evropě (OBSE), a to i v době mezinárodního napětí.
EU a její členské státy zdůrazňují, že v kyberprostoru platí stávající mezinárodní právo, a zdůrazňují, že je důležité pokračovat v úsilí o dodržování a prosazování rámce OSN pro odpovědné chování států a pracovat na jeho provádění, mimo jiné zavedením akčního programu na podporu odpovědného chování států v kyberprostoru.

33. V souladu se společnými prohlášeními o spolupráci mezi EU a NATO Rada vyzývá vysokého představitele, rovněž jakožto vedoucího agentury EDA, a Komisi, aby dále posílili, prohloubili a rozšířili partnerství s NATO v kybernetické oblasti, a to při plném dodržování zásad inkluzivnosti, reciprocity, vzájemné otevřenosti a transparentnosti a při zachování rozhodovací samostatnosti obou organizací. Rada bere v úvahu potřebu zajistit doplňkové a koordinované úsilí s co nejširším zapojením členských států, které nejsou součástí NATO, a zabránit zbytečnému zdvojování činností a vyzývá k vytvoření vazeb na příslušných úrovních mezi EU a NATO, pokud jde o odbornou přípravu, vzdělávání, informovanost o situaci, cvičení a platformy pro výzkum a vývoj, a k hledání možných synergií mezi příslušnými dobrovolnými závazky týkajícími se rozvoje vnitrostátních schopností kybernetické obrany a rámců pro řešení krizí, k úsilí zaměřenému na ochranu kritické infrastruktury a k posílení výměny informací o dané situaci, ke koordinované reakci na nepřátelské činnosti v kyberprostoru, jakož i k budování kapacit ve třetích zemích. To zahrnuje technické ujednání mezi složkou NATO pro schopnost reakce na počítačové incidenty (NCIRC) a týmem pro reakci na počítačové hrozby – EU (CERT-EU), jakož i posílený politický dialog o otázkách kybernetické obrany na všech úrovních.

V. **Závěr**

34. V návaznosti na závěry Rady o politice EU pro kybernetickou obranu Rada vyzývá vysokého představitele a Komisi, aby do druhého čtvrtletí roku 2023 vypracovali prováděcí plán této politiky, který schválí členské státy. Rada rovněž vyzývá členské státy, aby dobrovolně uvedly informace o svých ambicích a opatřeních v oblasti kybernetické obrany v souvislosti s politikou EU pro kybernetickou obranu a plně využívaly právně nezávazných dobrovolných doporučení a závazků ke zvýšení svého vnitrostátního a mnohonárodního úsilí v oblasti kybernetické obrany s cílem maximalizovat dopad na úrovni EU. Vysoký představitel, Komise a členské státy se vyzývají, aby počínaje druhým čtvrtletím roku 2024 podali zprávu a každoročně projednali pokrok při provádění prvků společného sdělení a jeho prováděcího plánu.