Rada
Evropské unie

Brusel 23. května 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

VÝSLEDEK JEDNÁNÍ

Odesílatel:	Generální sekretariát Rady
Datum:	23. května 2022
Příjemce:	Delegace
Předmět:	Závěry Rady o rozvoji kybernetické pozice Evropské unie – závěry schválené Radou na zasedání dne 23. května 2022

Delegace naleznou v příloze závěry Rady o rozvoji kybernetické pozice Evropské unie ve znění schváleném Radou na zasedání dne 23. května 2022.

PŘÍLOHA

Závěry Rady o rozvoji kybernetické pozice Evropské unie

RADA EVROPSKÉ UNIE,

PŘIPOMÍNAJÍC své závěry o:

– společném sdělení Evropskému parlamentu a Radě ze dne 25. června 2013 nazvaném Strategie kybernetické bezpečnosti Evropské unie: „Otevřený, bezpečný a chráněný kyberprostor“[1],

– politickém rámci EU pro kybernetickou obranu[2],

– správě internetu[3],

– kybernetické diplomacii[4],

– posílení evropského systému kybernetické odolnosti a o podpoře konkurenceschopného a inovativního odvětví kybernetické bezpečnosti[5],

– společném sdělení Evropskému parlamentu a Radě ze dne 20. listopadu 2017: „Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU“[6],

– rámci pro společnou diplomatickou reakci EU na nepřátelské činnosti v kyberprostoru („soubor nástrojů pro diplomacii v oblasti kybernetiky“)[7],

– koordinované reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[8],

– pokynech EU pro budování vnějších kybernetických kapacit[9],

---

1 Dokument 12109/13.
2 Dokument 15585/14.
3 Dokument 16200/14.
4 Dokument 6122/15 + COR 1.
5 Dokument 14540/16.
6 Dokument 14435/17 + COR 1.
7 Dokument 10474/17.
8 Dokument 10086/18.
9 Dokument 10496/18.

– prováděcím rozhodnutí Rady (EU) 2018/1993 ze dne 11. prosince 2018 o opatřeních pro integrovanou politickou reakci EU na krize[10],

– budování kapacit a schopností v oblasti kybernetické bezpečnosti v EU[11],

– významu 5G pro evropské hospodářství a potřebě zmírnit bezpečnostní rizika spojená s 5G[12],

– budoucnosti vysoce digitalizované Evropy po roce 2020: „Posílení digitální a hospodářské konkurenceschopnosti v Unii a digitální soudržnosti“[13],

– dalším úsilí za účelem posílení odolnosti a boje proti hybridním hrozbám[14],

– utváření digitální budoucnosti Evropy[15],

– kybernetické bezpečnosti zařízení připojených k internetu[16],

– strategii kybernetické bezpečnosti EU pro digitální dekádu[17],

– bezpečnosti a obraně[18],

– prozkoumání potenciálu iniciativy ke zřízení společné kybernetické jednotky, která by doplnila koordinovanou reakci EU na rozsáhlé kybernetické bezpečnostní incidenty a krize[19],

– Strategickém kompasu pro bezpečnost a obranu – Za Evropskou unii, která chrání své občany, hodnoty a zájmy a přispívá k mezinárodnímu míru a bezpečnosti[20],

---

10 Úř. věst. L 320, 17.12.2018, s. 28.
11 Dokument 7737/19.
12 Dokument 14517/19.
13 Dokument 9596/19.
14 Dokument 14972/19.
15 Dokument 8711/20.
16 Dokument 13629/20.
17 Dokument 7290/21.
18 Dokument 8396/21.
19 Dokument 13048/21.
20 Dokument 7371/22.

1. ZDŮRAZŇUJE, že nepřátelské chování v kyberprostoru, jehož zdrojem jsou státní i nestátní subjekty, se v posledních letech zintenzivnilo, včetně prudkého a soustavného nárůstu nepřátelských činností zaměřených na kritickou infrastrukturu, dodavatelské řetězce a duševní vlastnictví EU a jejích členských států, zvýšeného rizika vedlejších účinků, jakož i nárůstu ransomware útoků na naše podniky, organizace a občany. KONSTATUJE, že s návratem mocenské politiky se některé země stále více pokoušejí zpochybňovat a narušovat v kyberprostoru mezinárodní řád založený na pravidlech a přeměňují kybernetickou sféru, spolu s volným mořem, vzduchem a kosmickým prostorem, v oblasti, v nichž dochází ke stále intenzivnější soutěži. UZNÁVÁ, že rozsáhlé kybernetické útoky nebo pokusy o narušení nebo zničení sítí a informačních systémů a vniknutí do nich, které mají systémové účinky, se staly běžnějšími, mohly by narušit naši hospodářskou bezpečnost a ovlivnit naše demokratické instituce a procesy a ukázat připravenost některých aktérů vytvářet rizika pro mezinárodní bezpečnost a stabilitu. ZDŮRAZŇUJE, že vojenská agrese Ruska vůči Ukrajině prokázala, že ofenzivní kybernetická činnost může být prováděna jako nedílná součást hybridních strategií kombinujících zastrašování, destabilizaci a narušení ekonomiky.

2. OPAKUJE, že vzhledem k současným geopolitickým změnám spočívá síla naší Unie v jednotě, solidaritě a odhodlání a že provádění Strategického kompasu posílí strategickou autonomii EU a její schopnost spolupracovat s partnery na ochraně jejích hodnot a zájmů, a to i v kybernetické oblasti. ZDŮRAZŇUJE, že silnější a schopnější EU v oblasti bezpečnosti a obrany pozitivně přispěje ke globální a transatlantické bezpečnosti a bude doplňovat NATO, které pro své členy zůstává základem kolektivní obrany. ZNOVU POTVRZUJE záměr EU zintenzivnit podporu mezinárodnímu řádu založenému na pravidlech, jehož jádrem je Organizace spojených národů.

3. V souladu se závěry Rady o strategii kybernetické bezpečnosti EU a se Strategickým kompasem OPĚTOVNĚ UPOZORŇUJE na potřebu rozvíjení kybernetické pozice Unie tím, že posílíme naši schopnost předcházet kybernetickým útokům prostřednictvím budování kapacit, rozvoje schopností, odborné přípravy, cvičení, zvýšené odolnosti a rozhodným reagováním na kybernetické útoky proti EU a jejím členským státům s využitím všech dostupných nástrojů EU. To zahrnuje další úsilí prokazovat, že je EU odhodlána zajišťovat okamžitou i dlouhodobou reakci vůči aktérům hrozeb, kteří se snaží zabránit našemu bezpečnému a otevřenému přístupu do kyberprostoru a ovlivnit naše strategické zájmy, včetně bezpečnosti našich partnerů. V této souvislosti ZDŮRAZŇUJE, že cílem kybernetické pozice je kombinovat různé iniciativy, které jsou v souladu s opatřeními EU, jež upevňují mír a stabilitu v kyberprostoru, ve prospěch otevřeného, svobodného, globálního, stabilního a bezpečného kyberprostoru, a zároveň lépe koordinovat krátkodobá, střednědobá a dlouhodobá opatření s cílem předcházet kybernetickým hrozbám a útokům, odrazovat od nich a reagovat na ně a posilovat kybernetické kapacity. ZDŮRAZŇUJE, že tyto prvky by měly být začleněny do kybernetické pozice EU v souladu s pěti funkcemi EU v kybernetické oblasti: posilovat naši kybernetickou odolnost a kapacity pro ochranu, posilovat solidární a komplexní řešení krizí, prosazovat naši vizi kyberprostoru, posilovat spolupráci s partnerskými zeměmi a mezinárodními organizacemi, předcházet kybernetickým útokům, bránit se proti nim a reagovat na ně.

I. POSILOVAT NAŠI KYBERNETICKOU ODOLNOST A KAPACITY PRO OCHRANU

4. ZNOVU OPAKUJE, že je třeba zvýšit celkovou úroveň kybernetické bezpečnosti EU, OČEKÁVÁ rychlé přijetí návrhu směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS), návrhu nařízení o digitální provozní odolnosti finančních služeb (DORA) a návrhu směrnice o odolnosti kritických subjektů (CER) a BERE NA VĚDOMÍ návrh nařízení, kterým se stanoví opatření k zajištění vysoké úrovně kybernetické bezpečnosti v orgánech, institucích a jiných subjektech Unie, jež má Evropskou unii podpořit při ochraně jejích občanů, veřejných služeb a podniků v kyberprostoru. VYBÍZÍ Komisi, aby dokončila přijetí klíčových návrhů s cílem zajistit, aby digitální infrastruktury, technologie, produkty a služby byly zabezpečeny, a vyslala tak jasný signál o ambicích EU v této oblasti a zajistila podnikům příslušnou podporu, aby mohly této výzvě čelit. VYZÝVÁ Komisi, aby navrhla společné požadavky EU na kybernetickou bezpečnost pro připojená zařízení a související procesy a služby prostřednictvím aktu o kybernetické odolnosti, který by měla Komise navrhnout do konce roku 2022, přičemž zohlední potřebu horizontálního a uceleného přístupu, který bude pokrývat celý životní cyklus digitálních produktů, jakož i stávající regulaci, zejména v oblasti kybernetické bezpečnosti.

5. VYZÝVÁ příslušné orgány, jako je Sdružení evropských regulačních orgánů v oblasti elektronických komunikací (BEREC), Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) a skupina pro spolupráci v oblasti bezpečnosti sítí a informací, aby společně s Evropskou komisí vypracovaly na základě posouzení rizik doporučení členským státům a Evropské komisi s cílem posílit odolnost komunikačních sítí a infrastruktur v Evropské unii, včetně pokračujícího provádění souboru opatření EU pro 5G.

6. VYZÝVÁ EU a její členské státy, aby zintenzivnily úsilí o zvýšení celkové úrovně kybernetické bezpečnosti, například usnadněním vzniku důvěryhodných poskytovatelů služeb kybernetické bezpečnosti, a ZDŮRAZŇUJE, že podpora rozvoje těchto poskytovatelů by měla být prioritou průmyslové politiky EU v oblasti kybernetické bezpečnosti. VYZÝVÁ Komisi, aby s cílem lépe odolávat kybernetickým útokům s možnými systémovými účinky a bojovat proti nim a na základě zkušeností s řešením zranitelnosti softwaru v souvislosti se Solarwinds, Microsoft Exchange a Apache Log4J navrhla možnosti, jak podpořit vznik důvěryhodného odvětví služeb kybernetické bezpečnosti, posílit kybernetickou bezpečnost dodavatelského řetězce v oblasti IKT, řešit potenciální dopady zranitelnosti softwaru na EU a její členské státy, a to i s ohledem na nadcházející akt o kybernetické odolnosti, a zlepšit schopnosti odhalování a sdílení kybernetických hrozeb v členských státech a mezi nimi.

7. OPAKUJE, že investice do inovací a lepší využívání civilních technologií jsou klíčové pro posílení naší technologické suverenity, a to i v kybernetické oblasti, VYZÝVÁ Komisi, aby urychleně uvedla do provozu Evropské centrum kompetencí pro kybernetickou bezpečnost s cílem vytvořit silný evropský kybernetický výzkum a průmyslový a technologický ekosystém, a ZDŮRAZŇUJE, že je třeba posílit výzkum a inovace, více investovat do civilních a obranných oblastí s cílem posílit evropskou technologickou a průmyslovou základnu obrany a rozvíjet kybernetické schopnosti EU a jejích členských států, včetně strategických podpůrných schopností. ZDŮRAZŇUJE, že je důležité intenzivně využívat nové technologie, zejména kvantovou výpočetní techniku, umělou inteligenci a data velkého objemu, s cílem dosáhnout komparativních výhod, a to i pokud jde o operace reagující na kybernetiku.

8. UZNÁVÁ, že posílení naší kybernetické bezpečnosti je způsobem, jak zvýšit efektivitu a zabezpečení našeho úsilí na pevnině, ve vzduchu, na moři a v kosmickém prostoru, ZDŮRAZŇUJE, že je důležité začlenit otázky kybernetické bezpečnosti do všech veřejných politik EU, včetně odvětvových právních předpisů doplňujících směrnici NIS 2, a VYZÝVÁ Komisi, aby prozkoumala možnosti, jak zvýšit kybernetickou bezpečnost v celém dodavatelském řetězci evropské technologické a průmyslové základny obrany.

9. UZNÁVÁ, že pro rozvoj kybernetické pozice EU má zásadní význam zajištění odpovídajících finančních a lidských zdrojů pro kybernetickou bezpečnost a opatření zaměřená na vytvoření příznivého prostředí pro konkurenceschopnost soukromého sektoru a že otázka stabilního a dlouhodobého financování kybernetické bezpečnosti by měla být rovněž řešena na úrovni EU navržením a prováděním horizontálního mechanismu kombinujícího více zdrojů financování, včetně nákladů na vysoce kvalifikované lidské zdroje. VYZÝVÁ proto Komisi, aby do konce roku 2022 prozkoumala možnosti takového mechanismu, které budou projednány v příslušných orgánech Rady.

10. ZDŮRAZŇUJE, že je třeba zintenzivnit naše úsilí a posílit spolupráci v boji proti mezinárodní kyberkriminalitě, zejména proti ransomware, prostřednictvím mechanismu EMPACT (evropská multidisciplinární platforma pro boj proti hrozbám vyplývajícím z trestné činnosti), prostřednictvím výměn mezi odvětvími kybernetické bezpečnosti, prosazování práva a diplomacie a posílením schopností v oblasti prosazování práva při vyšetřování a stíhání kyberkriminality. OPAKUJE svůj závazek informovat veřejnost o kybernetických hrozbách a opatřeních přijatých proti nim na vnitrostátní úrovni i na úrovni EU, a to zapojením občanské společnosti, soukromého sektoru a akademické obce, s cílem zvýšit informovanost a podpořit odpovídající úroveň kybernetické ochrany a kybernetické hygieny. ZDŮRAZŇUJE, že je třeba se zaměřit na dovednosti a schopnosti občanů v oblasti kybernetické bezpečnosti na úrovni EU a členských států a na potřebu aktivně zapojit uživatele do jejich vlastní ochrany.

II. **POSILOVAT SOLIDÁRNÍ A KOMPLEXNÍ ŘEŠENÍ KRIZÍ**

11. Na základě každoročních kybernetických cvičení, dalších cvičení s kybernetickým rozměrem a cvičení EU CyCLES konaného v roce 2022 ZDŮRAZŇUJE, že je důležité za účasti Rady, ESVČ, Komise a relevantních zúčastněných stran, jako je agentura ENISA a soukromý sektor, zavést program pravidelných kybernetických cvičení napříč komunitami a na více úrovních s cílem testovat a rozvíjet vnitřní i vnější reakci EU na rozsáhlé kybernetické incidenty, který bude po rozpracování přispívat k obecné politice EU v oblasti cvičení. ZDŮRAZŇUJE, že je důležité dále rozvíjet cvičení Cyber Europe a BlueOLEx, která kombinují reakci na různých úrovních. UZNÁVÁ, že je třeba vyhodnotit a konsolidovat stávající cvičení a prozkoumat možnost dalších cvičení týkající se konkrétních segmentů kybernetické oblasti, zejména vojenského cvičení skupiny pro reakci na počítačové hrozby v orgánech, institucích a jiných subjektech EU (CERT) a cvičení zaměřeného na krizovou spolupráci mezi těmito subjekty. UZNÁVÁ, že kybernetická pozice Unie prostřednictvím různých akcí včetně odborné přípravy posílí naši schopnost předcházet kybernetickým útokům, a VYZÝVÁ proto členské státy, aby posílily civilně-vojenskou spolupráci při odborné přípravě a společných cvičeních v oblasti kybernetiky.

12. ZDŮRAZŇUJE, že je třeba dále testovat a posilovat operační spolupráci a sdílenou informovanost o situaci mezi členskými státy, mimo jiné prostřednictvím zavedených sítí, jako je síť CSIRT a Síť styčných organizací pro řešení kybernetických krizí (EU CyCLONe), s cílem zlepšit připravenost EU na řešení rozsáhlých kybernetických incidentů. ZDŮRAZŇUJE, že je důležité pracovat na vytvoření společného jazyka mezi členskými státy a orgány, institucemi a jinými subjekty EU, který bude uzpůsoben pro diskusi na politické úrovni, s cílem podpořit vypracování konsolidovaného posouzení závažnosti a dopadu relevantních kybernetických incidentů, jakož i možných scénářů vývoje a potřeb z nich vyplývajících. ZDŮRAZŇUJE v tomto ohledu, že je třeba zlepšit doplňkovost sdílených zpráv o situačním hodnocení, včetně zpráv sítě EU CyCLONe o dopadu a závažnosti rozsáhlých kybernetických incidentů ve všech členských státech EU a posouzení hrozeb, která poskytuje Zpravodajské a informační centrum EU v rámci souboru nástrojů EU pro diplomacii v oblasti kybernetiky. VYZÝVÁ Komisi, vysokého představitele a skupinu pro spolupráci v oblasti bezpečnosti sítí a informací, aby v koordinaci s příslušnými civilními i vojenskými orgány a agenturami a se zavedenými sítěmi včetně sítě EU CyCLONe provedli do konce roku 2022 hodnocení rizik a vypracovali rizikové scénáře z hlediska kybernetické bezpečnosti v situaci hrozby nebo možného útoku vůči členským státům nebo partnerským zemím a předložili je příslušným orgánům Rady. ZDŮRAZŇUJE potřebu vhodné a koordinované veřejné komunikace o reakci EU na rozsáhlé kybernetické incidenty.

13. ZDŮRAZŇUJE, že v případě rozsáhlých kybernetických incidentů je třeba posílit koordinaci a případně vycházet z dosaženého pokroku a práce týmů rychlé kybernetické reakce v rámci stálé strukturované spolupráce a vycházet z práce sítí CSIRT a EU CyCLONe a z dobrovolného sdružování našich kapacit pro reakci na incidenty mezi členskými státy. UZNÁVÁ, že veřejné kapacity by mohl posílit rozvoj vazeb se soukromým sektorem, zejména v souvislosti s nedostatkem kvalifikovaných pracovníků v celé EU, a že identifikace a koordinace těchto soukromých partnerů by mohla příznivě ovlivnit případy rozsáhlých incidentů. VYZÝVÁ Komisi, aby za účelem kompletní přípravy na řešení rozsáhlých kybernetických incidentů do konce třetího čtvrtletí roku 2022 předložila návrh nového fondu pro reakci na mimořádné události v oblasti kybernetické bezpečnosti.

14. V souladu se Strategickým kompasem OPAKUJE, že je třeba investovat do naší vzájemné pomoci podle čl. 42 odst. 7 Smlouvy o Evropské unii, jakož i do solidarity podle článku 222 Smlouvy o fungování Evropské unie, zejména prostřednictvím častých cvičení. V tomto rámci ZDŮRAZŇUJE, že je třeba dále pracovat na poskytování a koordinaci dvoustranné civilní nebo vojenské podpory, mimo jiné zkoumáním možné podpory poskytované EU na výslovnou žádost členských států, a na určení vhodných opatření reakce a komunikační strategie v souvislosti s prováděním čl. 42 odst. 7. KONSTATUJE, že by to mělo rovněž zahrnovat prostudování vazeb se stávajícími mechanismy EU pro řešení krizí a s mechanismem civilní ochrany EU.

15. ZDŮRAZŇUJE, že posílený kybernetický postoj EU bude vyžadovat zdokonalenou zabezpečenou komunikaci. Za tímto účelem ZNOVU UPOZORŇUJE na směry stanovené v tomto ohledu Strategickým kompasem a VYZÝVÁ Komisi a další příslušné orgány, instituce a agentury, aby do konce roku 2022 zmapovaly stávající nástroje pro zabezpečenou komunikaci v kybernetické oblasti, které budou projednány v příslušných orgánech Rady a s příslušnými skupinami pro spolupráci, jako jsou sítě CSIRT a EU CyCLONe.

III. PROSAZOVAT NAŠI VIZI KYBERPROSTORU

16. PŘIPOMÍNÁ, že cílem společného a komplexního přístupu EU ke kybernetické diplomacii je podílet se na předcházení konfliktům, zmírňování kybernetických hrozeb a větší stabilitě mezinárodních vztahů. V této souvislosti ZNOVU POTVRZUJE, že je odhodlána řešit mezinárodní spory v kyberprostoru mírovými prostředky a uplatňovat na činnosti států v kyberprostoru mezinárodní právo, včetně mezinárodního práva v oblasti lidských práv a mezinárodního humanitárního práva. ZDŮRAZŇUJE závazek EU a jejích členských států jednat v souladu s dobrovolnými nezávaznými normami odpovědného chování států v kyberprostoru, na nichž se dohodly všechny členské státy OSN. ZDŮRAZŇUJE význam otevřeného, svobodného, globálního, stabilního a bezpečného kyberprostoru, v němž se plně uplatňují lidská práva, základní svobody a zásady právního státu na podporu sociálního blahobytu, hospodářského růstu, prosperity a integrity našich svobodných a demokratických společností, a ZNOVU POTVRZUJE závazek EU a jejích členských států tyto hodnoty a zásady nadále prosazovat. S cílem vytvořit kanály pro konstruktivní, upřímný a otevřený dialog s klíčovými zúčastněnými stranami v kyberprostoru ZDŮRAZŇUJE, že je důležité učinit z kybernetických otázek, včetně souboru nástrojů EU pro diplomacii v oblasti kybernetiky, nedílnou součást jednání o přistoupení k Unii a strategických a politických dialogů EU s mezinárodními partnery i konkurenty, a současně VYZÝVÁ vysokého představitele, aby přezkoumal stávající dvoustranné dialogy o kyberprostoru a v případě potřeby navrhl zahájit podobnou spolupráci s dalšími zeměmi nebo relevantními mezinárodními organizacemi.

17. PŘIPOMÍNÁ význam spolupráce mnoha zúčastněných stran, neboť za kybernetickou bezpečnost nesou odpovědnost i další zúčastněné strany, zejména pokud jde o provádění doporučení a rozhodnutí přijatých na mezinárodních a regionálních fórech. VYZÝVÁ EU a její členské státy, aby dále podporovaly náš model kyberprostoru a internetu založený na přístupu zahrnujícím mnoho zúčastněných stran a prostřednictvím iniciativ, jako je pařížská výzva k zajištění důvěry a bezpečnosti v kyberprostoru a prohlášení o budoucnosti internetu, jež zdůrazňují sdílené přínosy stability v kyberprostoru a zvyšují celosvětové povědomí o nebezpečích státní a autoritářské vize internetu, a VYZÝVÁ EU a její členské státy, aby dále posilovaly spolupráci se společenstvím mnoha zúčastněných stran, mimo jiné využíváním relevantních projektů, jako je iniciativa EU pro kybernetickou diplomacii v rámci nástroje zahraniční politiky.

18. ZAVAZUJE SE k trvalému zapojení do příslušných mezinárodních organizací, zejména do procesů souvisejících s prvním a třetím výborem OSN, přičemž zdůrazňuje, že v kyberprostoru a s ohledem na kyberprostor se bez výhrad uplatňuje stávající mezinárodní právo. ZDŮRAZŇUJE význam soustavného úsilí o prosazování a podporu rámce OSN pro odpovědné chování států v kyberprostoru a PODTRHUJE, že EU a její členské státy budou aktivně usilovat o jeho posílené provádění, mimo jiné zřízením akčního programu na podporu odpovědného chování států v kyberprostoru. ZDŮRAZŇUJE, že EU a její členské státy se aktivně zapojí do jednání o budoucí úmluvě OSN, která má sloužit jako účinný nástroj pro donucovací a justiční orgány v celosvětovém boji proti kyberkriminalitě, přičemž plně zohlední stávající rámec mezinárodních a regionálních nástrojů v této oblasti, zejména Budapešťskou úmluvu o počítačové kriminalitě. ZDŮRAZŇUJE, že je důležité dále podporovat rozvoj a uplatňování opatření pro budování důvěry na regionální a mezinárodní úrovni a dále podporovat využívání stávajících opatření pro budování důvěry v kybernetické oblasti v rámci OBSE, a to i v době mezinárodního napětí.

19. PŘIPOMÍNÁ, že proaktivní přístup k zajištění mezinárodních norem v oblasti vznikajících technologií a základní internetové architektury v souladu s demokratickými hodnotami a zásadami, založený na lidských právech, má zásadní význam pro zajištění toho, aby internet zůstal globální, nefragmentovaný a otevřený, a PODPORUJE zásadu, že využívání a vývoj technologií respektuje lidská práva, jsou zaměřené na soukromí a jejich využívání má být zákonné, bezpečné a etické. VYBÍZÍ vysokého představitele a Komisi, aby vypracovali strategickou vizi technických otázek v digitální oblasti, které mají důsledky pro zahraniční politiku a mohly by mít dopad na stabilitu kyberprostoru a zejména internetu, a to i v rámci příslušných specializovaných mezinárodních organizací (např. Mezinárodní telekomunikační unie).

IV. POSILOVAT SPOLUPRÁCI S PARTNERSKÝMI ZEMĚMI A MEZINÁRODNÍMI ORGANIZACEMI

20. ZDŮRAZŇUJE, že je třeba lépe propojit strategii EU v oblasti budování kybernetických kapacit s normami OSN týkajícími se odpovědného chování států v kyberprostoru, mimo jiné vypracováním uzpůsobených programů spolupráce a budování kapacit s cílem podpořit třetí země při jejich provádění, a tím pokračovat v našem úsilí o podporu akčního programu OSN na prosazování odpovědného chování států v kyberprostoru a toto úsilí rozšiřovat. ZDŮRAZŇUJE, že je důležité plně začlenit budování kybernetických kapacit do nabídky EU jakožto zajišťovatele bezpečnosti, a to s odpovídající koordinací úsilí mezi členskými státy a orgány, institucemi a jinými subjekty EU, a zejména VÍTÁ spolupráci mezi členskými státy, jakož i s partnery z veřejného i soukromého sektoru, konkrétně prostřednictvím sítě EU CyberNet (síť EU pro budování kybernetických kapacit) a světového fóra pro počítačovou odbornost (GFCE), s cílem zajistit koordinaci a zabránit zdvojování činností.

VYZÝVÁ vysokého představitele a Komisi, aby do třetího čtvrtletí 2022 zřídili *Radu pro budování kybernetických kapacit* a aby pořádali pravidelné výměny informací v rámci Horizontální pracovní skupiny pro otázky týkající se kybernetiky. VYZÝVÁ Komisi a vysokého představitele, aby usilovali o další mobilizaci Nástroje pro sousedství a rozvojovou a mezinárodní spolupráci (NDICI), Nástroje předvstupní pomoci (NPP III) a dalších finančních nástrojů, jako je Evropský mírový nástroj (EPF) a iniciativa Global Gateway, s cílem podpořit posílení odolnosti našich partnerů, jejich kapacity pro identifikaci a řešení kybernetických hrozeb a vyšetřování a stíhání kyberkriminality a rozvoj projektů

spolupráce, a to i v krizové situaci, přičemž zejména VYBÍZÍ ke spolupráci s partnery na západním Balkáně a v zemích východního a jižního sousedství EU a k nasazení odborníků EU a členských států s cílem nabídnout podporu v případě kybernetických krizí, s ohledem na stávající právní mandáty.

21. ZDŮRAZŇUJE, že je třeba zintenzívnit úsilí o vytvoření strukturovaného a otevřeného přístupu EU k tomu, jak podpořit globální společné porozumění týkající se uplatňování mezinárodního práva v kyberprostoru, rámce OSN pro odpovědné chování států v kyberprostoru, včetně iniciativy pro akční program na podporu odpovědného chování států v kyberprostoru, jakož i postoje EU a jejích členských států v probíhajících jednáních o úmluvě OSN o kyberkriminalitě, a v rámci tohoto úsilí ŽÁDÁ vysokého představitele, aby do konce roku 2022 předložil Radě plán spolupráce. VYBÍZÍ vysokého představitele a útvary Komise, aby plně a systematicky využívali všech 145 delegací a rozvíjeli pravidelnou a plodnou spolupráci mezi nimi a velvyslanectvími členských států ve třetích zemích pod záštitou plánované sítě EU pro kybernetickou diplomacii. VYZÝVÁ vysokého představitele, aby do třetího čtvrtletí 2022 zřídil síť EU pro kybernetickou diplomacii, která bude přispívat k výměně informací, společným vzdělávacím činnostem pro zaměstnance EU a členských států, soudržnému úsilí o budování kapacit a posílenému provádění rámce OSN pro odpovědné chování států, jakož i k opatřením na budování důvěry mezi státy.

22. ZDŮRAZŇUJE, že je odhodlána dále spolupracovat s mezinárodními organizacemi a partnerskými zeměmi, aby se pokročilo ve společném chápání problematiky kybernetických hrozeb, rozvíjely se mechanismy spolupráce a proaktivně se identifikovaly diplomatické reakce založené na spolupráci. PŘIPOMÍNAJÍC klíčové úspěchy spolupráce mezi EU a NATO v oblasti kybernetické bezpečnosti v rámci provádění společných prohlášení z Varšavy z roku 2016 a z Bruselu z roku 2018, při plném respektování rozhodovací samostatnosti a postupů obou organizací a na základě zásad transparentnosti, reciprocity a inkluzivnosti, ZDŮRAZŇUJE, že je třeba dále posilovat kybernetickou spolupráci s NATO prostřednictvím cvičení, sdílení a výměn informací mezi odborníky, mimo jiné v oblasti rozvoje schopností a budování kapacit pro partnery, a misí a operací, jakož i prostřednictvím použitelnosti mezinárodního práva a norem OSN pro odpovědné chování států v kyberprostoru a možné koordinované reakce na nepřátelské činnosti v kyberprostoru.

V. PŘEDCHÁZET KYBERNETICKÝM ÚTOKŮM, BRÁNIT SE PROTI NIM A REAGOVAT NA NĚ

23. UZNÁVÁ, že kyberprostor se stal arénou geopolitického soupeření, a proto OPAKUJE, že EU musí být schopna rychle a důrazně reagovat na kybernetické útoky, jako jsou státem podporované nepřátelské činnosti v kyberprostoru zaměřené na EU a její členské státy, a proto musí posílit soubor nástrojů EU pro diplomacii v oblasti kybernetiky a plně využívat všech svých nástrojů, včetně dostupných politických, hospodářských, diplomatických, právních a strategických komunikačních nástrojů k předcházení nepřátelským činnostem v kyberprostoru, odrazování a odstrašování od nich a reakci na ně. ZDŮRAZŇUJE, že nepřátelští aktéři si musí být vědomi toho, že kybernetické útoky proti členským státům a orgánům EU budou včas odhaleny, neprodleně identifikovány a řešeny všemi nezbytnými nástroji a politikami. VYZÝVÁ členské státy a vysokého představitele, aby do konce prvního čtvrtletí 2023 za podpory Komise vypracovali revidovanou verzi prováděcích pokynů k souboru nástrojů EU pro diplomacii v oblasti kybernetiky, a to zejména prověřením dalších opatření v oblasti reakce a na základě prvků, které jsou obsaženy v kybernetické pozici EU, jakož i zkušeností získaných při provádění souboru nástrojů pro diplomacii v oblasti kybernetiky od jeho vzniku a z cvičení věnovaného kybernetické bezpečnosti (EU CyCLES).

24. ZDŮRAZŇUJE, že je třeba pořádat pravidelné výměny informací o problematice kybernetických hrozeb v příslušných orgánech a výborech Rady a zároveň pravidelně spolupracovat se soukromým sektorem a vycházet z posouzení dopadů a závažnosti nedávných incidentů, zvyšovat celkovou informovanost a připravenost na další aplikace souboru nástrojů EU pro diplomacii v oblasti kybernetiky a vyvíjet další nástroje na podporu jeho provádění. Ačkoli národní bezpečnost zůstává výlučnou odpovědností každého členského státu, KONSTATUJE, že je třeba posílit sdílení zpravodajských poznatků a informací a spolupráci mezi členskými státy, jakož i se střediskem EU INTCEN, aby bylo možné sdílet zpravodajské informace na začátku rozhodovacího procesu, a to též pokud jde o otázku přiřazování, a umožnit tak rychlou, účinnou a odůvodněnou reakci na nepřátelské činnosti v kyberprostoru zaměřené na EU a její partnery. OPAKUJE, že je důležité posílit kapacitu střediska EU INTCEN v kybernetické oblasti, a to na základě dobrovolných zpravodajských příspěvků členských států a aniž by byly dotčeny jejich pravomoci, a prozkoumat návrh na možné zřízení pracovní skupiny členských států pro kybernetickou zpravodajskou činnost.

25. UZNÁVAJÍC, že prohlášení a omezující opatření EU přijatá v rámci souboru nástrojů EU pro diplomacii v oblasti kybernetiky vyslala jasný signál, že nepřátelské činnosti v kyberprostoru, které představují vnější hrozbu pro EU, její členské státy a partnery, jsou nepřijatelné, a přispívají tak k předcházení nepřátelským činnostem v kyberprostoru, odrazování a odstrašování od těchto hrozeb a reakci na ně, ZNOVU OPAKUJE svůj závazek používat tato opatření s cílem připomenout povinnosti, které pro kyberprostor podle mezinárodního práva platí, včetně Charty OSN jako celku a podpory rámce OSN pro odpovědné chování států v kyberprostoru, jakož i povinnosti náležité péče pro všechny státy, aby nevědomě neumožnily, že jejich území bude využíváno pro mezinárodně protiprávní chování za využití informačních a komunikačních technologií, s cílem dále rozvíjet a prosazovat společný postoj EU k uplatňování mezinárodního práva v kyberprostoru. Berouc na vědomí, že vhodná a rychlá sdělení zmírňují rizika eskalace a mohou odrazovat útočníky, kteří se zaměřují na evropské zájmy, VYZÝVÁ vysokého představitele, aby vypracoval a předložil členským státům soudržnou komunikační strategii o využívání souboru nástrojů EU pro diplomacii v oblasti kybernetiky.

26. VYBÍZÍ k rozvoji postupného, cíleného a trvalého přístupu a reakcí na nepřátelské činnosti v kyberprostoru s využitím široké škály nástrojů poskytovaných souborem nástrojů EU pro diplomacii v oblasti kybernetiky, včetně režimu kybernetických sankcí EU, a k plánování doplňujících opatření. ZDŮRAZŇUJE, že je třeba zvýšit možnost v jednotlivých případech mobilizovat veškeré dostupné vnitřní i vnější nástroje k předcházení kybernetickým útokům, odrazování a odstrašování od těchto útoků a reakci na ně, a to prostřednictvím rychlého, účinného, postupného, cíleného a trvalého přístupu založeného na dlouhodobé strategické angažovanosti. VYZÝVÁ vysokého představitele, aby ve spolupráci s Komisí určil možné společné reakce EU na kybernetické útoky napříč spektrem, včetně možností sankcí, aby byla připravena přijmout v případě potřeby rychlá a účinná opatření, a předložil je Radě do konce prvního čtvrtletí 2023.

27. Berouc na vědomí, že odpovědnost za kybernetickou obranu nesou v první řadě členské státy, VYBÍZÍ je, aby dále rozvíjely své vlastní schopnosti provádět operace v oblasti kybernetické obrany, včetně proaktivních opatření s cílem chránit před kybernetickými útoky, odhalovat je, zabraňovat jim a odstrašovat od nich, a případně s cílem poskytovat podporu jiným členským státům a EU. Každý členský stát se vyzývá, aby podle potřeby posílil své vlastní schopnosti poskytovat a přijímat pomoc. ZDŮRAZŇUJE, že další rozvoj těchto schopností by měl být jedním z klíčových cílů nadcházející politiky EU v oblasti kybernetické obrany. KONSTATUJE, že politika EU v oblasti kybernetické obrany by měla více zohledňovat úlohu, kterou mohou hrát příslušné orgány a instituce EU při posilování spolupráce mezi příslušnými aktéry EU a členských států v oblasti kybernetické obrany a při rozvoji jejich vlastních schopností v souladu s jejich příslušnými mandáty. VYZÝVÁ vysokého představitele a Komisi, aby doplnili rozvoj kybernetické pozice EU tím, že v roce 2022 předloží ambiciózní návrh týkající se politiky EU v oblasti kybernetické obrany, který připraví půdu pro další rozvoj kybernetické pozice EU ze strany Rady.

28. ZDŮRAZŇUJE, že je třeba zvýšit interoperabilitu a sdílení informací prostřednictvím spolupráce mezi vojenskými skupinami pro reakci na počítačové hrozby (milCERT). VYZÝVÁ členské státy, aby na základě práce Evropské obranné agentury vytvořily síť milCERT s cílem rozvíjet spolupráci a usnadňovat výměnu informací, což by rovněž pomohlo posílit koordinaci s dalšími kybernetickými komunitami, jakož i sítí vojenských kybernetických velitelů za účelem posílení strategické spolupráce mezi kybernetickými veleními členských států EU nebo jinými odpovídajícími orgány. Zřízení těchto sítí spolu s projekty stálé strukturované spolupráce v oblasti kybernetické bezpečnosti by přispělo k posílení kybernetické obrany na úrovni EU. Zdůrazňuje význam spolupráce mezi navrhovanou sítí milCERT s již existující civilní sítí (CSIRT) s cílem posílit sdílení informací a zlepšit informovanost o situaci.

29. Na základě vojenské vize a strategie EU pro kyberprostor jako oblast operací a s ohledem na probíhající vývoj vojenské koncepce kybernetické obrany pro vojenské operace a mise vedené EU ZNOVU OPAKUJE, že je zapotřebí začlenit kybernetický rozměr do plánování a vedení misí a operací SBOP, mimo jiné posílením jejich kybernetických schopností, a ZDŮRAZŇUJE, že to přispěje k lepšímu povědomí o kybernetické situaci na úrovni EU.

30. Závěrem KONSTATUJE, že kybernetická pozice bude krokem k vytvoření doktríny EU pro činnost v kyberprostoru založené na posílené odolnosti, schopnostech a možnostech reakce, jakož i na společném postoji k uplatňování mezinárodního práva v kyberprostoru. Rada v roce 2023 ZHODNOTÍ pokrok dosažený při provádění těchto závěrů s cílem zajistit další rozvoj kybernetické pozice EU.