Rada
Európskej únie

V Bruseli 23. mája 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	

VÝSLEDOK ROKOVANIA

Od:	Generálny sekretariát Rady
Dátum:	23. mája 2022
Komu:	Delegácie
Predmet:	Závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti – závery Rady, ktoré Rada schválila na zasadnutí 23. mája 2022

Delegáciám v prílohe zasielame závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti, ktoré Rada schválila na zasadnutí 23. mája 2022.

PRÍLOHA

Závery Rady o vývoji prístupu Európskej únie ku kybernetickej bezpečnosti

RADA EURÓPSKEJ ÚNIE,

PRIPOMÍNAJÚC:

– závery o spoločnom oznámení Európskemu parlamentu a Rade z 25. júna 2013 s názvom Stratégia kybernetickej bezpečnosti Európskej únie: otvorený, bezpečný a chránený kybernetický priestor[1],

– politický rámec EÚ pre kybernetickú obranu[2],

– závery o správe internetu[3],

– závery o kybernetickej diplomacii[4],

– závery o posilnení európskeho systému kybernetickej odolnosti a podpore konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti[5],

– závery o spoločnom oznámení Európskemu parlamentu a Rade z 20. novembra 2017: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ[6],

– závery o rámci pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti („súbor kybernetických nástrojov“)[7],

– závery o koordinovanej reakcii EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu[8],

– závery o usmerneniach EÚ týkajúcich sa budovania vonkajších kybernetických kapacít[9],

---

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

– vykonávacie rozhodnutie Rady (EÚ) 2018/1993 z 11. decembra 2018 o dojednaniach EÚ o integrovanej politickej reakcii na krízu[10],

– závery o budovaní kapacít a spôsobilostí v oblasti kybernetickej bezpečnosti v EÚ[11],

– závery o význame 5G pre európske hospodárstvo a potrebe zmierniť bezpečnostné riziká spojené s 5G[12],

– závery o budúcnosti vysoko digitalizovanej Európy po roku 2020: „Zvýšenie digitálnej a hospodárskej konkurencieschopnosti v celej Únii a digitálna súdržnosť“[13],

– závery o komplementárnom úsilí zameranom na zvyšovanie odolnosti a boj proti hybridným hrozbám[14],

– závery o formovaní digitálnej budúcnosti Európy[15],

– závery o kybernetickej bezpečnosti pripojených zariadení[16],

– závery o stratégii kybernetickej bezpečnosti EÚ pre digitálnu dekádu[17],

– závery o bezpečnosti a obrane[18],

– závery o preskúmaní potenciálu iniciatívy na zriadenie spoločnej kybernetickej jednotky, ktorou sa dopĺňa koordinovaná reakcia EÚ na kybernetickobezpečnostné incidenty a krízy veľkého rozsahu[19],

– Strategický kompas pre bezpečnosť a obranu – za Európsku úniu, ktorá chráni svojich občanov, hodnoty a záujmy a prispieva k medzinárodnému mieru a bezpečnosti[20],

---

10 Ú. v. EÚ L 320, 17.12.2018, s. 28 – 34.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. ZDÔRAZŇUJE, že škodlivé správanie v kybernetickom priestore, ktorého sa dopúšťajú štátne aj neštátne subjekty, sa v posledných rokoch zintenzívnilo vrátane prudkého a neustáleho nárastu škodlivých činností zameraných na kritickú infraštruktúru, dodávateľské reťazce a duševné vlastníctvo EÚ a jej členských štátov, zvýšeného rizika účinkov presahovania, ako aj nárastu ransomvérových útokov na naše podniky, organizácie a občanov. KONŠTATUJE, že s návratom mocenskej politiky sa niektoré krajiny čoraz viac snažia spochybňovať a narušovať v kybernetickom priestore medzinárodný poriadok založený na pravidlách, čo spôsobuje, že kybernetická sféra spolu so širym morom, vzdušným priestorom a kozmickým priestorom sú doménami, ktoré sú čoraz častejšie predmetom sporov. UZNÁVA, že rozsiahle kybernetické útoky alebo pokusy, ktoré sa zameriavajú na narušenie alebo zničenie sietí a informačných systémov, ako aj vniknutie do nich, a majú systémové účinky, sa stali bežnejšími, mohli by ohroziť našu hospodársku bezpečnosť a ovplyvniť naše demokratické inštitúcie a procesy a svedčia o pripravenosti niektorých aktérov ohroziť medzinárodnú bezpečnosť a stabilitu. ZDÔRAZŇUJE, že vojenská agresia Ruska voči Ukrajine ukázala, že ofenzívna kybernetická činnosť sa môže vykonávať ako neoddeliteľná súčasť hybridných stratégií kombinujúcich zastrašovanie, destabilizáciu a narušenie hospodárstva.

2. OPÄTOVNE ZDÔRAZŇUJE, že vzhľadom na súčasné geopolitické zmeny sila našej Únie spočíva v jednote, solidarite a odhodlaní a že vykonávaním Strategického kompasu sa posilní strategická autonómia EÚ a jej schopnosť spolupracovať s partnermi na ochrane jej hodnôt a záujmov, a to aj v kybernetickej oblasti. ZDÔRAZŇUJE, že silnejšia a schopnejšia EÚ v oblasti bezpečnosti a obrany pozitívne prispeje aj ku globálnej a transatlantickej bezpečnosti a je doplnkom k NATO, ktoré zostáva základom kolektívnej obrany jeho členov. OPÄTOVNE POTVRDZUJE zámer EÚ zintenzívniť podporu medzinárodného poriadku založeného na pravidlách, ktorého jadrom je Organizácia Spojených národov.

3. V súlade so závermi Rady o stratégii kybernetickej bezpečnosti EÚ a so Strategickým kompasom OPÄTOVNE ZDÔRAZŇUJE potrebu rozvíjať prístup Únie ku kybernetickej bezpečnosti posilňovaním našej schopnosti predchádzať kybernetickým útokom prostredníctvom budovania kapacít, rozvoja spôsobilostí, výcviku, cvičení, zvýšenej odolnosti a dôslednej reakcie na kybernetické útoky proti EÚ a jej členským štátom, pričom využijeme všetky dostupné nástroje EÚ. To zahŕňa, aby EÚ naďalej preukazovala svoje odhodlanie k okamžitej a dlhodobej reakcii voči aktérom hrozieb, ktorí sa snažia nám brániť v bezpečnom a otvorenom prístupe do kybernetického priestoru a ovplyvňovať naše strategické záujmy vrátane bezpečnosti našich partnerov. V tejto súvislosti ZDÔRAZŇUJE, že cieľom prístupu ku kybernetickej bezpečnosti je kombinovať rôzne iniciatívy, ktoré prispievajú k opatreniam EÚ na upevnenie mieru a stability v kybernetickom priestore a v prospech otvoreného, slobodného, globálneho, stabilného a bezpečného kybernetického priestoru, a zároveň lepšie koordinovať krátkodobé, strednodobé a dlhodobé opatrenia na predchádzanie kybernetickým hrozbám a útokom, odrádzanie od nich a reakciu na ne a využívať kybernetické spôsobilosti. ZDÔRAZŇUJE, že tieto prvky by sa mali začleniť do prístupu EÚ ku kybernetickej bezpečnosti v súlade s piatimi funkciami EÚ v kybernetickej oblasti: posilňovanie našej kybernetickej odolnosti a kapacity na ochranu; posilňovanie solidárneho a komplexného krízového riadenia; presadzovanie našej vízie kybernetického priestoru; posilňovanie spolupráce s partnerskými krajinami a medzinárodnými organizáciami; predchádzanie kybernetickým útokom, obrana proti nim a reakcia na ne.

I. POSILŇOVANIE NAŠEJ KYBERNETICKEJ ODOLNOSTI A KAPACITY NA OCHRANU

4. OPÄTOVNE ZDÔRAZŇUJE potrebu zvýšiť celkovú úroveň kybernetickej bezpečnosti EÚ, SO ZÁUJMOM OČAKÁVA rýchle prijatie návrhu smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (smernica NIS), návrhu nariadenia o digitálnej prevádzkovej odolnosti finančného sektora (nariadenie DORA), návrhu smernice o odolnosti kritických subjektov (smernica CER) a BERIE NA VEDOMIE návrh nariadenia, ktorým sa stanovujú opatrenia na zabezpečenie vysokej úrovne kybernetickej bezpečnosti v inštitúciách, orgánoch, úradoch a agentúrach Únie, s cieľom podporiť Európsku úniu, ktorá chráni svojich občanov, verejné služby a podniky v kybernetickom priestore. NABÁDA Komisiu, aby dokončila prijatie kľúčových návrhov v záujme zabezpečenia toho, aby digitálne infraštruktúry, technológie, produkty a služby boli zabezpečené, s cieľom vyslať jasný signál o ambíciách EÚ v týchto oblastiach a umožniť podporu pre spoločnosti, aby tejto výzve mohli čeliť. VYZÝVA Komisiu, aby navrhla spoločné požiadavky EÚ na kybernetickú bezpečnosť, pokiaľ ide o pripojené zariadenia, a súvisiace procesy a služby, prostredníctvom aktu o kybernetickej odolnosti, ktorý by mala navrhnúť do konca roka 2022, pričom je potrebné, aby zohľadnila potrebu horizontálneho a holistického prístupu, ktorý sa vzťahuje na celý životný cyklus digitálnych produktov, ako aj existujúcu reguláciu, najmä v oblasti kybernetickej bezpečnosti.

5. VYZÝVA príslušné orgány, ako je Orgán európskych regulátorov pre elektronické komunikácie (BEREC), Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) a skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti (NIS), aby spolu s Európskou komisiou na základe posúdenia rizika vypracovali odporúčania pre členské štáty a Európsku komisiu s cieľom posilniť odolnosť komunikačných sietí a infraštruktúr v rámci Európskej únie vrátane pokračujúceho vykonávania súboru nástrojov EÚ pre 5G.

6. VYZÝVA EÚ a jej členské štáty, aby zintenzívnili úsilie o zvýšenie celkovej úrovne kybernetickej bezpečnosti, napríklad uľahčením vzniku dôveryhodných poskytovateľov služieb v oblasti kybernetickej bezpečnosti, a ZDÔRAZŇUJE, že podpora rozvoja takýchto poskytovateľov by mala byť prioritou priemyselnej politiky EÚ v oblasti kybernetickej bezpečnosti. S cieľom lepšie odolávať kybernetickým útokom s možnými systémovými účinkami a bojovať proti nim a na základe ponaučení z riešenia zraniteľností, pokiaľ ide o softvér Solarwinds, Microsoft Exchange a Apache Log4J, VYZÝVA Komisiu, aby navrhla možnosti, ako podporiť vznik dôveryhodného odvetvia služieb v oblasti kybernetickej bezpečnosti, posilniť kybernetickú bezpečnosť dodávateľského reťazca IKT, riešiť potenciálne účinky zraniteľností softvéru na EÚ a jej členské štáty, a to aj vzhľadom na pripravovaný akt o kybernetickej odolnosti, a zlepšiť spôsobilosti odhaľovania kybernetických hrozieb a výmeny informácií o nich v členských štátoch a medzi nimi.

7. PRIPOMÍNA, že investície do inovácie a lepšie využívanie civilných technológií sú kľúčom k posilneniu našej technologickej suverenity, a to aj v kybernetickej oblasti, VYZÝVA Komisiu, aby urýchlene uviedla do prevádzky Európske centrum kompetencií v oblasti kybernetickej bezpečnosti s cieľom vytvoriť silný európsky kybernetický výskum, ako aj priemyselný a technologický ekosystém, ZDÔRAZŇUJE, že je potrebné posilniť výskum a inováciu, viac investovať do civilnej a obrannej oblasti s cieľom posilniť obrannú technologickú a priemyselnú základňu EÚ (EDTIB) a rozvíjať kybernetické spôsobilosti EÚ a jej členských štátov vrátane strategických podporných spôsobilostí. ZDÔRAZŇUJE, že je dôležité intenzívne využívať nové technológie, najmä kvantovú výpočtovú techniku, umelú inteligenciu a veľké dáta, s cieľom dosiahnuť komparatívne výhody, a to aj pokiaľ ide o operácie reagujúce na kybernetické incidenty.

8. UZNÁVA, že posilnenie našej kybernetickej bezpečnosti je spôsobom, ako zvýšiť účinnosť a bezpečnosť nášho úsilia na pevnine, vo vzduchu, na mori a vo vesmíre, ZDÔRAZŇUJE, že je dôležité začleniť aspekty kybernetickej bezpečnosti do všetkých verejných politík EÚ vrátane odvetvových právnych predpisov dopĺňajúcich smernicu NIS 2, a VYZÝVA Komisiu, aby preskúmala možnosti zvýšenia kybernetickej bezpečnosti v celom dodávateľskom reťazci obrannej technologickej a priemyselnej základne EÚ (EDTIB).

9. UZNÁVA, že zabezpečenie primeraných finančných a ľudských zdrojov pre kybernetickú bezpečnosť a opatrenia zamerané na vytvorenie priaznivého prostredia pre konkurencieschopnosť súkromného sektora sú nevyhnutné, pokiaľ ide o rozvoj prístupu EÚ ku kybernetickej bezpečnosti, a že otázka stabilného a dlhodobého financovania kybernetickej bezpečnosti by sa mala riešiť aj na úrovni EÚ navrhnutím a vykonávaním horizontálneho mechanizmu kombinujúceho viaceré zdroje financovania vrátane nákladov na vysokokvalifikované ľudské zdroje. Preto VYZÝVA Komisiu, aby do konca roka 2022 preskúmala možnosti takéhoto mechanizmu, aby sa o nich mohlo rokovať v príslušných orgánoch Rady.

10. ZDÔRAZŇUJE, že je potrebné posilniť naše úsilie a zintenzívniť spoluprácu v boji proti medzinárodnej počítačovej kriminalite, najmä ransomvéru, prostredníctvom mechanizmu EMPACT (Európska multidisciplinárna platforma proti hrozbám trestnej činnosti), výmen medzi sektorom kybernetickej bezpečnosti, presadzovania práva a diplomatickým sektorom a prostredníctvom posilnenia spôsobilostí v oblasti presadzovania práva pri vyšetrovaní a stíhaní počítačovej kriminality. OPÄTOVNE ZDÔRAZŇUJE svoj záväzok informovať verejnosť o kybernetických hrozbách a opatreniach prijatých na vnútroštátnej úrovni a na úrovni EÚ proti týmto hrozbám zapojením občianskej spoločnosti, súkromného sektora a akademickej obce s cieľom zvýšiť informovanosť a podporiť primeranú úroveň kybernetickej ochrany a kybernetickej hygieny. ZDÔRAZŇUJE, že je potrebné zamerať sa na zručnosti a schopnosti občanov v oblasti kybernetickej bezpečnosti na úrovni EÚ a členských štátov, ako aj aktívne zapájať používateľov do ich vlastnej ochrany.

II. POSILŇOVANIE SOLIDÁRNEHO A KOMPLEXNÉHO KRÍZOVÉHO RIADENIA

11. Na základe každoročných kybernetických cvičení, iných cvičení zahŕňajúcich kybernetický rozmer a cvičenia EU CyCLES v roku 2022 ZDÔRAZŇUJE, že je dôležité vytvoriť program pravidelných kybernetických cvičení medzi komunitami a na viacerých úrovniach s cieľom za účasti Rady, ESVČ, Komisie a príslušných zainteresovaných strán, ako sú napríklad ENISA a súkromný sektor, testovať a rozvíjať vnútornú a vonkajšiu reakciu EÚ na rozsiahle kybernetické incidenty, ktorý bude prepojený so všeobecnou politikou EÚ v oblasti cvičení a bude k nej prispievať. ZDÔRAZŇUJE význam ďalšieho rozvoja cvičení Cyber Europe a BlueOLEx, v ktorých sa kombinuje reakcia na rôznych úrovniach. UZNÁVA, že je potrebné vyhodnotiť a konsolidovať existujúce cvičenia a preskúmať možnosť ďalších cvičení v súvislosti s konkrétnymi segmentmi kybernetickej oblasti, najmä vojenské cvičenie CERT a cvičenie zamerané na krízovú spoluprácu medzi inštitúciami, orgánmi a agentúrami EÚ. UZNÁVA, že prístup Únie ku kybernetickej bezpečnosti posilní našu schopnosť predchádzať kybernetickým útokom prostredníctvom rôznych opatrení vrátane odbornej prípravy, a preto VYZÝVA členské štáty, aby posilnili civilno-vojenskú spoluprácu v oblasti kybernetickej odbornej prípravy a v rámci spoločných cvičení.

12. ZDÔRAZŇUJE, že je potrebné ďalej testovať a posilňovať operačnú spoluprácu a spoločnú situačnú informovanosť medzi členskými štátmi, a to aj prostredníctvom zavedených sietí, ako je napríklad sieť jednotiek CSIRT a sieť styčných organizácií pre kybernetické krízy (EU-CyCLONe), s cieľom zlepšiť pripravenosť EÚ čeliť rozsiahlym kybernetickým incidentom. ZDÔRAZŇUJE, že je dôležité pracovať na vytvorení spoločného jazyka medzi členskými štátmi a s inštitúciami, orgánmi a agentúrami EÚ, ktorý bude prispôsobený diskusiám na politickej úrovni, s cieľom podporiť vypracovanie konsolidovaného posúdenia závažnosti a vplyvu relevantných kybernetických incidentov, ako aj možných scenárov vývoja a prípadných potrieb, ktoré z nich vyplývajú. ZDÔRAZŇUJE v tejto súvislosti potrebu zlepšiť komplementárnosť spoločných správ o situačnom hodnotení vrátane správ siete EU-CyCLONe o vplyve a závažnosti rozsiahlych kybernetických incidentov v členských štátoch EÚ a posúdení hrozieb, ktoré poskytuje Spravodajské a situačné centrum EÚ (EU INTCEN) v rámci súboru nástrojov kybernetickej diplomacie EÚ. VYZÝVA Komisiu, vysokého predstaviteľa a skupinu pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, aby v koordinácii s príslušnými civilnými a vojenskými orgánmi a agentúrami a existujúcimi sieťami vrátane siete EU-CyCLONe vykonali do konca roka 2022 hodnotenie rizík a vypracovali scenáre rizík z hľadiska kybernetickej bezpečnosti v situácii hrozby alebo možného útoku voči členským štátom alebo partnerským krajinám a predložili ich príslušným orgánom Rady. ZDÔRAZŇUJE potrebu primeranej a koordinovanej verejnej komunikácie o reakcii EÚ na rozsiahle kybernetické incidenty.

13. V prípade rozsiahleho kybernetického incidentu ZDÔRAZŇUJE potrebu posilniť koordináciu a v prípade potreby vychádzať z dosiahnutého pokroku a práce tímov rýchlej kybernetickej reakcie v rámci PESCO a čerpať z práce siete jednotiek CSIRT a siete EU-CyCLONe, z dobrovoľného združovania našich kapacít reakcie na incidenty medzi členskými štátmi. UZNÁVA, že rozvoj vzťahov so súkromným sektorom by mohol posilniť verejné kapacity, najmä v súvislosti s nedostatkom zručností v celej EÚ, a že identifikácia a koordinácia týchto súkromných partnerov by mohla mať zásadný vplyv v prípade rozsiahlych incidentov. V záujme zabezpečenia pripravenosti čeliť rozsiahlym kybernetickým incidentom VYZÝVA Komisiu, aby do konca tretieho štvrťroka 2022 predložila návrh nového Fondu pre reakcie na núdzové situácie v oblasti kybernetickej bezpečnosti.

14. V súlade so Strategickým kompasom OPÄTOVNE POTVRDZUJE, že je potrebné naďalej investovať do našej vzájomnej pomoci podľa článku 42 ods. 7 Zmluvy o Európskej únii, ako aj do solidarity podľa článku 222 Zmluvy o fungovaní Európskej únie, a to najmä prostredníctvom častých cvičení. V tejto súvislosti ZDÔRAZŇUJE, že je potrebné ďalej pracovať na poskytovaní a koordinácii dvojstrannej civilnej a/alebo vojenskej podpory, a to aj preskúmaním možnej podpory, ktorú EÚ poskytuje na výslovnú žiadosť členských štátov, a na určení vhodných opatrení reakcie, a to aj prostredníctvom rozvoja koordinovanej komunikačnej stratégie v kontexte vykonávania článku 42 ods. 7. KONŠTATUJE, že by to malo zahŕňať aj preskúmanie prepojení s existujúcimi mechanizmami EÚ v oblasti krízového riadenia a mechanizmom EÚ v oblasti civilnej ochrany

15. ZDÔRAZŇUJE, že posilnený prístup EÚ ku kybernetickej bezpečnosti si bude vyžadovať bezpečné komunikačné prostriedky na vyššej úrovni. Na tento účel OPÄTOVNE POTVRDZUJE usmernenia, ktoré sa v tejto súvislosti stanovujú v Strategickom kompase, a VYZÝVA Komisiu a ďalšie príslušné inštitúcie, orgány a agentúry, aby do konca roka 2022 zmapovali existujúce nástroje na bezpečnú komunikáciu v kybernetickej oblasti, o ktorých sa má rokovať v príslušných orgánoch Rady a s príslušnými skupinami pre spoluprácu, ako je napríklad sieť jednotiek CSIRT a sieť EU-CyCLONe.

III. PRESADZOVANIE NAŠEJ VÍZIE KYBERNETICKÉHO PRIESTORU

16. PRIPOMÍNA, že cieľom spoločného a komplexného prístupu EÚ ku kybernetickej diplomacii je prispievať k predchádzaniu konfliktom, zmierňovaniu kybernetických hrozieb a väčšej stabilite v medzinárodných vzťahoch. V tejto súvislosti OPÄTOVNE POTVRDZUJE záväzok EÚ urovnávať medzinárodné spory v kybernetickom priestore mierovými prostriedkami a uplatňovať medzinárodné právo vrátane medzinárodného práva v oblasti ľudských práv a medzinárodného humanitárneho práva na činnosti štátov v kybernetickom priestore. ZDÔRAZŇUJE záväzok EÚ a jej členských štátov konať v súlade s dobrovoľnými, nezáväznými normami týkajúcimi sa zodpovedného správania štátov v kybernetickom priestore, na ktorých sa dohodli všetky členské štáty OSN. ZDÔRAZŇUJE význam otvoreného, slobodného, globálneho, stabilného a bezpečného kybernetického priestoru, v ktorom sa v plnej miere uplatňujú ľudské práva, základné slobody a zásady právneho štátu v záujme podpory sociálneho blahobytu, hospodárskeho rastu, prosperity a integrity našich slobodných a demokratických spoločností, a OPÄTOVNE POTVRDZUJE záväzok EÚ a jej členských štátov naďalej presadzovať tieto hodnoty a zásady. V záujme rozvoja kanálov pre konštruktívny, úprimný a otvorený dialóg s kľúčovými zainteresovanými stranami v kybernetickom priestore ZDÔRAZŇUJE, že je dôležité, aby sa kybernetické otázky vrátane súboru nástrojov kybernetickej diplomacie EÚ stali neoddeliteľnou súčasťou prístupových rokovaní Únie a strategických a politických dialógov EÚ s medzinárodnými partnermi, ako a konkurentmi, a zároveň VYZÝVA vysokého predstaviteľa, aby preskúmal existujúce dvojstranné kybernetické dialógy a v prípade potreby navrhol nadviazanie podobnej spolupráce s ďalšími krajinami alebo príslušnými medzinárodnými organizáciami.

17. PRIPOMÍNA význam spolupráce viacerých zainteresovaných strán, keďže za kybernetickú bezpečnosť nesú zodpovednosť aj iné zainteresované strany, najmä pokiaľ ide o vykonávanie odporúčaní a rozhodnutí prijatých na medzinárodných a regionálnych fórach. VYZÝVA EÚ a jej členské štáty, aby naďalej presadzovali náš model kybernetického priestoru a internetu založený na prístupe viacerých zainteresovaných strán a prostredníctvom iniciatív, ako je napríklad Parížska výzva na dôveru a bezpečnosť v kybernetickom priestore a Vyhlásenie o budúcnosti internetu, zdôrazňovaním spoločných prínosov stability v kybernetickom priestore a zvyšovaním globálneho povedomia o nebezpečenstvách vízie internetu, ktorá sa sústreďuje na štát a ktorá je autoritárska, a VYZÝVA EÚ a jej členské štáty, aby naďalej posilňovali spoluprácu s komunitou viacerých zainteresovaných strán, a to aj využívaním príslušných projektov, ako je napríklad iniciatíva kybernetickej diplomacie EÚ v rámci nástroja zahraničnej politiky EÚ.

18. ZAVÄZUJE SA, že sa bude naďalej zapájať do činností príslušných medzinárodných organizácií, najmä do procesov súvisiacich s prvým a tretím výborom OSN, a zároveň zdôrazňuje, že v kybernetickom priestore a v súvislosti s ním sa bez výhrad uplatňuje platné medzinárodné právo. VYZDVIHUJE význam pokračujúceho úsilia o zachovanie a podporu rámca OSN pre zodpovedné správanie štátov a ZDÔRAZŇUJE, že EÚ a jej členské štáty budú aktívne pracovať na posilňovaní jeho vykonávania, a to aj prostredníctvom vytvorenia akčného programu na posilňovanie zodpovedného správania štátov v kybernetickom priestore. ZDÔRAZŇUJE, že EÚ a jej členské štáty sa budú aktívne zapájať do rokovaní o budúcom dohovore OSN, ktorý bude slúžiť ako účinný nástroj pre orgány presadzovania práva a justičné orgány v celosvetovom boji proti počítačovej kriminalite, pričom v plnej miere zohľadnia existujúci rámec medzinárodných a regionálnych nástrojov v tejto oblasti, najmä budapeštiansky Dohovor o počítačovej kriminalite. ZDÔRAZŇUJE, že je dôležité naďalej podporovať rozvoj a vykonávanie opatrení na budovanie dôvery na regionálnej a medzinárodnej úrovni a ďalej nabádať na využívanie existujúcich opatrení na budovanie dôvery v kybernetickej oblasti v rámci OBSE, a to aj v čase medzinárodného napätia.

19. PRIPOMÍNA, že proaktívny prístup k zabezpečeniu medzinárodných noriem v oblasti vznikajúcich technológií a základnej internetovej architektúry v súlade s demokratickými hodnotami a zásadami, ktorý sa zakladá na ľudských právach, je nevyhnutný na zabezpečenie toho, aby internet zostal globálny, nefragmentovaný a otvorený, a PODPORUJE zásadu, podľa ktorej používanie a vývoj technológií rešpektuje ľudské práva, je zamerané na človeka, na súkromie a ich používanie je zákonné, bezpečné a etické. NABÁDA vysokého predstaviteľa a Komisiu, aby vypracovali strategickú víziu technických otázok v digitálnej oblasti, ktoré majú vplyv na zahraničnú politiku a mohli by mať vplyv najmä na stabilitu kybernetického priestoru a internetu, a to aj v príslušných špecializovaných medzinárodných organizáciách (Medzinárodná telekomunikačná únia atď.).

IV. POSILŇOVANIE SPOLUPRÁCE S PARTNERSKÝMI KRAJINAMI A MEDZINÁRODNÝMI ORGANIZÁCIAMI

20. ZDÔRAZŇUJE, že je potrebné lepšie prepojiť stratégiu EÚ v oblasti budovania kybernetických kapacít s normami OSN týkajúcimi sa zodpovedného správania štátov v kybernetickom priestore, a to aj vypracovaním prispôsobených programov spolupráce a budovania kapacít s cieľom podporiť tretie štáty v ich úsilí o vykonávanie, a pokračovať tak v našom úsilí o podporu akčného programu OSN na posilňovanie zodpovedného správania štátov v kybernetickom priestore a toto úsilie rozširovať. ZDÔRAZŇUJE, že je dôležité, aby sa budovanie kybernetických kapacít v plnej miere integrovalo ako súčasť ponuky EÚ ako poskytovateľa bezpečnosti, a to s primeranou koordináciou úsilia medzi členskými štátmi a inštitúciami, orgánmi a agentúrami EÚ, a predovšetkým VÍTA spoluprácu medzi členskými štátmi, ako aj s partnermi z verejného a súkromného sektora, najmä prostredníctvom siete EU CyberNet (sieť EÚ na budovanie kybernetických kapacít) a Globálneho fóra o kybernetických odborných znalostiach (GFCE), s cieľom zabezpečiť koordináciu a zabrániť duplicite.

VYZÝVA vysokého predstaviteľa a Komisiu, aby do tretieho štvrťroka 2022 zriadili *radu pre budovanie kybernetických kapacít* a uskutočňovali pravidelné výmeny v rámci horizontálnej pracovnej skupiny pre kybernetické otázky. VYZÝVA Komisiu a vysokého predstaviteľa, aby ďalej mobilizovali Nástroj susedstva a rozvojovej a medzinárodnej spolupráce (NDICI), nástroj predvstupovej pomoci (IPA III) a ďalšie finančné nástroje, ako je napríklad Európsky mierový nástroj (EPF) a iniciatíva *Global Gateway*, s cieľom podporiť posilnenie odolnosti

našich partnerov, ich kapacitu na identifikáciu a riešenie kybernetických hrozieb a na vyšetrovanie a stíhanie počítačovej kriminality, ako aj rozvoj projektov spolupráce, a to aj v kontexte krízy, pričom predovšetkým NABÁDA na spoluprácu s partnermi na západnom Balkáne a v krajinách východného a južného susedstva EÚ a na vysielanie expertov EÚ a členských štátov na účely poskytovania podpory v prípade kybernetických kríz, a to pri zohľadnení existujúcich právnych mandátov.

21. ZDÔRAZŇUJE, že je potrebné zintenzívniť úsilie o vypracovanie štruktúrovaného a otvoreného prístupu EÚ zameraného na to, ako podporiť globálne spoločné chápanie uplatňovania medzinárodného práva v kybernetickom priestore, rámca OSN pre zodpovedné správanie štátov v kybernetickom priestore vrátane iniciatívy pre akčný program na posilňovanie zodpovedného správania štátov v kybernetickom priestore, ako aj pozície EÚ a jej členských štátov v prebiehajúcich rokovaniach o Dohovore OSN o počítačovej kriminalite, a v rámci tohto úsilia ŽIADA vysokého predstaviteľa, aby do konca roka 2022 predložil Rade informačný plán. NABÁDA vysokého predstaviteľa a útvary Komisie, aby v plnom rozsahu a systematicky využívali 145 delegácií a rozvíjali pravidelnú a plodnú spoluprácu medzi nimi a veľvyslanectvami členských štátov v tretích krajinách pod záštitou plánovanej siete kybernetickej diplomacie EÚ. VYZÝVA vysokého predstaviteľa, aby do tretieho štvrťroka 2022 zriadil sieť kybernetickej diplomacie EÚ, ktorou sa prispeje k výmene informácií, spoločným činnostiam odbornej prípravy pre personál EÚ a členských štátov, jednotnému úsiliu o budovanie kapacít a posilneniu vykonávania rámca OSN pre zodpovedné správanie štátov, ako aj k opatreniam na budovanie dôvery medzi štátmi.

22. ZDÔRAZŇUJE svoj záväzok ďalej spolupracovať s medzinárodnými organizáciami a partnerskými krajinami s cieľom dosiahnuť pokrok v spoločnom chápaní panorámy kybernetických hrozieb, rozvíjať mechanizmy spolupráce a proaktívne identifikovať kooperatívne diplomatické reakcie. PRIPOMÍNAJÚC kľúčové úspechy spolupráce medzi EÚ a NATO v oblasti kybernetickej bezpečnosti v rámci vykonávania spoločného vyhlásenia z Varšavy z roku 2016 a z Bruselu z roku 2018, pri plnom rešpektovaní rozhodovacej autonómie a postupov oboch organizácií a na základe zásad transparentnosti, reciprocity a inkluzívnosti, ZDÔRAZŇUJE, že je potrebné naďalej posilňovať spoluprácu s NATO v kybernetickej oblasti prostredníctvom cvičení, spoločného využívania a výmeny informácií medzi odborníkmi, a to aj o rozvoji spôsobilostí, budovaní kapacít pre partnerov, misie a operácie, ako aj o uplatniteľnosti medzinárodného práva a noriem OSN týkajúcich sa zodpovedného správania štátov v kybernetickom priestore, a posilňovať prípadnú koordinovanú reakciu na škodlivé kybernetické činnosti.

V. PREDCHÁDZANIE KYBERNETICKÝM ÚTOKOM, OBRANA PROTI NIM A REAKCIA NA NE

23. UZNÁVA, že kybernetický priestor sa stal arénou pre geopolitické súperenie, a preto OPÄTOVNE ZDÔRAZŇUJE, že EÚ musí byť schopná rýchlo a rázne reagovať na kybernetické útoky, ako sú napríklad štátom podporované škodlivé kybernetické činnosti zamerané na EÚ a jej členské štáty, a preto musí posilniť súbor nástrojov kybernetickej diplomacie EÚ a plne využívať všetky jeho nástroje vrátane dostupných politických, hospodárskych, diplomatických a právnych nástrojov a nástrojov strategickej komunikácie s cieľom predchádzať škodlivým kybernetickým činnostiam, odrádzať od nich a reagovať na ne. ZDÔRAZŇUJE, že nepriateľskí aktéri si musia byť vedomí toho, že kybernetické útoky proti členským štátom a inštitúciám EÚ sa odhalia včas, rýchlo sa identifikujú a reagovať sa na ne bude všetkými potrebnými nástrojmi a politikami. VYZÝVA členské štáty a vysokého predstaviteľa, aby s podporou Komisie do konca prvého štvrťroka 2023 vypracovali revidovanú verziu vykonávacích usmernení k súboru nástrojov kybernetickej diplomacie EÚ, a to najmä preskúmaním ďalších opatrení v oblasti reakcie, a vychádzali pri tom najmä z prvkov, ktoré obsahuje prístup ku kybernetickej bezpečnosti, a zo skúseností získaných z vykonávania súboru nástrojov kybernetickej diplomacie od jeho vzniku a z cvičení EU CyCLES.

24. ZDÔRAZŇUJE, že je potrebné v príslušných orgánoch a výboroch Rady pravidelne uskutočňovať výmenu informácií o panoráme kybernetických hrozieb a zároveň pravidelne spolupracovať so súkromným sektorom a vychádzať z posúdenia vplyvu a závažnosti nedávnych incidentov, zvyšovať celkovú informovanosť a pripravenosť na ďalšie aplikácie súboru nástrojov kybernetickej diplomacie EÚ a vyvinúť ďalšie nástroje na podporu jeho vykonávania. Hoci národná bezpečnosť zostáva vo výlučnej zodpovednosti každého členského štátu, KONŠTATUJE, že je potrebné posilniť výmenu informácií a spravodajských informácií a spoluprácu medzi členskými štátmi, ako aj s centrom EU INTCEN, aby bolo možné vymieňať si spravodajské informácie na začiatku rozhodovacieho procesu, a to aj pokiaľ ide o otázku pripisovania zodpovednosti, a tým umožniť rýchlu, účinnú a odôvodnenú reakciu na škodlivé kybernetické činnosti zamerané na EÚ a jej partnerov. OPÄTOVNE ZDÔRAZŇUJE, že je dôležité posilniť kapacitu centra EU INTCEN v kybernetickej oblasti, a to na základe dobrovoľných spravodajských príspevkov členských štátov a bez toho, aby boli dotknuté ich právomoci, a preskúmať návrh o možnom zriadení pracovnej skupiny členských štátov pre kybernetické spravodajstvo.

25. UZNÁVA, že vyhlásenia a reštriktívne opatrenia EÚ prijaté v rámci súboru nástrojov kybernetickej diplomacie EÚ vyslali jasný signál, že škodlivé kybernetické činnosti, ktoré predstavujú vonkajšiu hrozbu pre EÚ, jej členské štáty a partnerov, sú neprijateľné, a tým prispievajú k predchádzaniu škodlivým kybernetickým činnostiam, odrádzaniu od nich a reakcii na ne, a OPÄTOVNE POTVRDZUJE svoj záväzok využívať tieto opatrenia s cieľom pripomenúť záväzky, ktoré sa na kybernetický priestor vzťahujú podľa medzinárodného práva vrátane Charty OSN v celom rozsahu, a posilňovať rámec OSN pre zodpovedné správanie štátov v kybernetickom priestore vrátane povinnosti náležitej starostlivosti pre všetky štáty na účely zabránenia tomu, aby nevedome umožňovali, aby sa ich územie využívalo na páchanie medzinárodných protiprávnych činov prostredníctvom informačných a komunikačných technológií, v záujme ďalšieho rozvoja a podpory spoločnej pozície EÚ týkajúcej sa uplatňovania medzinárodného práva v kybernetickom priestore. Poukazujúc na to, že vhodné a rýchle správy zmierňujú riziká eskalácie a môžu odrádzať útočníkov, ktorí sa zameriavajú na európske záujmy, VYZÝVA vysokého predstaviteľa, aby vypracoval koherentnú komunikačnú stratégiu o používaní súboru nástrojov kybernetickej diplomacie EÚ a predložil ju členským štátom.

26. NABÁDA na rozvoj postupných, cielených a trvalých prístupov k škodlivým kybernetickým činnostiam a reakcie na ne, a to pri využití širokej škály nástrojov, ktoré poskytuje súbor nástrojov kybernetickej diplomacie EÚ vrátane režimu kybernetických sankcií EÚ, a na stanovenie ďalších opatrení. ZDÔRAZŇUJE, že je potrebné zlepšiť možnosť v jednotlivých prípadoch mobilizovať všetky dostupné vnútorné aj vonkajšie nástroje s cieľom predchádzať kybernetickým útokom, odrádzať od nich a reagovať na ne, a to rýchlym, účinným, postupným, cieleným a trvalým prístupom založeným na dlhodobej strategickej angažovanosti. VYZÝVA vysokého predstaviteľa, aby v spolupráci s Komisiou identifikoval v celom spektre možné spoločné reakcie EÚ na kybernetické útoky vrátane možností sankcií, aby boli v prípade potreby pripravené na prijatie rýchle a účinné opatrenia, a predložil ich Rade do konca prvého štvrťroka 2023.

27. Berúc na vedomie, že kybernetická obrana je primárne zodpovednosťou členských štátov, NABÁDA členské štáty, aby ďalej rozvíjali svoje vlastné spôsobilosti na vykonávanie operácií kybernetickej obrany vrátane proaktívnych opatrení s cieľom chrániť sa pred kybernetickými útokmi, odhaľovať ich, ubrániť sa im a odrádzať od nich a prípadne na podporu iných členských štátov a EÚ. Každý členský štát sa nabáda k tomu, aby podľa potreby posilnil svoje vlastné schopnosti poskytovať a prijímať pomoc a podporu. ZDÔRAZŇUJE, že ďalší rozvoj týchto spôsobilosti by mal byť jedným z kľúčových cieľov nadchádzajúcej politiky EÚ v oblasti kybernetickej obrany. KONŠTATUJE, že v rámci politiky EÚ v oblasti kybernetickej obrany by sa mala väčšia pozornosť venovať tomu, akú úlohu môžu príslušné inštitúcie a orgány EÚ v súlade so svojimi príslušnými mandátmi zohrávať pri zintenzívňovaní spolupráce medzi príslušnými aktérmi EÚ a členských štátov v oblasti kybernetickej obrany a pri vytváraní ich vlastných kapacít. VYZÝVA vysokého predstaviteľa, aby spolu s Komisiou doplnil rozvoj prístupu EÚ ku kybernetickej bezpečnosti tým, že v roku 2022 predloží ambiciózny návrh týkajúci sa politiky EÚ v oblasti kybernetickej obrany, ktorým sa pripraví pôda pre ďalší rozvoj prístupu EÚ ku kybernetickej bezpečnosti zo strany Rady.

28. ZDÔRAZŇUJE, že je potrebné zlepšiť interoperabilitu a výmenu informácií prostredníctvom spolupráce medzi vojenskými tímami reakcie na núdzové počítačové situácie (milCERT). VYZÝVA členské štáty, aby na základe práce Európskej obrannej agentúry vytvorili sieť milCERT s cieľom rozvíjať spoluprácu a uľahčovať výmenu informácií, čím by sa tiež pomohlo posilniť koordináciu s ďalšími kybernetickými komunitami, ako aj sieť vojenských veliteľov pre kybernetickú oblasť na účely posilňovania strategickej spolupráce medzi kybernetickými veliteľstvami členských štátov EÚ alebo inými zodpovedajúcimi orgánmi. Vytvorením týchto sietí by sa spolu s projektmi PESCO v kybernetickej oblasti prispelo k posilnenej kybernetickej obrane na úrovni EÚ. Zdôrazňuje význam spolupráce medzi navrhovanou sieťou milCERT a už existujúcou civilnou sieťou (CSIRT) v záujme posilnenia výmeny informácií a zlepšenia situačného povedomia.

29. Na základe vojenskej vízie a stratégie EÚ pre kybernetický priestor ako operačnú oblasť a so zreteľom na prebiehajúci vývoj vojenskej koncepcie kybernetickej obrany pre vojenské operácie a misie pod vedením EÚ OPÄTOVNE ZDÔRAZŇUJE, že je potrebné začleniť kybernetický rozmer do plánovania a vedenia misií a operácií SBOP, a to aj prostredníctvom posilnenia ich kybernetických spôsobilostí, a ZDÔRAZŇUJE, že sa tým na úrovni EÚ prispeje k lepšiemu situačnému povedomiu v kybernetickej oblasti.

30. Na záver KONŠTATUJE, že prístup ku kybernetickej bezpečnosti bude krokom k vytvoreniu doktríny EÚ pre činnosť v kybernetickom priestore založenej na posilnenej odolnosti, spôsobilostiach a možnostiach reakcie, ako aj na spoločnej pozícii k uplatňovaniu medzinárodného práva v kybernetickom priestore. Rada ZHODNOTÍ pokrok dosiahnutý pri vykonávaní týchto záverov v roku 2023 s cieľom zabezpečiť ďalší rozvoj prístupu EÚ ku kybernetickej bezpečnosti.