Europos Sąjungos
Taryba

Briuselis, 2022 m. gegužės 23 d.
(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	

POSĖDŽIO REZULTATAI

nuo:	Tarybos generalinio sekretoriato
data:	2022 m. gegužės 23 d.
kam:	Delegacijoms
Dalykas:	Tarybos išvados dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo – Tarybos išvados, Tarybos patvirtintos 2022 m. gegužės 23 d. posėdyje

Delegacijoms pridedamos Tarybos išvados dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo, kurias Taryba patvirtino 2022 m. gegužės 23 d. posėdyje.

PRIEDAS

Tarybos išvados dėl Europos Sąjungos pozicijos kibernetiniais klausimais parengimo

EUROPOS SĄJUNGOS TARYBA,

PRIMINDAMA savo išvadas dėl:

– 2013 m. birželio 25 d. bendro komunikato Europos Parlamentui ir Tarybai „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“[1],

– ES kibernetinės gynybos politikos metmenų[2],

– interneto valdymo[3],

– kibernetinio saugumo diplomatijos[4],

– Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo[5],

– 2017 m. lapkričio 20 d. bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“[6],

– bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos („Kibernetinio saugumo diplomatijos priemonių rinkinio“)[7],

– ES koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes[8],

– ES išorės kibernetinių pajėgumų stiprinimo gairių[9],

– 2018 m. gruodžio 11 d. Tarybos įgyvendinimo sprendimo (ES) 2018/1993 dėl ES integruoto politinio atsako į krizes mechanizmo[10],

---

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

– kibernetinio saugumo pajėgumų ir gebėjimų stiprinimo ES[11],

– 5G svarbos Europos ekonomikai ir poreikio mažinti su 5G susijusią saugumo riziką[12],

– aukšto skaitmeninimo lygio Europos ateities po 2020 m. „Skaitmeninio ir ekonominio konkurencingumo visoje Sąjungoje ir skaitmeninės sanglaudos stiprinimas“[13],

– papildomų pastangų siekiant didinti atsparumą ir kovoti su hibridinėmis grėsmėmis[14],

– Europos skaitmeninės ateities kūrimo[15],

– prijungtųjų įrenginių kibernetinio saugumo[16],

– Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategijos[17],

– saugumo ir gynybos[18],

– pasinaudojimo Jungtinio kibernetinio saugumo padalinio iniciatyvos galimybėmis, papildant ES koordinuotą atsaką į didelio masto kibernetinio saugumo incidentus ir krizes[19],

– Saugumo ir gynybos strateginio kelrodžio – Europos Sąjungai, kuri gina savo piliečius, vertybes bei interesus ir prisideda prie tarptautinės taikos ir saugumo[20],

---

10 OL L 320, 2018 12 17, p. 28–34.
11 Dok. 7737/19.
12 Dok. 14517/19.
13 Dok. 9596/19.
14 Dok. 14972/19.
15 Dok. 8711/20.
16 Dok. 13629/20.
17 Dok. 7290/21.
18 Dok. 8396/21.
19 Dok. 13048/21.
20 Dok. 7371/22.

1. PABRĖŽIA, kad pastaraisiais metais suintensyvėjo tiek valstybinių, tiek nevalstybinių subjektų piktavališkas elgesys kibernetinėje erdvėje, be kita ko, staigiai ir nuolat intensyvėjo kenkimo veikla, nukreipta prieš ES ir jos valstybių narių ypatingos svarbos infrastruktūrą, tiekimo grandines ir intelektinę nuosavybę, augo šalutinio poveikio rizika, taip pat daugėjo išpuolių prieš mūsų įmones, organizacijas ir piliečius naudojant išpirkos reikalavimo programinę įrangą; PAŽYMI, kad vėl pradėjus taikyti galios politiką kai kurios šalys vis dažniau bando ginčyti ir pažeisti taisyklėmis grindžiamą tarptautinę tvarką kibernetinėje erdvėje, todėl kibernetinė erdvė kartu su atvirąja jūra, oro ir kosmoso erdve tampa vis daugiau ginčų keliančia sritimi; PRIPAŽĮSTA, kad sisteminį poveikį darantys didelio masto kibernetiniai išpuoliai arba bandymai įsilaužti į tinklus ir informacines sistemas, juos sutrikdyti ar sunaikinti, tapo vis dažnesni, gali pakenkti mūsų ekonominiam saugumui ir daryti poveikį mūsų demokratinėms institucijoms bei procesams ir rodo kai kurių subjektų pasirengimą rizikuoti tarptautiniu saugumu ir stabilumu; PABRĖŽIA, kad Rusijos karinė agresija prieš Ukrainą parodė, kad puolamoji kibernetinė veikla gali būti vykdoma kaip neatsiejama hibridinių strategijų, kuriose derinami bauginimas, destabilizavimas ir ekonomikos trikdymas, dalis;

2. PAKARTOJA, kad susiduriant su dabartiniais geopolitiniais pokyčiais, mūsų Sąjungos stiprybė grindžiama vienybe, solidarumu bei ryžtingumu ir kad įgyvendinus strateginį kelrodį padidės ES strateginis savarankiškumas ir jos gebėjimas bendradarbiauti su partneriais, kad būtų apsaugotos jos vertybės ir interesai, be kita ko, kibernetinėje srityje; PABRĖŽIA, kad saugumo ir gynybos srityje stipresnė ir pajėgesnė ES teigiamai prisidės prie pasaulinio bei transatlantinio saugumo ir ji papildo NATO, kuri tebėra jos narių kolektyvinės gynybos pagrindas; DAR KARTĄ PATVIRTINA ES ketinimą intensyvinti paramą taisyklėmis grindžiamai tarptautinei tvarkai, kurios pagrindas – Jungtinės Tautos;

3. vadovaudamasi Tarybos išvadomis dėl ES kibernetinio saugumo strategijos ir strateginio kelrodžio, PAKARTOJA, kad reikia parengti Sąjungos poziciją kibernetiniais klausimais: didinti mūsų gebėjimą užkirsti kelią kibernetiniams išpuoliams stiprinant ir plėtojant pajėgumus, rengiant mokymus ir pratybas, didinant atsparumą ir ryžtingai reaguoti į kibernetinius išpuolius prieš ES ir jos valstybes nares naudojantis visomis ES turimomis priemonėmis. Tai apima tolesnį demonstravimą, kad ES yra pasiryžusi nedelsiant pateikti ilgalaikį atsaką grėsmę keliantiems subjektams, kurie siekia neleisti mums saugiai ir atvirai naudotis kibernetine erdve ir daryti poveikį mūsų strateginiams interesams, be kita ko, mūsų partnerių saugumui; šiame kontekste AKCENTUOJA, kad pozicija kibernetiniais klausimais siekiama suderinti įvairias iniciatyvas, kurios atitinka ES veiksmus, kuriais stiprinama taika ir stabilumas kibernetinėje erdvėje ir siekiama atviros, laisvos, stabilios ir saugios kibernetinės erdvės, kartu geriau koordinuojant trumpalaikius, vidutinio laikotarpio ir ilgalaikius veiksmus, skirtus užkirsti kelią kibernetinėms grėsmėms ir išpuoliams, atgrasyti nuo jų ir į juos reaguoti, ir išnaudojant kibernetinius pajėgumus; PABRĖŽIA, kad šie elementai turėtų būti įtraukti į ES poziciją kibernetiniais klausimais pagal penkias ES funkcijas kibernetinėje srityje: stiprinti mūsų kibernetinį atsparumą ir apsaugos pajėgumus; stiprinti solidarų ir visapusišką krizių valdymą; propaguoti mūsų kibernetinės erdvės viziją; stiprinti bendradarbiavimą su šalimis partnerėmis ir tarptautinėmis organizacijomis; užkirsti kelią kibernetiniams išpuoliams, gintis nuo jų ir į juos reaguoti.

I. STIPRINTI MŪSŲ KIBERNETINĮ ATSPARUMĄ IR APSAUGOS PAJĖGUMUS

4. PAKARTOJA, kad reikia didinti bendrą ES kibernetinio saugumo lygį, TIKISI, kad bus greitai priimtas Direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS) projektas, Reglamento dėl skaitmeninės veiklos atsparumo finansų sektoriuje (DORA) projektas , Direktyvos dėl ypatingos svarbos subjektų atsparumo (CER) projektas ir ATKREIPIA DĖMESĮ į pasiūlymą dėl reglamento, kuriuo nustatomos priemonės aukštam kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti, siekiant puoselėti Europos Sąjungą, kuri saugo savo piliečius, viešąsias tarnybas ir įmones kibernetinėje erdvėje; RAGINA Komisiją užbaigti pagrindinių pasiūlymų, skirtų užtikrinti, kad skaitmeninė infrastruktūra, technologijos, produktai ir paslaugos būtų saugūs, priėmimą, kad būtų galima aiškiai parodyti ES užmojus šiais klausimais ir sudaryti sąlygas teikti paramą įmonėms, kad jos galėtų įveikti šį iššūkį; RAGINA Komisiją pasiūlyti ES bendrus kibernetinio saugumo reikalavimus, taikomus susietiesiems įrenginiams ir susijusiems procesams bei paslaugoms, pasitelkiant Kibernetinio atsparumo aktą, kurį Komisija turėtų pasiūlyti iki 2022 m. pabaigos, atsižvelgiant į tai, kad reikalingas horizontalusis ir holistinis požiūris, apimantis visą skaitmeninių produktų gyvavimo ciklą, taip pat į esamą reglamentavimą, visų pirma kibernetinio saugumo srityje;

5. PRAŠO atitinkamų institucijų, pavyzdžiui, Europos elektroninių ryšių reguliuotojų institucijos (BEREC), Europos Sąjungos kibernetinio saugumo agentūros (ENISA) ir Tinklų ir informacijos saugumo (TIS) bendradarbiavimo grupės, kartu su Europos Komisija parengti rizikos vertinimu grindžiamas rekomendacijas valstybėms narėms ir Europos Komisijai siekiant sustiprinti ryšių tinklų ir infrastruktūros atsparumą Europos Sąjungoje, įskaitant tolesnį ES 5G priemonių rinkinio įgyvendinimą;

6. RAGINA ES ir jos valstybes nares dėti daugiau pastangų siekiant padidinti bendrą kibernetinio saugumo lygį, pavyzdžiui, sudarant palankesnes sąlygas patikimų kibernetinio saugumo paslaugų teikėjų atsiradimui, ir PABRĖŽIA, kad tokių paslaugų teikėjų plėtros skatinimas turėtų būti ES pramonės politikos kibernetinio saugumo srityje prioritetas; siekiant geriau pasipriešinti kibernetiniams išpuoliams, galintiems daryti sisteminį poveikį, ir su jais kovoti, taip pat remiantis patirtimi, įgyta valdant „Solarwinds“, „Microsoft Exchange“ ir „Apache Log4J“ pažeidžiamumą, PRAŠO Komisijos pasiūlyti galimybių skatinti patikimos kibernetinio saugumo paslaugų pramonės atsiradimą, stiprinti informacinių ir ryšių technologijų (IRT) tiekimo grandinės kibernetinį saugumą, šalinti galimą programinės įrangos pažeidžiamumo poveikį ES ir jos valstybėms narėms, be kita ko, atsižvelgiant į būsimą Kibernetinio atsparumo aktą, ir gerinti kibernetinių grėsmių atskleidimo bei dalijimosi informacija apie jas pajėgumus valstybėse narėse ir tarp jų;

7. PAKARTODAMA, kad investicijos į inovacijas ir geresnis civilinių technologijų panaudojimas yra itin svarbūs stiprinant mūsų technologinį suverenumą, be kita ko, kibernetinėje srityje, RAGINA Komisiją skubiai įsteigti Europos kibernetinio saugumo kompetencijos centrą siekiant sukurti stiprią Europos kibernetinių tyrimų, pramonės ir technologijų ekosistemą, PABRĖŽIA, kad reikia skatinti mokslinius tyrimus ir inovacijas, daugiau investuoti į civilines ir gynybos sritis siekiant stiprinti ES gynybos pramoninę ir technologinę bazę (EGPTB) ir plėtoti ES bei jos valstybių narių kibernetinius pajėgumus, įskaitant strateginės paramos pajėgumus; PABRĖŽIA, kad siekiant įgyti lyginamųjų pranašumų, be kita ko, reagavimo į kibernetinius išpuolius operacijų srityje, svarbu intensyviai naudoti naujas technologijas, visų pirma kvantinę kompiuteriją, dirbtinį intelektą ir didžiuosius duomenis;

8. PRIPAŽINDAMA, kad mūsų kibernetinio saugumo stiprinimas yra būdas padidinti mūsų pastangų sausumoje, ore, jūroje ir kosminėje erdvėje veiksmingumą ir saugumą, PABRĖŽIA, jog svarbu, kad kibernetinio saugumo aspektai būtų įtraukti į visas ES viešosios politikos sritis, įskaitant sektorių teisės aktus, papildančius Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2 direktyva), ir PRAŠO Komisijos išnagrinėti galimybes sustiprinti kibernetinį saugumą visoje ES gynybos pramoninės ir technologinės bazės (EGPTB) tiekimo grandinėje;

9. PRIPAŽĮSTA, kad siekiant parengti ES poziciją kibernetiniais klausimais labai svarbu užtikrinti tinkamus finansinius bei žmogiškuosius išteklius kibernetiniam saugumui ir priemones, kuriomis būtų siekiama sukurti palankią aplinką privačiajam sektoriui, kad jis būtų konkurencingas, ir kad kibernetinio saugumo stabilaus ir ilgalaikio finansavimo klausimas turėtų būti sprendžiamas ES lygmeniu sukuriant ir įgyvendinant horizontalųjį mechanizmą, apimantį įvairius finansavimo šaltinius, įskaitant aukštos kvalifikacijos žmogiškųjų išteklių išlaidas; todėl RAGINA Komisiją iki 2022 m. pabaigos išnagrinėti su tokiu mechanizmu susijusias galimybes, kurios turi būti aptartos atitinkamuose Tarybos organuose;

10. PABRĖŽIA, kad reikia stiprinti mūsų pastangas ir intensyvinti bendradarbiavimą kovos su tarptautiniais kibernetiniais nusikaltimais srityje, visų pirma išpirkos reikalavimo programinės įrangos klausimu, pasitelkiant Europos kovos su nusikalstamumo grėsmėmis daugiadalykės platformos (EMPACT) mechanizmą, keičiantis informacija tarp kibernetinio saugumo, teisėsaugos ir diplomatinių sektorių ir stiprinant teisėsaugos pajėgumus kibernetinių nusikaltimų tyrimo ir baudžiamojo persekiojimo už juos srityje; PAKARTOJA savo įsipareigojimą informuoti visuomenę apie kibernetines grėsmes ir priemones, kurių imtasi nacionaliniu ir ES lygmenimis siekiant kovoti su šiomis grėsmėmis, įtraukiant pilietinę visuomenę, privatųjį sektorių ir akademinę bendruomenę, kad būtų didinamas informuotumas ir skatinama tinkamo lygio kibernetinė apsauga ir kibernetinė higiena; PABRĖŽIA, kad reikia sutelkti dėmesį į piliečių kibernetinio saugumo įgūdžius bei gebėjimus ES ir valstybių narių lygmenimis ir aktyviai įtraukti naudotojus į jų pačių apsaugą.

II. **STIPRINTI SOLIDARŲ IR VISAPUSIŠKĄ KRIZIŲ VALDYMĄ**

11. Remdamasi metinėmis kibernetinio saugumo pratybomis, kitomis su kibernetiniu aspektu susijusiomis pratybomis ir 2022 m. ES Kibernetinių krizių valdymo pratybomis (EU CyCLES), PABRĖŽIA, kad svarbu parengti reguliarių tarpbendruomeninių ir daugiapakopių kibernetinio saugumo pratybų programą, siekiant išbandyti ir plėtoti ES vidaus ir išorės atsaką į didelio masto kibernetinius incidentus, dalyvaujant Tarybai, EIVT, Komisijai ir atitinkamiems suinteresuotiesiems subjektams, pavyzdžiui, Europos Sąjungos kibernetinio saugumo agentūrai (ENISA) ir privačiajam sektoriui, kuri bus aiškiai suformuluota ir kuria bus prisidedama prie bendros ES pratybų politikos; PABRĖŽIA, kad svarbu toliau plėtoti „Cyber Europe“ ir „BlueOLEx“pratybas, apimančias atsakomuosius veiksmus įvairiais lygmenimis; PRIPAŽĮSTA, kad reikia įvertinti ir stiprinti esamas pratybas ir nagrinėti tolesnių pratybų galimybes, visų pirma, pratybų konkrečiuose kibernetinės srities segmentuose, t. y. karinių kompiuterinių incidentų tyrimo tarnybų (CERT) pratybų ir pratybų, kuriose daugiausia dėmesio būtų skirta Europos Sąjungos institucijų, įstaigų ir agentūrų bendradarbiavimui krizių atveju; PRIPAŽĮSTA, kad Sąjungos pozicija kibernetiniais klausimais sustiprins mūsų gebėjimą užkirsti kelią kibernetiniams išpuoliams vykdant įvairius veiksmus, įskaitant mokymą, ir todėl PRAŠO valstybių narių stiprinti civilinį ir karinį bendradarbiavimą mokymo ir pratybų kibernetinėje srityje klausimais;

12. PABRĖŽIA, kad reikia toliau testuoti ir sustiprinti operatyvinį bendradarbiavimą ir bendrą informuotumą tarp valstybių narių, be kita ko, pasitelkiant sukurtus tinklus, pavyzdžiui, Reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklą ir Ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (EU CyCLONe), kad būtų gerinama ES parengtis reaguoti į didelio masto kibernetinius incidentus; PABRĖŽIA, jog svarbu dirbti siekiant išplėtoti bendrą valstybių narių tarpusavio ir su Europos Sąjungos institucijomis, įstaigomis ir agentūromis kalbą, kuri būtų pritaikyta diskusijoms politiniu lygmeniu, kad būtų remiamas konsoliduoto atitinkamų kibernetinių incidentų sunkumo ir poveikio vertinimo, taip pat galimų raidos scenarijų ir atitinkamai dėl jų atsirandančių poreikių, nustatymas; šiuo atžvilgiu; PABRĖŽIA, kad reikia gerinti bendrų padėties vertinimo ataskaitų, įskaitant EU CyCLONe ataskaitas dėl didelio masto kibernetinių incidentų poveikio ir sunkumo ES valstybėse narėse ir grėsmių vertinimus, kuriuos ES žvalgybos ir situacijų centras (EU INTCEN) teikia ES kibernetinio saugumo diplomatijos priemonių rinkinio kontekste, papildomumą; PRAŠO Komisijos bei vyriausiojo įgaliotinio ir TIS bendradarbiavimo grupės, koordinuojant veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis ir agentūromis ir sukurtais tinklais, įskaitant EU CyCLONe, iki 2022 m. pabaigos atlikti rizikos vertinimą ir parengti rizikos kibernetinio saugumo aspektu scenarijus esant grėsmei ar galimam išpuoliui prieš valstybes nares ar šalis partneres ir pateikti juos atitinkamiems Tarybos organams; PABRĖŽIA, kad reikia tinkamai ir koordinuotai informuoti visuomenę apie ES atsaką į didelio masto kibernetinius incidentus;

13. didelio masto kibernetinių incidentų atveju, PABRĖŽIA, kad reikia stiprinti koordinavimą ir, kai tinkama, remiantis PESCO sistemos Greitojo reagavimo į kibernetinius incidentus komandų padaryta pažanga ir atliekamu darbu, ir pasinaudojant CSIRT tinklo ir EU CyCLONe darbu, stiprinti savanorišką valstybių narių reagavimo į incidentus pajėgumų telkimą; PRIPAŽĮSTA, kad plėtojant ryšius su privačiuoju sektoriumi galėtų būti sustiprinti viešieji pajėgumai, visų pirma atsižvelgiant į įgūdžių trūkumą visoje ES, ir kad nustačius šiuos privačius partnerius ir koordinuojant jų veiksmus, būtų galima pakeisti padėtį didelio masto incidentų atveju; siekiant visapusiškai pasirengti didelio masto kibernetiniams incidentams, PRAŠO Komisijos ne vėliau kaip 2022 m. trečiojo ketvirčio pabaigoje pateikti pasiūlymą dėl naujo Reagavimo į kibernetinio saugumo krizes fondo;

14. atsižvelgdama į Strateginį kelrodį, PAKARTOJA, kad reikia investuoti į mūsų savitarpio pagalbą pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį ir į solidarumą pagal Sutarties dėl Europos Sąjungos veikimo 222 straipsnį, visų pirma dažnai rengiant pratybas; šiame kontekste PABRĖŽIA, kad reikia tęsti darbą, susijusį su dvišalės civilinės ir (arba) karinės paramos teikimu ir koordinavimu, be kita ko, analizuojant galimą paramą, kurią teiktų ES esant aiškiam valstybių narių prašymui, ir nustatant tinkamas reagavimo priemones, be kita ko, parengiant koordinuotą komunikacijos strategiją, įgyvendinant 42 straipsnio 7 dalį; PAŽYMI, kad tai taip pat galėtų apimti koordinavimo su esamais ES krizių valdymo mechanizmais ir ES civilinės saugos mechanizmu gerinimą;

15. PABRĖŽIA, kad siekiant užtikrinti sustiprintą ES poziciją kibernetiniais klausimais, reikės sustiprintų saugių ryšių; šiuo tikslu PAKARTOJA Strateginiu kelrodžiu suteiktas gaires šiuo atžvilgiu ir PRAŠO Komisijos ir kitų atitinkamų institucijų, įstaigų ir agentūrų iki 2022 m. pabaigos parengti esamų saugios komunikacijos kibernetinėje erdvėje priemonių sąrašą, kuris turi būti aptartas atitinkamuose Tarybos organuose ir su atitinkamomis bendradarbiavimo grupėmis, pavyzdžiui, CSIRT tinklu ir EU CyCLONe.

III. PROPAGUOTI MŪSŲ KIBERNETINĖS ERDVĖS VIZIJĄ

16. PRIMENA, kad bendro ir visapusiško ES požiūrio į kibernetinę diplomatiją tikslas yra padėti vykdant konfliktų prevenciją, mažinant kibernetinio saugumo grėsmes ir užtikrinant stabilesnius tarptautinius santykius; Šiame kontekste DAR KARTĄ PATVIRTINA ES įsipareigojimą tarptautinius ginčus kibernetinės erdvės klausimais spręsti taikiomis priemonėmis ir taikant tarptautinę teisę, įskaitant tarptautinę žmogaus teisių teisę ir tarptautinę humanitarinę teisę, valstybių veiksmams kibernetinėje erdvėje; PABRĖŽIA ES ir valstybių narių įsipareigojimą įsipareigojimą veikti laikantis savanoriškų, neprivalomų atsakingo valstybių elgesio kibernetinėje erdvėje normų, dėl kurių susitarė visos JT valstybės narės; AKCENTUOJA atviros, laisvos, visuotinos, stabilios ir saugios kibernetinės erdvės, kurioje visapusiškai užtikrinamos žmogaus teisės, pagrindinės laisvės ir laikomasi teisinės valstybės principo remiant mūsų laisvos ir demokratinės visuomenės socialinę gerovę, ekonominį augimą, klestėjimą ir vientisumą, svarbą ir DAR KARTĄ PATVIRTINA ES ir jos valstybių narių įsipareigojimą toliau propaguoti šias vertybes ir principus; siekiant plėtoti konstruktyvaus, nuoširdaus ir atviro dialogo su pagrindiniais kibernetinės erdvės suinteresuotaisiais subjektais kanalus, PABRĖŽIA, jog svarbu, kad kibernetiniai klausimai, įskaitant ES kibernetinio saugumo diplomatijos priemonių rinkinį, taptų neatsiejama Sąjungos stojimo derybų ir ES strateginių ir politinių dialogų su tarptautiniais partneriais ir konkurentais dalis, ir tuo pačiu metu RAGINA vyriausiąjį įgaliotinį peržiūrėti esamus dvišalius dialogus kibernetiniais klausimais ir prireikus pasiūlyti pradėti panašų bendradarbiavimą su papildomomis šalimis ar atitinkamomis tarptautinėmis organizacijomis;

17. PRIMENA daugiašalio suinteresuotųjų subjektų bendradarbiavimo svarbą, nes kiti suinteresuotieji subjektai taip pat yra atsakingi už kibernetinį saugumą, visų pirma kai tai susiję su rekomendacijų ir sprendimų, priimtų tarptautiniuose ir regioniniuose forumuose, įgyvendinimu; RAGINA ES ir jos valstybes nares toliau propaguoti mūsų kibernetinės erdvės ir interneto modelį, grindžiamą daugiasubjekčiu požiūriu, pasitelkiant tokias iniciatyvas kaip Paryžiaus kvietimas užtikrinti pasitikėjimą ir saugumą kibernetinėje erdvėje ir Deklaracija dėl interneto ateities, pabrėžiant bendrą stabilumo kibernetinėje erdvėje naudą ir visame pasaulyje didinant informuotumą apie į valstybę orientuotos ir autoritarinės interneto vizijos keliamus pavojus, ir RAGINA ES ir jos valstybes nares toliau stiprinti bendradarbiavimą su įvairių suinteresuotųjų subjektų bendruomene, be kita ko, pasinaudojant atitinkamais projektais, pavyzdžiui, ES užsienio politikos priemone ES kibernetinės diplomatijos iniciatyva;

18. ĮSIPAREIGOJA nuolat dalyvauti atitinkamose tarptautinėse organizacijose, ypač su JT Pirmuoju komitetu ir Trečiuoju komitetu susijusiuose procesuose, kartu pabrėždama, kad esama tarptautinė teisė be išlygų taikoma kibernetinėje erdvėje ir jos atžvilgiu; PABRĖŽIA, kad svarbu toliau dėti pastangas siekiant išlaikyti ir propaguoti JT atsakingo valstybių elgesio sistemą, ir PABRĖŽIA, kad ES ir jos valstybės narės aktyviai dirbs siekdamos stiprinti jos įgyvendinimą, be kita ko, sukurdamos Veiksmų programą, skirtą atsakingo valstybių elgesio kibernetinėje erdvėje skatinimui; PABRĖŽIA, kad ES ir jos valstybės narės aktyviai dalyvaus derybose dėl būsimos JT konvencijos, kuri būtų veiksminga teisėsaugos ir teisminių institucijų priemonė pasauliniu mastu kovojant su kibernetiniais nusikaltimais, visapusiškai atsižvelgiant į esamą šios srities tarptautinių ir regioninių priemonių sistemą, visų pirma Budapešto konvenciją dėl elektroninių nusikaltimų; PABRĖŽIA, kad svarbu toliau remti pasitikėjimo stiprinimo priemonių kūrimą ir įgyvendinimą regioniniu ir tarptautiniu lygmenimis, ir toliau skatinti naudoti esamas ESBO kibernetines priemones, be kita ko, tarptautinės įtampos metu;

19. PRIMENA, jog siekiant užtikrinti, kad internetas toliau būtų pasaulinis, nesuskaidytas ir atviras, būtina laikytis proaktyvaus žmogaus teisėmis grindžiamo požiūrio, kad vadovaujantis demokratinėmis vertybėmis ir principais būtų užtikrinti tarptautiniai standartai naujai atsirandančių technologijų ir pagrindinės interneto architektūros srityse, ir PRITARIA principui, pagal kurį technologijos naudojamos ir kuriamos gerbiant žmogaus teises, itin daug dėmesio skiriant privatumo apsaugai ir naudojamos teisėtai, saugiai ir etiškai; RAGINA vyriausiąjį įgaliotinį ir Komisiją parengti strateginę skaitmeninės srities viziją techniniais klausimais, kurie turi įtakos užsienio politikai ir galėtų daryti poveikį kibernetinės erdvės ir, visų pirma, interneto stabilumui, be kita ko, atitinkamose specializuotose tarptautinėse organizacijose (Tarptautinėje telekomunikacijų sąjungoje ir kt.).

IV. STIPRINTI BENDRADARBIAVIMĄ SU ŠALIMIS PARTNERĖMIS IR TARPTAUTINĖMIS ORGANIZACIJOMIS

20. PABRĖŽIA, kad ES kibernetinių pajėgumų stiprinimo strategiją reikia geriau susieti su JT atsakingo valstybių elgesio kibernetinėje erdvėje normomis: be kita ko, plėtoti pritaikytą bendradarbiavimą ir pajėgumų stiprinimo programas siekiant remti trečiųjų valstybių dedamas įgyvendinimo pastangas, ir, tai darant, toliau dėti pastangas propaguoti JT atsakingo valstybių elgesio kibernetinėje erdvėje gerinimo veiksmų programą ir šias pastangas plėsti; PABRĖŽIA, kad svarbu visapusiškai integruoti kibernetinių pajėgumų stiprinimą į ES, kaip saugumo užtikrintojos, pasiūlymą, tinkamai koordinuojant valstybių narių ir ES institucijų, įstaigų ir agentūrų pastangas, ir, visų pirma, PALANKIAI VERTINA valstybių narių, taip pat viešojo ir privačiojo sektorių partnerių bendradarbiavimą, visų pirma pasitelkiant ES kibernetinį tinklą (ES kibernetinių pajėgumų stiprinimo tinklą) ir Pasaulinį kibernetinių ekspertinių žinių forumą (GFCE), kad būtų užtikrintas bendradarbiavimas ir išvengta dubliavimosi;

PRAŠO vyriausiojo įgaliotinio ir Komisijos ne vėliau kaip 2022 m. trečiąjį ketvirtį įsteigti *kibernetinių pajėgumų stiprinimo valdybą* ir reguliariai keistis informacija Kibernetinių klausimų horizontalioji darbo grupėje; PRAŠO Komisijos ir vyriausiojo įgaliotinio toliau telkti Kaimynystės, vystomojo ir tarptautinio bendradarbiavimo priemonę „Globali Europa“ (KVTBP), Pasirengimo narystei paramos priemonę (PNPP II) ir kitas finansines priemones, pavyzdžiui, Europos taikos priemonę (ETP) ir strategiją „Global Gateway“, siekiant remti mūsų partnerių atsparumo stiprinimą, jų pajėgumus nustatyti ir šalinti kibernetines grėsmes ir

tirti kibernetinius nusikaltimus bei patraukti baudžiamojon atsakomybėn jų vykdytojus ir bendradarbiavimo projektų plėtojimą, be kita ko, krizių kontekste; visų pirma RAGINA bendradarbiauti su Vakarų Balkanų partneriais ir ES rytinėmis bei pietinėmis kaimyninėmis šalimis ir dislokuoti ES ir valstybių narių ekspertus, kad būtų pasiūlyta pagalba kibernetinių krizių atvejais, atsižvelgiant į esamus teisinius įgaliojimus;

21. PAŽYMI, jog reikia dėti daugiau pastangų siekiant parengti struktūrišką ir atvirą ES informavimo požiūrį į tai, kaip propaguoti bendrą pasaulinį supratimą apie tarptautinės teisės taikymą kibernetinėje erdvėje, JT atsakingo valstybių elgesio sistemą kibernetinėje erdvėje, įskaitant iniciatyvą dėl Veiksmų programos, skirtos atsakingo valstybių elgesio kibernetinėje erdvėje skatinimui, taip pat į ES ir jos valstybių narių poziciją vykstančiose JT konvencijos dėl kibernetinių nusikaltimų derybose ir dedant šias pastangas PRAŠO vyriausiojo įgaliotinio ne vėliau kaip 2022 m. pabaigoje pateikti Tarybai informavimo planą; RAGINA vyriausiąjį įgaliotinį ir Komisijos tarnybas visapusiškai ir sistemiškai naudotis 145 delegacijomis ir plėtoti reguliarų bei produktyvų jų ir valstybių narių ambasadų trečiosiose šalyse bendradarbiavimą, remiant numatytam ES kibernetinio saugumo diplomatijos tinklui; PRAŠO vyriausiojo įgaliotinio ne vėliau kaip 2022 m. trečiąjį ketvirtį sukurti ES kibernetinio saugumo diplomatijos tinklą, kuris prisidėtų prie keitimosi informacija, bendros ES ir valstybių narių darbuotojams skirtos mokymo veiklos, suderintų pajėgumų stiprinimo pastangų ir JT atsakingo valstybių elgesio sistemos įgyvendinimo stiprinimo, taip pat pasitikėjimo stiprinimo priemonių tarp valstybių;

22. PABRĖŽIA savo įsipareigojimą toliau bendradarbiauti su tarptautinėmis organizacijomis ir šalimis partnerėmis siekiant gerinti bendrą supratimą apie kibernetinių grėsmių aplinką, rengti bendradarbiavimo mechanizmus ir proaktyviai nustatyti bendradarbiavimu grindžiamą diplomatinį atsaką; PRIMINDAMA pagrindinius ES ir NATO bendradarbiavimo kibernetinio saugumo srityje pasiekimus įgyvendinant 2016 m. Varšuvos ir 2018 m. Briuselio bendras deklaracijas, visapusiškai gerbdama sprendimų priėmimo autonomiškumą bei abiejų organizacijų procedūras ir remdamasi skaidrumo, abipusiškumo ir įtraukumo principais, PABRĖŽIA, kad reikia toliau stiprinti bendradarbiavimą kibernetinėje srityje su NATO vykdant pratybas, dalijantis informacija ir ekspertams keičiantis informacija, be kita ko, dėl pajėgumų plėtojimo, partnerių, misijų ir operacijų pajėgumų stiprinimo, taip pat dėl tarptautinės teisės ir atsakingo valstybių elgesio normų taikymo kibernetinėje erdvėje, ir galimų koordinuotų atsakomųjų veiksmų reaguojant į kibernetinę kenkimo veiklą.

V. UŽKIRSTI KELIĄ KIBERNETINIAMS IŠPUOLIAMS, GINTIS NUO JŲ IR REAGUOTI Į JUOS

23. PRIPAŽĮSTA, kad kibernetinė erdvė tapo geopolitinės konkurencijos arena, todėl DAR KARTĄ PAKARTOJA, kad ES privalo gebėti sparčiai ir ryžtingai reaguoti į kibernetinius išpuolius, pavyzdžiui, valstybių remiamą kibernetinę kenkimo veiklą, nukreiptą prieš ES ir jos valstybes nares, taigi turi stiprinti ES kibernetinio saugumo diplomatijos priemonių rinkinį ir visapusiškai pasinaudoti visomis savo priemonėmis, įskaitant esamas politines, ekonomines, diplomatines, teisines ir strateginės komunikacijos priemones, kad užkirstų kelią kibernetinei kenkimo veiklai, nuo jos atgrasytų ir į ją reaguotų; PABRĖŽIA, jog priešiški subjektai turi žinoti, kad prieš valstybes nares ir ES institucijas nukreipti kibernetiniai išpuoliai bus atskleisti ankstyvame etape, nustatyti greitai ir į juos bus reaguojama pasitelkiant visas reikiamas priemones ir politiką; remdamasi visų pirma pozicijoje kibernetiniais klausimais pateiktais elementais ir patirtimi, įgyta įgyvendinant Kibernetinio saugumo diplomatijos priemonių rinkinį nuo jo priėmimo ir vykdant pratybas „EU CyCLES“, PRAŠO valstybių narių ir vyriausiojo įgaliotinio, padedant Komisijai, siekti ne vėliau kaip 2023 m. pirmojo ketvirčio pabaigoje parengti peržiūrėtą ES kibernetinio saugumo diplomatijos priemonių rinkinio įgyvendinimo gairių redakciją, visų pirma išnagrinėjant papildomas atsako priemones;

24. PABRĖŽIA būtinybę atitinkamuose Tarybos organuose ir komitetuose reguliariai keistis informacija apie kibernetinių grėsmių aplinką, kartu taip pat reguliariai bendradarbiaujant su privačiuoju sektoriumi ir remiantis poveikio bei pastarojo meto incidentų rimtumo vertinimu, siekiant didinti bendrą informuotumą ir pasirengimą tolesniam ES kibernetinio saugumo diplomatijos priemonių rinkinio taikymui, ir toliau plėtoti priemones, skirtas jo įgyvendinimui remti; nors už nacionalinį saugumą ir toliau atsako kiekviena valstybė narė, PAŽYMI, kad reikia stiprinti dalijimąsi žvalgybos informacija bei duomenimis ir bendradarbiavimą tarp valstybių narių, taip pat su ES žvalgybos ir situacijų centru (EU INTCEN), kad būtų galima dalytis žvalgybos informacija sprendimų priėmimo proceso pradžioje, be kita ko, priskyrimo klausimu, ir taip sudaryti sąlygas sparčiai, veiksmingai ir pagrįstai reaguoti į kibernetinę kenkimo veiklą, nukreiptą prieš ES ir jos partnerius; PAKARTOJA, kad svarbu stiprinti EU INTCEN pajėgumus kibernetinėje srityje, remiantis savanorišku valstybių narių žvalgybos indėliu ir nedarant poveikio jų kompetencijai, ir išnagrinėti pasiūlymą dėl galimo valstybių narių kibernetinės žvalgybos darbo grupės įsteigimo;

25. PRIPAŽINDAMA, kad ES deklaracijomis ir ribojamosiomis priemonėmis, kurių imtasi pagal ES kibernetinio saugumo diplomatijos priemonių rinkinį, pasiųsta aiški žinia, jog ES, jos valstybėms narėms ir partneriams išorės grėsmę kelianti kibernetinė kenkimo veikla yra nepriimtina, todėl jomis prisidedama prie kibernetinės kenkimo veiklos prevencijos, atgrasymo nuo jos ir reagavimo į ją, DAR KARTĄ PAKARTOJA savo įsipareigojimą naudotis šiomis priemonėmis siekiant priminti pareigas, kurios taikomos kibernetinėje erdvėje pagal tarptautinę teisę, įskaitant visą JT chartiją, ir skatinti JT atsakingo valstybių elgesio kibernetinėje erdvėje sistemą, be kita ko, išsamaus patikrinimo pareigos taikymą visoms valstybėms, kad sąmoningai nebūtų leidžiama jų teritorijoje naudojantis informacinėmis ir ryšių technologijomis (IRT) vykdyti tarptautiniu mastu neteisėtų veiksmų, siekiant toliau plėtoti ir propaguoti ES bendrą požiūrį į tarptautinės teisės taikymą kibernetinėje erdvėje; pažymėdama, kad tinkamais ir greitais pranešimais mažinama eskalavimo grėsmė ir jie gali atgrasyti išpuolių, nukreiptų prieš Europos interesus, vykdytojus, PRAŠO vyriausiojo įgaliotinio parengti ir pateikti valstybėms narėms nuoseklią komunikacijos strategiją ES kibernetinio saugumo diplomatijos priemonių rinkinio naudojimo klausimu;

26. RAGINA plėtoti laipsniškus, tikslinius ir nuoseklius požiūrius ir atsakomuosius veiksmus reaguojant į kibernetinę kenkimo veiklą, naudojantis įvairiomis ES kibernetinio saugumo diplomatijos priemonių rinkinio priemonėmis, įskaitant ES kibernetinių sankcijų režimą, ir numatant papildomas priemones; PABRĖŽIA, kad reikia didinti galimybes kiekvienu konkrečiu atveju sutelkti visas turimas vidaus ir išorės priemones siekiant užkirsti kelią kibernetiniams išpuoliams, atgrasyti nuo jų ir į juos reaguoti, ir įgyvendinti jas taikant spartų, veiksmingą, laipsnišką, tikslinį ir nuoseklų požiūrį, grindžiamą ilgalaikiu strateginiu įsipareigojimu; PRAŠO vyriausiojo įgaliotinio bendradarbiaujant su Komisija nustatyti įvairius galimus bendrus ES reagavimo į kibernetinius išpuolius veiksmus, įskaitant sankcijų galimybes, kad būtų pasirengta prireikus imtis skubių ir veiksmingų veiksmų, ir pateikti juos Tarybai ne vėliau kaip 2023 m. pirmojo ketvirčio pabaigoje;

27. pažymėdama, kad kibernetinė gynyba yra pirmiausia nacionalinė atsakomybė, RAGINA valstybes nares toliau plėtoti savo pačių pajėgumus vykdyti kibernetinės gynybos operacijas, įskaitant proaktyvias apsaugos nuo kibernetinių išpuolių, jų atskleidimo, gynybos ir atgrasymo nuo jų priemones, ir galimai remiant kitas valstybes nares ir ES; kiekviena valstybė narė raginama prireikus stiprinti savo gebėjimus teikti ir priimti paramą ir pagalbą; PABRĖŽIA, kad vienas iš pagrindinių būsimos ES kibernetinės gynybos politikos tikslų turėtų būti tolesnis šių pajėgumų plėtojimas; PAŽYMI, kad ES kibernetinės gynybos politikoje turėtų būti labiau atsižvelgiama į tai, kokį vaidmenį atitinkamos ES institucijos ir įstaigos gali atlikti, kad pagerintų ES ir valstybių narių atitinkamų kibernetinės gynybos subjektų bendradarbiavimą ir plėtotų savo pačių pajėgumus, atsižvelgiant į jų atitinkamus įgaliojimus; PRAŠO vyriausiojo įgaliotinio kartu su Komisija prisidėti prie ES pozicijos kibernetiniais klausimais rengimo 2022 m. pateikiant plataus užmojo pasiūlymą dėl ES kibernetinės gynybos politikos, kuri sudarys sąlygas Tarybai toliau rengti ES poziciją kibernetiniais klausimais;

28. PABRĖŽIA, kad reikia didinti sąveikumą ir dalijimąsi informacija vykdant karinių kompiuterinių incidentų tyrimo tarnybų (milCERT) bendradarbiavimą; PRAŠO valstybių narių remiantis Europos gynybos agentūros (EGA) darbu sukurti MilCERT tinklą siekiant plėtoti bendradarbiavimą ir sudaryti palankesnes sąlygas keistis informacija (tai taip pat padėtų skatinti bendradarbiavimą su kitomis kibernetinėmis bendruomenėmis), taip pat karinių kibernetinės gynybos vadų tinklą siekiant sustiprinti strateginį valstybių narių kibernetinės gynybos vadovybių ar kitų atitinkamų institucijų bendradarbiavimą. Sukūrus šiuos tinklus kartu su PESCO kibernetinės srities projektais būtų prisidėta prie kibernetinės gynybos stiprinimo ES lygmeniu. Pabrėžia siūlomo MilCERT tinklo ir jau esamo civilinio (reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT)) tinklo bendradarbiavimo svarbą siekiant gerinti keitimąsi informacija ir didinti informuotumą apie padėtį;

29. remdamasi ES karine vizija bei strategija dėl kibernetinės erdvės kaip operacijų srities ir atsižvelgdama į tai, kad šiuo metu rengiama ES vadovaujamoms karinėms operacijoms ir misijoms skirta karinė kibernetinės gynybos koncepcija, PAKARTOJA, kad kibernetinį aspektą reikia integruoti į BSGP misijų ir operacijų planavimą ir vykdymą, be kita ko, stiprinant jų kibernetinius pajėgumus, ir PABRĖŽIA, kad tai padės užtikrinti geresnį informuotumą apie kibernetinę padėtį ES lygmeniu;

30. baigdama PAŽYMI, kad pozicija kibernetiniais klausimais bus žingsnis į priekį siekiant sukurti ES veiksmų kibernetinėje erdvėje doktriną, grindžiamą didesniu atsparumu, pajėgumais ir reagavimo galimybėmis, taip pat nustatyti bendrą poziciją dėl tarptautinės teisės taikymo kibernetinėje erdvėje; Taryba ATKREIPS DĖMESĮ į pažangą, kuri bus padaryta įgyvendinant šias išvadas 2023 m., kad būtų užtikrintas tolesnis ES pozicijos kibernetiniais klausimais plėtojimas.