Europos Parlamentas
2019-2024

PRIIMTI TEKSTAI

P9_TA(2021)0412

ES kibernetinės gynybos pajėgumų padėtis

2021 m. spalio 7 d. Europos Parlamento rezoliucija dėl ES kibernetinės gynybos pajėgumų padėties (2020/2256(INI))

Europos Parlamentas,

– atsižvelgdamas į Europos Sąjungos sutartį (ES sutartis) ir į Sutartį dėl Europos Sąjungos veikimo (SESV),

– atsižvelgdamas į 2016 m. birželio 28 d. Komisijos pirmininko pavaduotojo ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai (pirmininko pavaduotojas ir vyriausiasis įgaliotinis) pristatytą dokumentą „Bendra vizija, bendri veiksmai: stipresnė Europa. Visuotinė Europos Sąjungos užsienio ir saugumo politikos strategija“,

– atsižvelgdamas į 2013 m. gruodžio 20 d., 2015 m. birželio 26 d., 2016 m. gruodžio 15 d., 2017 m. kovo 9 d., 2017 m. birželio 22 d., 2017 m. lapkričio 20 d. ir 2017 m. gruodžio 15 d. Europos Vadovų Tarybos išvadas,

– atsižvelgdamas į 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[1],

– atsižvelgdamas į 2017 m. birželio 19 d. Tarybos išvadas dėl bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos („Kibernetinio saugumo diplomatijos priemonių rinkinio“),

– atsižvelgdamas į 2017 m. rugsėjo 13 d. Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendrą komunikatą „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ (JOIN(2017)0450),

– atsižvelgdamas į 2018 m. liepos mėn. pasirašytą bendrą deklaraciją dėl ES ir NATO bendradarbiavimo,

– atsižvelgdamas į 2019 m. gegužės 17 d. Tarybos sprendimą (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais,

– atsižvelgdamas į 2019 m. gruodžio 10 d. Tarybos išvadas dėl papildomų pastangų

[1] OL L 194, 2016 7 19, p. 1.

siekiant didinti atsparumą ir kovoti su hibridinėmis grėsmėmis,

– atsižvelgdamas į 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentą (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo (Kibernetinio saugumo aktas)[1],

– atsižvelgdamas į 2020 m. birželio 16 d. Tarybos išvadas dėl ES išorės veiksmų terorizmo ir smurtinio ekstremizmo prevencijos ir kovos su jais srityje,

– atsižvelgdamas į Tarybos ir Taryboje posėdžiavusių valstybių narių vyriausybių atstovų išvadas dėl susitarimo dėl civilinių BSGP pajėgumų nustatymo,

– atsižvelgdamas į 2020 m. liepos 30 d. Tarybos sprendimą (BUSP) 2020/1127[2], kuriuo iš dalies keičiamas Sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais,

– atsižvelgdamas į 2020 m. spalio 22 d. Tarybos sprendimą (BUSP) 2020/1537[3], kuriuo iš dalies keičiamas Sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais,

– atsižvelgdamas į 2020 m. liepos 24 d. Komisijos komunikatą dėl ES saugumo sąjungos strategijos (COM(2020)0605),

– atsižvelgdamas į 2020 m. gruodžio 16 d. Komisijos ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai bendrą komunikatą „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“ (JOIN(2020)0018),

– atsižvelgdamas į 2020 m. gruodžio 16 d. Komisijos pasiūlymą dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria panaikinama Direktyva (ES) 2016/1148 (COM(2020)0823),

– atsižvelgdamas į 2020 m. gruodžio 16 d. Komisijos pasiūlymą dėl Europos Parlamento ir Tarybos direktyvos dėl ypatingos svarbos subjektų atsparumo (COM(2020)0829),

– atsižvelgdamas į 2021 m. kovo 9 d. Tarybos išvadas dėl Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategijos,

– atsižvelgdamas į 2021 m. kovo 25 d. Europos Vadovų Tarybos susitikimo išvadas,

– atsižvelgdamas į 2021 m. kovo 10 d. neribotos sudėties darbo grupės ataskaitą,

– atsižvelgdamas į JT nusiginklavimo darbotvarkę „Mūsų bendros ateities užtikrinimas“,

– atsižvelgdamas į Jungtinių Tautų darnaus vystymosi tikslus ir ypač į 16-ąjį DVT, kurio tikslas – skatinti taikias ir įtraukias visuomenes darniam vystymuisi,

– atsižvelgdamas į Europos Audito Rūmų apžvalgą Nr. 09/2019 dėl Europos gynybos,

---

1 OL L 151, 2019 6 7, p. 15.
2 OL L 246, 2020 7 30, p. 12.
3 OL L 351 I, 2020 10 22, p. 5.

– atsižvelgdamas į savo 2018 m. birželio 13 d. rezoliuciją dėl kibernetinės gynybos[1],

– atsižvelgdamas į Darbo tvarkos taisyklių 54 straipsnį,

– atsižvelgdamas į Užsienio reikalų komiteto pranešimą (A9-0234/2021),

A. kadangi ES ir jos valstybės narės turi toliau plėtoti kibernetinio saugumo strategiją, kurioje nustatomi realistiški, tikslūs ir plataus užmojo tikslai bei aiškiai apibrėžiama politika tiek karinėje, tiek civilinėje srityje, taip pat ten, kur abu sektoriai sutampa; kadangi visos ES institucijos ir ES valstybės narės turi labiau bendradarbiauti visais lygmenimis, kad parengtų šią strategiją, kurios pagrindinis tikslas turėtų būti toliau stiprinti atsparumą ir plėtoti ne tik bendrus, bet ir geresnius nacionalinius, tvirtus civilinės ir karininės srities kibernetinius pajėgumus bei bendradarbiavimą, kad galėtų reaguoti į ilgalaikius saugumo iššūkius;

B. kadangi ES yra įsipareigojusi kibernetinėje erdvėje taikyti galiojančią tarptautinę teisę, visų pirma JT chartiją, kurioje valstybės raginamos spręsti tarptautinius ginčus taikiomis priemonėmis ir savo tarptautiniuose santykiuose susilaikyti nuo grasinimų panaudoti jėga ir jos panaudojimo tiek prieš kurios nors valstybės teritorinį vientisumą arba politinę nepriklausomybę, tiek bet kuriuo kitu būdu, nesuderinamu su Jungtinių Tautų tikslais;

C. kadangi pastaraisiais metais pastebėjome, kad nuolat daugėjo valstybinių ir nevalstybinių subjektų vykdomų kibernetinių kenkimo operacijų, nukreiptų prieš ES ir jos valstybes nares ir rodančių, kad Europos saugumui būtini tinklai yra pažeidžiami; kadangi didėja puolamųjų kibernetinių subjektų įvairovė, sudėtingumas ir skaičius; kadangi dėl šių išpuolių pirmiausia turi būti stiprinamas gynybos pajėgumas ir plėtojami Europos kibernetiniai pajėgumai; kadangi kenksmingi kibernetiniai išpuoliai galimi bet kada ir tiek ES, tiek nacionaliniu lygmenimis subjektai turėtų būti skatinami imtis būtinų priemonių veiksmingiems kibernetinės gynybos pajėgumams nuolat palaikyti taikos metu;

D. kadangi COVID-19 pandemija ir padidėjęs kibernetinis nesaugumas parodė, kad būtini tarptautiniai susitarimai; kadangi COVID-19 pandemijos metu kibernetinių išpuolių labai padaugėjo ir kadangi ES ir jos valstybės narės stebėjo kibernetines grėsmes ir kibernetinę kenkimo veiklą, nukreiptą prieš pagrindinius veiklos vykdytojus, įskaitant išpuolius, kuriais siekiama sutrikdyti ypatingos svarbos infrastruktūrą, pvz., energetikos, transporto ir sveikatos priežiūros sistemas, taip pat didelį užsienio kišimąsi pasinaudojant kibernetine erdve, dėl kurio išnyko riba tarp taikos ir karo veiksmų; kadangi Europos ekonomikos gaivinimo plane numatytos papildomos investicijos į kibernetinį saugumą;

E. kadangi kibernetinė erdvė šiuo metu yra pripažįstama veiklos sritimi; kadangi kibernetinės grėsmės gali pakenkti visoms tradicinėms karinėms sritims ir kadangi tradicinės sritys priklauso nuo kibernetinės erdvės funkcionalumo, o ne atvirkščiai; kadangi konfliktai gali vykti visose fizinėse (sausumos, oro, jūrų ir kosmoso) ir virtualiose (kibernetinėje) srityse ir gali būti plečiami hibridinio karo elementais, pvz., dezinformacijos kampanijomis pasinaudojant kibernetine erdve, per trečiąsias šalis vykdomais karais, kibernetinių pajėgumų naudojimu puolimo ir gynybos tikslais ir strateginiais išpuoliais prieš skaitmeninių paslaugų teikėjus siekiant sutrikdyti ypatingos

[1] OL C 28, 2020 1 27, p. 57.

svarbos infrastruktūrą bei mūsų demokratines institucijas, taip pat sukelti didelių finansinių nuostolių;

F. kadangi Europos išorės veiksmų tarnyba (EIVT), Komisija ir Europos gynybos agentūra (EGA) turėtų remti valstybes nares joms koordinuojant ir dedant daugiau pastangų siekiant užtikrinti kibernetinės gynybos pajėgumus ir technologijas, atsižvelgiant į visus pajėgumų plėtojimo aspektus, įskaitant doktriną, lyderystę, organizavimą, personalą, mokymą, pramonę, technologijas, infrastruktūrą, logistiką, sąveikumą ir išteklius;

G. kadangi kuriant 2017 m. poreikių katalogą, kuris naudojamas siekiant nustatyti visus bendros saugumo ir gynybos politikos (BSGP) karinius poreikius pagal keletą pavyzdinių scenarijų, kibernetinės gynybos pajėgumų poreikis tapo vienu iš svarbiausių prioritetų;

H. kadangi sėkmingas ES misijų ir operacijų vykdymas vis labiau priklauso nuo nepertraukiamos prieigos prie saugios kibernetinės erdvės, todėl tam reikia atsparių kibernetinės veiklos pajėgumų;

I. kadangi 2018 m. atnaujintuose ES kibernetinės gynybos politikos metmenyse (KGPM) nustatyti tokie prioritetai kaip kibernetinės gynybos pajėgumų plėtojimas bei BSGP ryšių ir informacijos tinklų apsauga;

J. kadangi Komisijos pirmininkė savo 2021 m. pranešime apie Sąjungos padėtį pabrėžė, kad reikia sukurti ES kibernetinės gynybos politiką;

K. kadangi vis didesnė dirbtinio intelekto integracija į gynybos pajėgų kibernetinius pajėgumus (kibernetines fizines sistemas, įskaitant komunikacijos ir duomenų ryšius tarp transporto priemonių tinklu pagrįstoje sistemoje) gali sukelti pažeidžiamumą elektroninių karo išpuolių, pvz., trukdymo, apsimetinėjimo ar įsilaužimo, atžvilgiu;

L. kadangi Europos skaitmeninių ir geopolitinių užmojų sėkmė yra glaudžiai susijusi su ES kibernetinio saugumo ir kibernetinės gynybos lygio didinimu, kuris padidintų atsparumą ir padėtų laiku reaguoti į kibernetinių išpuolių sudėtingumo ir grėsmės augimą; kadangi ES, įtvirtinusi kibernetinio saugumo kultūrą ir plėtodama stiprias kibernetinio saugumo technologijas, įskaitant gebėjimą laiku ir veiksmingai nustatyti ir atsekti kenkėjiškus veiksmus ir tinkamai į juos reaguoti, galėtų apsaugoti savo piliečius ir savo valstybių narių saugumą;

M. kadangi tarptautinės teroristų organizacijos įgijo daugiau praktinės patirties kibernetinio karto srityje bei dažniau jo imasi ir kibernetinių išpuolių vykdytojai naudoja pažangiausias technologijas, kad ištirtų sistemų ir prietaisų pažeidžiamumą ir rengtų didelio ir labai didelio masto kibernetinius išpuolius;

N. kadangi gynybos ir kosmoso pramonėje susiduriama su precedento neturinčia pasauline konkurencija ir plataus masto technologiniais pokyčiais kuriant pažangias kibernetines technologijas; kadangi Europos Audito Rūmai atkreipė dėmesį į pajėgumų spragas IRT technologijų, kibernetinio karo ir dirbtinio intelekto srityse; kadangi ES yra grynoji kibernetinio saugumo produktų ir paslaugų importuotoja, o tai padidina technologinės priklausomybės ir pažeidžiamumo ne ES veiklos vykdytojų atžvilgiu riziką; kadangi bendri ES dirbtinio intelekto pajėgumai turėtų panaikinti techninę nelygybę ir užtikrinti, kad atitinkamų technologijų ir pramonės srities ekspertinių žinių arba gebėjimų diegti dirbtinio intelekto sistemas savo gynybos ministerijose neturinčios valstybės neatsiliktų;

O. kadangi su šnipinėjimo programa „Pegasus“ susijęs skandalas parodė, kad buvo šnipinėjami daugybė žurnalistų, žmogaus teisių aktyvistų, išrinktų atstovų ir kitų ES piliečių; kadangi įvairūs valstybiniai subjektai, tokie kaip Rusija, Kinija ir Šiaurės Korėja, dalyvavo kibernetinėje kenkimo veikloje, siekdami politinių, ekonominių ar saugumo tikslų, įskaitant išpuolius prieš ypatingos svarbos infrastruktūros objektus, kibernetinį šnipinėjimą ir masinį ES piliečių sekimą, pagalbą dezinformacijos kampanijoms ir kenkimo programinės įrangos platinimą, taip pat prieigos prie interneto ir IT sistemų veikimo ribojimą; kadangi vykdant tokią veiklą nepaisoma tarptautinės teisės, žmogaus teisių ir ES pagrindinių teisių ir jos yra pažeidžiamos, taip pat keliama grėsmė demokratijai, saugumui, viešajai tvarkai ir ES strateginiam savarankiškumui, todėl pateisinamas bendras ES atsakas, pvz., bendro ES diplomatinio atsako sistema, įskaitant ribojamųjų priemonių, numatytų ES kibernetinės diplomatijos priemonių rinkiniui, naudojimą;

P. kadangi 2020 m. liepos 30 d. Taryba pirmą kartą priėmė sprendimą nustatyti ribojamąsias priemones asmenims, subjektams ir įstaigoms, atsakingiems už įvairius kibernetinius išpuolius arba dalyvaujantiems juos vykdant, siekdama geriau užkirsti kelią kenkimo veiklai kibernetinėje erdvėje, nuo jos atgrasyti, nukreipti ir į ją reaguoti; kadangi 2019 m. gegužės mėn. buvo priimta ES kibernetinių sankcijų režimų teisinė sistema;

Q. kadangi įvairių formų atsakomybės nustatymas yra pagrindinė kibernetinės diplomatijos ir atgrasymo strategijų sudedamoji dalis;

R. kadangi per pastaruosius metus ES ir NATO bendradarbiavimas suintensyvėjo įvairiose srityse, įskaitant kibernetinį saugumą ir gynybą, atsižvelgiant į 2016 m. ES ir NATO bendrą deklaraciją;

S. kadangi Jungtinių Tautų vyriausybių ekspertų grupės (UN GGE) 2010 m., 2013 m. ir 2015 m. bendro sutarimo ataskaitos, kurias patvirtino JT Generalinė Asamblėja, sudaro visuotinę kibernetinio stabilumo norminę sistemą, kuri apima pripažinimą, kad galiojanti tarptautinė teisė, įskaitant visą JT Chartiją, ir 11 savanoriškų neprivalomų atsakingo valstybių elgesio normų taikomos kibernetinėje erdvėje, taip pat pasitikėjimo stiprinimo priemones bei pajėgumų stiprinimą;

ES kibernetinės gynybos pajėgumų padėtis

1. pabrėžia, kad bendra kibernetinės gynybos politika ir platus ES lygmens bendradarbiavimas kuriant bendrus ir didesnius kibernetinės gynybos pajėgumus – tai pagrindiniai elementai siekiant kurti glaudesnę ir tvirtesnę Europos gynybos sąjungą, ir tam reikia įvairių kompleksinių techninių, strateginių ir veiklos pajėgumų; pažymi, kad kibernetinė gynyba – tai veiksmai, priemonės ir procesai, kurie yra proporcingi ir atitinka tarptautinę teisę bei apima tiek karinius, tiek civilinius elementus ir kuriais siekiama, be kita ko, apsaugoti BSGP ryšių ir informacijos tinklus, BSGP misijas ir operacijas bei padėti valstybėms narėms; pabrėžia, kad reikia nedelsiant plėtoti ir stiprinti tiek bendrus, tiek valstybių narių karinius kibernetinės gynybos pajėgumus;

2. primena, kad tarpvalstybinis kibernetinės erdvės pobūdis, taip pat didelis kibernetinių išpuolių, kurie tampa vis sudėtingesni, skaičius reikalauja koordinuoto Sąjungos lygmens atsako, įskaitant bendrus valstybių narių paramos pajėgumus ir valstybių narių paramą ES kibernetinės diplomatijos priemonių rinkiniui, taip pat intensyvesnio ES ir NATO bendradarbiavimo, grindžiamo keitimusi informacija tarp reagavimo į

kibernetines krizes grupių, keitimusi geriausia patirtimi, intensyvesniais mokymais, moksliniais tyrimais ir pratybomis;

3. teigiamai vertina kibernetinės gynybos politikos metmenis (KGPM) kaip priemonę, kuria remiama valstybių narių kibernetinės gynybos pajėgumų plėtra; pabrėžia, kad persvarstant KGPM turėtų būti pirmiausia atkreiptas dėmesys į esamas ES ir nacionalinių karinių struktūrų spragas ir pažeidžiamumą; pabrėžia, kad turi būti sustiprintas koordinavimas tarp ES institucijų, agentūrų ir įstaigų, tarp valstybių narių ir su jomis, taip pat su Europos Parlamentu, siekiant užtikrinti, kad pagal atnaujintus kibernetinės gynybos politikos metmenis būtų pasiekti ES kibernetinės gynybos tikslai;

4. ragina EIVT ir Europos Komisiją, bendradarbiaujant su valstybėmis narėmis, toliau formuoti visapusišką priemonių rinkinį ir nuoseklią IT saugumo politiką siekiant stiprinti atsparumą ir karinės kibernetinės gynybos koordinavimą; primygtinai ragina stiprinti bendradarbiavimą su ES civiline Kompiuterinių incidentų tyrimo tarnyba (CERT-EU), siekiant apsaugoti visų ES institucijų, įstaigų ir agentūrų naudojamus tinklus, glaudžiai bendradarbiaujant su vyriausiaisiais informaciniais pareigūnais atitinkamuose subjektuose, taip pat ES institucijų, įstaigų ir agentūrų ryšius su valstybėmis narėmis; ragina Parlamentą užtikrinti, kad jo dalyvavimas CERT-EU veikloje užtikrintų tokį IT saugumo lygį, kuris sudarytų jam sąlygas gauti visą reikiamą įslaptintą ir neįslaptintą informaciją ir vykdyti savo pareigas pagal Sutartis, įskaitant kylančias iš dabartinio proceso, kuriuo siekiama pakeisti 2002 m. tarpinstitucinį susitarimą dėl galimybės gauti informaciją saugumo ir gynybos srityje; ragina EIVT užtikrinti tinkamą EIVT turto, patalpų ir veiklos, įskaitant būstinę, ES delegacijas ir BSGP misijas bei operacijas, kibernetinio saugumo lygį;

5. atkreipia dėmesį į 2018 m. kibernetinės gynybos politikos metmenų tikslą sukurti ES karinį kompiuterinių incidentų tyrimo tarnybų (CERT) tinklą; ragina valstybes nares gerokai padidinti keitimosi įslaptinta informacija pajėgumus, kad būtų sudarytos palankesnės sąlygos dalytis informacija, kai tai reikalinga ir naudinga, ir sukurti spartų ir saugų Europos tinklą, skirtą kibernetinių išpuoliams aptikti, įvertinti ir į juos reaguoti;

6. primena, kad pagal Pajėgumų plėtojimo planą parengtuose 2018 m. ES pajėgumų plėtojimo prioritetuose apsvarstytas poreikis plėtoti visapusiškus pajėgumus, o kibernetinė gynybą įvardyta pagrindiniu prioritetu; primena, kad Pajėgumų plėtojimo plane pabrėžta, jog informuotumo apie kibernetinę padėtį technologijos ir gynybinės kibernetinės technologijos yra labai svarbios kovojant su grėsmėmis saugumui; teigiamai vertina tai, kad Europos gynybos agentūra (EGA) remia valstybes nares didinant jų pajėgumus siekiant pagerinti kibernetinį atsparumą, pavyzdžiui, gebėjimą aptikti bet kokius kibernetinius išpuolius, juos atlaikyti ir atsigauti po jų; atkreipia dėmesį į įvairias priemones, kurių EGA ėmėsi valstybės narės, įskaitant EGA projektą „Kibernetinės gynybos reikalavimų inžinerija“ (CyDRE), pagal kurį turėtų būti sukurta kibernetinės erdvės operacijų organizacinė struktūra, įskaitant taikymo sritį, funkcijas ir reikalavimus, remiantis nacionaliniais ir ES teisės aktais;

7. ragina valstybes nares nustatyti bendrą komunikacijos standartą, kuris galėtų būti naudojamas įslaptintai ir neįslaptintai informacijai, siekiant padidinti reagavimo greitį ir užtikrinti kovos su kibernetiniais išpuoliais tinklo saugumą;

8. teigiamai vertina suderintą metinę peržiūrą gynybos srityje (CARD), kuri yra pirmoji visapusiška apžvalga gynybos srityje ES lygmeniu ir viena iš pagrindinių priemonių, kuria remiamas bendras valstybių narių gynybos išlaidų, gynybos planavimo bei

bendradarbiavimo gynybos srityje nuoseklumas ir kuria turėtų būti padedama skatinti investicijas į kibernetinės gynybos pajėgumų plėtojimą;

9. palankiai vertina pažangą, jau pasiektą įgyvendinant Europos gynybos pramonės plėtros programą vykdant keletą susijusių žvalgybos, saugaus ryšio ir kibernetinės gynybos projektų; ypač palankiai vertina raginimą sukurti lengvai dislokuojamą ir tarpusavyje sujungtą kibernetinių gynybos priemonių rinkinį ir tai, kad Europos gynybos fondas (EGF) taip pat padės stiprinti atsparumą, pasirengimą, reagavimą ir bendradarbiavimą kibernetinėje srityje, su sąlyga, kad dėl tokio prioriteto bus nuspręsta derantis dėl atitinkamų EGF veiklos programų; pabrėžia, kad ES pajėgumas plėtoti kibernetinės gynybos projektus priklauso nuo technologijų, įrangos, paslaugų, duomenų tvarkymo ir pačių duomenų kontrolės, taip pat nuo patikimų sektorių suinteresuotųjų subjektų bazės, kartu ragina visapusiškai įgyvendinti Viešųjų pirkimų gynybos srityje direktyvą[1] ir užtikrinti jos vykdymą; ragina valstybes nares pasinaudoti EGF teikiamomis galimybėmis siekiant kartu plėtoti kibernetinės gynybos pajėgumus;

10. teigiamai vertina sustiprintą valstybių narių bendradarbiavimą kibernetinės gynybos ir vadovavimo, kontrolės, ryšių, kompiuterių, žvalgybos, sekimo ir iššvalgymo (C4ISR) srityje bei pažangą įgyvendinant nuolatinį struktūrizuotą bendradarbiavimą (PESCO), be kita ko, įgyvendinant konkrečius projektus, pavyzdžiui, Greitojo reagavimo į kibernetinius incidentus komandų ir savitarpio pagalbos kibernetinio saugumo srityje projektą; primena, kad įgyvendinant EGF ir PESCO sudaromos puikios galimybės plėtoti kibernetinės gynybos pajėgumus ir paspartinti kibernetinio saugumo iniciatyvas, pavyzdžiui, naudojantis Dalijimosi informacija apie reagavimą į kibernetines grėsmes ir incidentus platforma ir Kibernetinės ir informacinės srities koordinavimo centru; ragina visas valstybes nares užtikrinti nuoseklumą ir sutelkti dėmesį į kibernetinius pajėgumus, kuriant bendrą strateginį požiūrį į prioritetus; ragina skatinti mokslinius tyrimus, inovacijas ir keitimąsi ekspertinėmis žiniomis, kad būtų visapusiškai išnaudotos PESCO ir EGF galimybės; palankiai vertina 2020 m. lapkričio 5 d. Tarybos sprendimą leisti trečiosioms šalims tam tikrais konkrečiais atvejais prisijungti prie atskirų PESCO projektų, atsižvelgiant į tai, kad jie gali suteikti pridėtinės vertės ir teikti technines ekspertines žinias bei papildomus pajėgumus, jei jie atitinka sutartas politines, materialines ir teisines sąlygas; pabrėžia, kad ES gali būti strategiškai naudinga, jei išimties tvarka kiekvienu konkrečiu atveju valstybės narės ir ES nepriklausančios valstybės dalyvautų su kibernetine erdve susijusiuose PESCO projektuose, kad būtų įvykdyti platesnio užmojo įsipareigojimai, remiantis veiksmingu abipusiškumu;

11. pabrėžia, kad kibernetinė gynyba yra laikoma operatyvine visų BSGP misijų užduotimi ir kad kibernetinis atsparumas ir susiję pajėgumai turi būti nustatyti, patikrinti ir dislokuoti prieš pradedant BSGP planavimo procesus; primena, kad sėkmingas ES misijų ir veiklos vykdymas vis labiau priklauso nuo nepertraukiamos prieigos prie saugios kibernetinės erdvės, todėl reikia tvirtų ir atsparių kibernetinės veiklos pajėgumų, taip pat būtina tinkamai reaguoti į išpuolius prieš karinę infrastruktūrą, misijas ir operacijas; pabrėžia, kad, laikantis Susitarimo dėl civilinių BSGP misijų pajėgumų, turi būti užtikrintas civilinių BSGP pajėgumų kibernetinis atsparumas ir jais prireikus turi būti remiamos priimančiosios šalys, be kita ko, vykdant stebėseną, kuravimą ir konsultacijas; rekomenduoja išnagrinėti galimybes skatinti mūsų partnerių

---

[1] 2009 m. liepos 13 d. Europos Parlamento ir Tarybos direktyva 2009/81/EB dėl darbų, prekių ir paslaugų pirkimo tam tikrų sutarčių, kurias sudaro perkančiosios organizacijos ar subjektai gynybos ir saugumo srityse, sudarymo tvarkos derinimo (OL L 216, 2009 8 20, p. 76).

kibernetinių pajėgumų stiprinimą, pavyzdžiui, išplėsti ES mokymo misijų įgaliojimus, kad jos taip pat apimtų kibernetinės gynybos aspektus, arba pradėti civilines kibernetines misijas;

12. teigiamai vertina Tarybos 2019 m. gegužės 14 d. sprendimą dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais, pagal kurį leidžiama taikyti ribojamąsias priemones skirtas atgrasyti nuo kibernetinių išpuolių, keliančių grėsmę ES ar jos valstybėms narėms, įskaitant kibernetinius išpuolius prieš trečiąsias valstybes ar tarptautines organizacijas, ir į juos reaguoti; teigiamai vertina tai, kad tokios ribojamosios priemonės pritaikytos 2020 m. liepos mėn. ir 2020 m. spalio mėn., nes tai yra įtikinamas žingsnis įgyvendinant ES kibernetinės diplomatijos priemonių rinkinį, įskaitant ribojamąsias priemones, ir stiprinant ES kibernetinio atgrasymo poziciją; ragina toliau plėtoti ir griežtai vykdyti proporcingų ribojamųjų priemonių sistemą, skirtą kibernetiniams išpuoliams sustabdyti, kartu laikantis Europos vizijos dėl interneto, kuris turi būti vienas, atviras, neutralus, laisvas, saugus ir nesuskaidytas tinklas;

13. primena, kad, atsižvelgiant į dvejopą kibernetinių technologijų pobūdį, saugūs civiliniai produktai ir paslaugos yra labai svarbūs kariuomenei ir padeda užtikrinti geresnę kibernetinę gynybą; todėl teigiamai vertina ES kibernetinio saugumo agentūros (ENISA) kartu su valstybėmis narėmis ir suinteresuotaisiais subjektais vykdomą darbą, siekiant suteikti ES IRT produktų, paslaugų ir procesų sertifikavimo schemas, kad būtų padidintas bendras kibernetinio saugumo lygis bendrojoje skaitmeninėje rinkoje; pabrėžia esminį novatorišką ES vaidmenį rengiant standartus, kuriais formuojama kibernetinio saugumo aplinka, prisidedama prie sąžiningos konkurencijos Europos Sąjungoje ir pasauliniu mastu ir reaguojama į trečiųjų šalių ekstrateritorines priemones bei šių šalių keliamą riziką saugumui; be to, pripažįsta svarbų ENISA vaidmenį remiant mokslinių tyrimų iniciatyvas ir kitų formų bendradarbiavimą, kuriuo siekiama didinti kibernetinį saugumą; pabrėžia investicijų į kibernetinės gynybos ir kibernetinio saugumo pajėgumus svarbą siekiant didinti ES ir valstybių narių atsparumą ir strateginius pajėgumus; šiuo atžvilgiu pabrėžia Skaitmeninės Europos programos ir programos „Europos horizontas“, ypač jos veiksmų grupės „Civilinis saugumas visuomenei“, svarbą; atkreipia dėmesį į tai, kad svarbios atitinkamos finansinės priemonės, numatytos pagal 2021–2027 m. daugiametę finansinę programą (DFP) ir Ekonomikos gaivinimo ir atsparumo didinimo priemonę (EGADP);

14. teigiamai vertina kai kurių ES valstybių narių pasiektą pažangą kuriant kibernetinės gynybos vadovavimo struktūras savo kariuomenėje;

Strateginė vizija: kibernetinės gynybos atsparumo užtikrinimas

15. pažymi, kad pagal Strateginį kelrodį bus sustiprintas ES užmojų saugumo ir gynybos srityje įgyvendinimas ir bus padedama juos įgyvendinti, taip pat šie užmojai bus paversti pajėgumų poreikiais, be kita ko, prioriteto tvarka kibernetinės gynybos srityje, ir taip bus padidintas ES ir valstybių narių gebėjimas nustatyti, aptikti kibernetinę kenkimo veiklą, užkirsti jai kelią, nuo jos atgrasyti, nukreipti, į ją reaguoti ir atsigauti po jos, stiprinant ES poziciją, informuotumą apie padėtį, teisinę ir etinę sistemą, priemones, procedūras ir partnerystes;

16. tvirtina, kad Strateginis kelrodis turėtų sustiprinti strateginę kultūrą kibernetinėje srityje ir pašalinti bet kokį pajėgumų ir įgaliojimų dubliavimąsi; pabrėžia, kad labai svarbu pašalinti dabartinį bendros kibernetinės struktūros susiskaidymą ir sudėtingumą

Europos Sąjungoje ir sukurti bendrą viziją, kaip pasiekti saugumą ir stabilumą kibernetinėje erdvėje;

17. pabrėžia, kad kartu su susiskaidymu kyla didelis susirūpinimas dėl išteklių ir darbuotojų trūkumo ES lygmeniu, trukdančio sukurti saugesnę skaitmeninę aplinką, todėl pabrėžia, kad reikia didinti ir išteklius, ir darbuotojų skaičių; primygtinai ragina pirmininko pavaduotoją ir vyriausiąjį įgaliotinį ir (arba) valstybes nares padidinti finansinius ir personalo, ypač kibernetinės žvalgybos analitikų ir kibernetinės kriminalistikos ekspertų, išteklius, taip pat stiprinti darbuotojų mokymą sprendimų ir politikos formavimo, politikos įgyvendinimo, reagavimo į kibernetinius incidentus ir tyrimų srityse, įskaitant kibernetinių įgūdžių ugdymą, siekiant stiprinti ES gebėjimą įvertinti kibernetinius išpuolius ir nustatyti jų vykdytojus, taip užtikrinant tinkamą greitą politinį, civilinį ir karinį atsaką; ragina toliau finansuoti CERT-EU ir ES žvalgybos ir situacijų centrą (INTCEN) bei remti valstybių narių veiklą steigiant ir stiprinant saugumo operacijų centrus (SOC), kad visoje ES būtų sukurtas SOC tinklas, kuris galėtų sustiprinti civilinį ir karinį bendradarbiavimą, kad būtų laiku įspėta apie kibernetinio saugumo incidentus;

18. pažymi, kad racionalizuotas ES karinis mokymas ir švietimas kibernetinėje srityje gerokai padidintų valstybių narių tarpusavio pasitikėjimą, pagerintų standartines veiklos procedūras ir užtikrintų aiškesnių taisyklių sukūrimą bei pagerintų vykdymą; atkreipia dėmesį į svarbią Europos saugumo ir gynybos koledžo (ESGK) mokymo veiklą kibernetinės gynybos srityje ir šiuo požiūriu teigiamai vertina Švietimo, mokymo, vertinimo ir pratybų (angl. ETEE) kibernetinėje srityje platformos, kuria siekiama spręsti kibernetinio saugumo ir gynybos mokymų teikimo civiliniam ir kariniam personalui problemas, taip pat nustatyti būtiną kibernetinės srities mokymo suderinimą ir standartizavimą, sukūrimą; pabrėžia, kad ESGK turėtų labiau pasinaudoti struktūriniu Sąjungos finansavimu, kad galėtų padidinti savo indėlį į ES kibernetinės gynybos įgūdžių stiprinimą, visų pirma atsižvelgiant į padidėjusį aukščiausio lygio kibernetinių ekspertų poreikį; ragina valstybes nares propaguoti partnerystę su akademine bendruomene, siekiant skatinti kibernetinio saugumo srities mokslinių tyrimų ir plėtros programas, kad būtų galima plėtoti naujas bendras technologijas, priemones ir įgūdžius, taikomus tiek civiliniame, tiek gynybos sektoriuose; pabrėžia, kad švietimas svarbus didinant visuomenės informuotumą ir tobulinant piliečių įgūdžius, kad jie galėtų apsiginti nuo kibernetinių išpuolių;

19. pabrėžia, kad ES kibernetinės gynybos politikoje reikia atsižvelgti į lyčių aspektą ir būti plačių užmojų mažinant lyčių nelygybę tarp kibernetinės gynybos specialistų, visų pirma pasitelkiant aktyvią lyčių integravimo politiką ir moterims pritaikytas mokymo programas;

20. primena, kad kibernetinė gynyba turi tiek karinį, tiek civilinį matmenį, todėl reikalingas tvirtesnis bendradarbiavimas, sinergija ir priemonių suderinamumas; pabrėžia, kad pirmiausia reikia išanalizuoti bei aptarti bendradarbiavimo ir koordinavimo, taip pat žmogiškųjų ir techninių išteklių spragas tiek nacionaliniu, tiek ES lygmeniu; pažymi, kad sėkmingą karinių ir civilinių išteklių integravimą galima užtikrinti tik per mokymus ir pratybas su visais atitinkamai suinteresuotaisiais subjektais; atsižvelgdamas į tai, atkreipia dėmesį į NATO pratybas „Suglausti skydai“ (angl. „Locked shields“) kaip vieną iš geriausių civilinių ir karinių kibernetinės gynybos pajėgumų tikrinimo ir tobulinimo pavyzdžių; todėl ragina pirmininko pavaduotoją ir vyriausiąjį įgaliotinį bei Komisiją parengti integruotą politinę strategiją ir skatinti karinio CERT tinklo, CERT-EU ir CSIRT tinklo sinergiją ir glaudų bendradarbiavimą;

21. teigiamai vertina pirmininko pavaduotojo ir vyriausiojo įgaliotinio bei Komisijos bendrą komunikatą „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“, kuriuo siekiama stiprinti civilinės, gynybos ir kosmoso sričių kibernetinės veiklos sinergiją ir bendradarbiavimą; laikosi nuomonės, kad ši strategija yra svarbus žingsnis stiprinant ES ir valstybių narių kibernetinį atsparumą, taip stiprinant ES pirmavimą skaitmeninėje srityje ir jos strateginius pajėgumus;

22. rekomenduoja įsteigti Jungtinį kibernetinio saugumo padalinį, kad būtų sustiprintas bendradarbiavimas siekiant reaguoti į nepakankamą keitimąsi informacija tarp ES institucijų, įstaigų ir agentūrų, užtikrinant saugų ir greitą keitimosi informacija tinklą, taip pat sudaryti sąlygas visapusiškai išnaudoti esamas struktūras, išteklius ir pajėgumus; atkreipia dėmesį į svarbų vaidmenį, kurį galėtų atlikti Jungtinis kibernetinio saugumo padalinys apsaugant ES nuo sunkių tarpvalstybinių kibernetinių išpuolių, remiantis sektorių dalijimosi informacija koncepcija; pabrėžia koordinavimo svarbą siekiant išvengti struktūrų ir atsakomybės dubliavimosi padalinio kūrimo etapu; šiuo atžvilgiu palankiai vertina 2021 m. birželio 23 d. Komisijos rekomendaciją, kurioje nustatyta, kad turėtų būti sukurtos specialios sąsajos su Jungtiniu kibernetinio saugumo padaliniu, siekiant sudaryti sąlygas keistis informacija su kibernetinės gynybos bendruomene, visų pirma per EIVT atstovavimą; taip pat pabrėžia, kad Jungtinį kibernetinio saugumo padalinį turėtų paremti atitinkamų PESCO projektų atstovai, ypač informuotumo apie padėtį ir pasirengimo imtis veiksmų klausimais;

23. primena, kad, atsižvelgiant į dažną dvejopą kibernetinės gynybos pajėgumų naudojimą, jų stiprinimui taip pat reikia užtikrinti ekspertines žinias apie informacijos saugumą ir civilinius tinklus; pabrėžia, kad dvejopo naudojimo standartinių sistemų plitimas gali kelti sunkumų, nes sistemomis naudojasi vis daugiau valstybinių ir nevalstybinių priešiškų subjektų; ragina Komisiją ir valstybes nares naudoti keletą svertų, pvz., sertifikavimą ir privačiojo sektoriaus subjektų atsakomybės priežiūrą; pabrėžia, kad technologines inovacijas daugiausia skatina privačiojo sektoriaus įmonės, todėl bendradarbiavimas su privačiojo sektoriaus ir civiliais suinteresuotaisiais subjektais, įskaitant pramonės įmones ir subjektus, susijusius su ypatingos svarbos infrastruktūros objektų valdymu, taip pat MVĮ, pilietinę visuomenę, organizacijas ir akademinę bendruomenę, yra labai svarbus ir turėtų būti stiprinamas; atkreipia dėmesį tai, kad pasiūlyta peržiūrėti Direktyvą dėl tinklų ir informacinių sistemų saugumo (TIS direktyva), taip pat į pasiūlymą dėl direktyvos dėl ypatingos svarbos subjektų atsparumo, siekiant apsaugoti ypatingos svarbos infrastruktūros objektus, stiprinti tiekimo grandinės saugumą ir reguliuojamų subjektų įtraukimą į skaitmeninę ekosistemą; primena, kad kiekviena valstybė narė turėtų įgyvendinti specialią kibernetinio saugumo tiekimo grandinės rizikos valdymo politiką, visų pirma sprendžiat patikimų pardavėjų klausimą; primena, kad TIS direktyvoje turėtų būti gerbiama valstybių narių kompetencija, ir siūlo atsižvelgti į atitinkamas Saugumo ir gynybos pakomitečio nuomones dėl abiejų pasiūlymų;

24. teigiamai vertina 2020 m. rugsėjo 29 d. įsteigtą Ryšių palaikymo dėl kibernetinių krizių organizacinis tinklą (CyCLONe), kuris dar labiau padidino galimybes laiku keistis informacija ir informuoti apie padėtį, panaikinant atotrūkį tarp ES techninio ir politinio lygmenų; pažymi, kad siekiant užtikrinti veiksmingos kibernetinės gynybos pajėgumus, reikia pakeisti dalijimosi informacija kultūrą iš pagrįstos principu „būtina žinoti“ į pagrįstą principu „būtina dalytis“;

25. palankiai vertina Komisijos Civilinės, kosmoso ir gynybos pramonės sinergijos veiksmų planą ir primena, kad šie trys sektoriai kibernetinės gynybos srityje yra glaudžiai

tarpusavyje susiję; pažymi, kad, kitaip nei kitose karinėse srityse, kibernetinei erdvei „kurti“ naudojamą infrastruktūrą visų pirma valdo komerciniai subjektai, daugiausia įsteigti už ES ribų, o tai sukuria pramoninę ir technologinę priklausomybę nuo trečiųjų šalių; yra tvirtai įsitikinęs, kad ES turi stiprinti savo technologinį suverenumą ir skatinti inovacijas, investuodama į etišką naujų technologijų, pvz., dirbtinio intelekto ir kvantinės kompiuterijos, naudojimą saugumo ir gynybos srityse; primygtinai ragina valstybėse narėse vystyti mokslinių tyrimų ir plėtros darbotvarkę, sutelktą į dirbtinį intelektą; vis dėlto pabrėžia, kad dirbtinio intelekto naudojimas karinėje srityje turi atitikti tarptautinę žmogaus teisių teisę ir tarptautinę humanitarinę teisę ir kad ES turi imtis iniciatyvos propaguodama pasaulinę dirbtinio intelekto reglamentavimo sistemą, pagrįstą demokratinėmis vertybėmis ir „žmogaus priežiūros“ principu (angl. „human-in-the-loop approach“);

26. atkreipia dėmesį į tai, kad ES palydovų centras (SATCEN) vykdo svarbų darbą, ir pabrėžia, kad Sąjunga turi turėti pakankamai išteklių kosmoso vaizdų ir žvalgybos duomenų rinkimo srityse; prašo šios agentūros išanalizuoti ir pateikti ataskaitą dėl ES ir valstybių narių palydovų saugumo ir (arba) pažeidžiamumo kosminių šiukšlių ir kibernetinių išpuolių atžvilgiu; pabrėžia, kad ES SATCEN turėtų gauti daugiau struktūrinių Sąjungos lėšų, kad galėtų toliau prisidėti prie Sąjungos veiksmų; pabrėžia, kad kibernetinės gynybos pajėgumai yra nepaprastai svarbūs užtikrinant saugų ir atsparų keitimąsi informacija su SATCEN tiek saugumo iš kosmoso, tiek kosmoso srityse, siekiant išsaugoti ir sustiprinti ES strateginį savarankiškumą informuotumo apie padėtį srityje; pabrėžia, kad ES turi stengtis užkirsti kelią ginklavimuisi kosmose;

27. palankiai vertina Tarybos sprendimą Bukarešte įsteigti Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą, kuris paskirstys su kibernetiniu saugumu susijusį finansavimą pagal programą „Europos horizontas“ ir Skaitmeninės Europos programą, taip pat ragina sklandžiai bendradarbiauti su centro nacionalinių koordinavimo centrų tinklu; pabrėžia šio centro svarbą įgyvendinant atitinkamus kibernetinio saugumo projektus ir iniciatyvas, kurios padės sukurti naujus pajėgumus, būtinus Sąjungos atsparumui palaikyti bei civilinio ir gynybos kibernetinio saugumo sektorių koordinavimui sustiprinti; pabrėžia, kad Kibernetinio saugumo kompetencijos centro veikloje turi dalyvauti pagrindiniai Europos suinteresuotieji subjektai, įskaitant pramonę, akademines bei mokslinių tyrimų organizacijas ir kitas atitinkamas pilietinės visuomenės asociacijas, kad kibernetinio saugumo ekspertinės žinios būtų kaupiamos ir skleidžiamos visoje ES;

28. pabrėžia šifravimo ir teisėtos prieigos prie šifruotų duomenų svarbą; primena, kad duomenų šifravimas bei tokių pajėgumų stiprinimas ir kuo platesnis jų naudojimas gali stipriai padidinti valstybių, visuomenių ir pramonės kibernetinį saugumą; skatina įgyvendinti Europos skaitmeninio suvereniteto programą, siekiant puoselėti ir stiprinti esamus kibernetinių ir šifravimo priemonių pajėgumus, įkvėptus pagrindinių Europos teisių ir vertybių, tokių kaip privatumas, saviraiškos laisvė ir demokratija, siekiant sustiprinti Europos konkurencingumą kibernetinio saugumo rinkoje ir padidinti vidaus paklausą;

29. palankiai vertina būsimą karinę viziją ir strategiją dėl kibernetinės erdvės kaip operacijų srities, kurioje kibernetinė erdvė bus apibrėžta kaip ES BSGP operacijų sritis: ragina nuolat vertinti BSGP misijų informacinės infrastruktūros pažeidžiamumą ir įgyvendinti bendrus suderintus švietimo, mokymo ir pratybų kibernetinės gynybos srityje standartus, siekiant remti BSGP misijas;

30. apgailestauja dėl to, kad dabartiniai ES Karinių misijų planavimo ir vykdymo centro (MPCC) įslaptintų sistemų trūkumai varžo jo pajėgumus; todėl ragina EIVT skubiai suteikti MPCC pažangiausią autonominę ir saugią ryšių ir informacinę sistemą, kuria galima tvarkyti ES slaptus duomenis jos BSGP misijose ir operacijose, užtikrinant deramą apsaugą ir atsparumą dislokuotam pajėgų štabui;

31. ragina toliau integruoti kibernetinį saugumą į ES reagavimo į krizes mechanizmus ir susieti esamas įvairių kibernetinių bendruomenių iniciatyvas, struktūras ir procedūras siekiant padidinti valstybių narių savitarpio pagalbą ir operatyvų bendradarbiavimą, visų pirma didelių kibernetinių išpuolių atveju, kad būtų padidintas sąveikumas ir plėtojamas bendras supratimas apie kibernetinę gynybą; tvirtai pabrėžia, kad svarbu vykdyti tolesnes pratybas, bet tai reikia daryti dažniau, ir scenarijais grindžiamas politikos diskusijas dėl krizių valdymo, be kita ko, dėl savitarpio pagalbos sąlygos (ES sutarties 42 straipsnio 7 dalis) didelio hipotetinio kibernetinio išpuolio atveju, kurį būtų galima laikyti ginkluotu išpuoliu; ragina, kad tokiomis iniciatyvomis būtų stiprinamas bendras supratimas apie savitarpio pagalbos ir (arba) solidarumo įgyvendinimo procedūras pagal ES sutarties 42 straipsnio 7 dalį ir SESV 222 straipsnį, be kita ko, siekiant konkretaus tikslo taikyti šias procedūras kibernetinių išpuolių prieš valstybes nares atveju; palankiai vertina 2021 m. birželio 14 d. NATO Briuselio aukščiausiojo lygio susitikimo komunikatą, kuriame dar kartą patvirtinamas NATO įsipareigojimas visada naudoti visus pajėgumus siekiant aktyviai atgrasyti nuo visų kibernetinių grėsmių, nuo jų apsisaugoti ir kovoti su jomis, įskaitant sprendimą kiekvienu konkrečiu atveju taikyti 5 straipsnį; teigiamai vertina tolesnes diskusijas dėl ES kibernetinio saugumo krizių valdymo sistemos ir kibernetinės diplomatijos priemonių rinkinio susiejimo;

32. pažymi, kad ES vis dažniau įsitraukia į hibridinius konfliktus su geopolitiniais priešininkais; pabrėžia, kad šie veiksmai yra ypač destabilizuojantys ir pavojingi, nes išnyksta ribos tarp karo ir taikos, destabilizuojamos demokratinės valstybės ir skleidžiamos abejonės tarp tikslinių gyventojų; primena, kad šie išpuoliai patys savaime dažnai nėra pakankamai rimti, kad būtų taikomas NATO sutarties 5 straipsnis arba ES sutarties 42 straipsnio 7 dalis, nors jie daro bendrą strateginį poveikį ir jų neįmanoma veiksmingai įveikti nukentėjusios valstybės narės atsakomosiomis priemonėmis; mano, kad dėl to ES turėtų stengtis rasti sprendimą, kaip užpildyti šį teisinį vakuumą, iš naujo išaiškinant ES sutarties 42 straipsnio 7 dalį ir Sutarties dėl Europos Sąjungos veikimo 222 straipsnį taip, kad būtų išlaikyta teisė į kolektyvinę gynybą, neviršijant kolektyvinės gynybos ribos, ir ES valstybėms narėms būtų leista savanoriškai imtis kolektyvinių priemonių ir dirbti kartu su sąjungininkais siekiant panašaus sprendimo tarptautiniu lygmeniu; pabrėžia, kad tai yra vienintelė veiksminga priemonė kovojant su sąstingiu reaguojant į hibridines grėsmes ir priemonė padidinti priešininkų išlaidas;

33. pakartoja, kad bendri tvirti priskyrimo pajėgumai yra viena iš pagrindinių ES ir valstybių narių pajėgumų stiprinimo priemonių ir esminė veiksmingos kibernetinės gynybos ir atgrasymo kibernetinėje erdvėje dalis; pabrėžia, kad pagerinus valstybių narių keitimąsi informacija, susijusia su technine informacija, analize ir žvalgybine informacija apie grėsmes ES lygmeniu, būtų sudarytos sąlygos bendram priskyrimui ES lygmeniu; pripažįsta, kad kibernetinė gynyba tam tikru mastu yra veiksmingesnė, jei ji apima ir tam tikrus puolamuosius būdus ir priemones, su sąlyga, kad jų naudojimas atitinka tarptautinę teisę; pabrėžia, kad aiškus kibernetinių išpuolių priskyrimas yra naudinga atgrasymo priemonė; ragina apsvarstyti bendro viešo kenkėjiškos kibernetinės veiklos priskyrimo galimybę, įskaitant galimybę parengti kibernetinio elgesio ataskaitas, remiant EIVT, apie konkrečius subjektus, kad būtų galima apibendrinti

valstybės remiamą kenkėjišką kibernetinę veiklą prieš valstybes nares ES lygmeniu;

34. laikosi nuomonės, kad nepaprastai svarbus yra ES ir NATO bendradarbiavimas kibernetiniais klausimais, nes juo būtų sudarytos sąlygos oficialiam bendram ir sustiprintam kenkėjiškų kibernetinių incidentų priskyrimui, taigi ir ribojamųjų sankcijų bei priemonių taikymui; pažymi, kad funkcinis atsparumas ir veiksmingas atgrasymas būtų užtikrinti, jei nusikalstamos veikos vykdytojai žinotų apie galimų atsakomųjų priemonių (pagrįstų kibernetinių išpuolių sunkumu, mastu ir taikiniu) katalogą, jų proporcingumą ir tinkamumą, jų atitiktį tarptautinei teisei, visų pirma JT chartijai;

35. teigiamai vertina Komisijos pirmininko pavaduotojo ir Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai pasiūlymą skatinti ir palengvinti valstybių narių ES kibernetinės žvalgybos darbo grupės įsteigimą ES žvalgybos ir situacijos centre (INTCEN), siekiant paskatinti strateginį bendradarbiavimą žvalgybos srityje kovojant su kibernetinėmis grėsmėmis ir veikla, kad būtų galima toliau remti ES informuotumą apie padėtį ir sprendimų dėl bendro diplomatinio atsakymo priėmimą; ragina toliau daryti pažangą rengiant bendrą pasiūlymų rinkinį, visų pirma užtikrinant nuolatinę sąveiką su ES hibridinių grėsmių analizės ir informavimo centru ir NATO hibridinių grėsmių analizės centru dalijantis informacija apie padėtį ir atliekant analizę, taip pat vykdant taktinį ir operatyvinį bendradarbiavimą;

Partnerystės stiprinimas ir ES vaidmens tarptautinėje arenoje didinimas

36. laikosi nuomonės, kad bendradarbiavimas su NATO kibernetinės gynybos srityje yra svarbus siekiant užkirsti kelią kibernetiniams išpuoliams, darantiems poveikį valstybių narių kolektyvinio saugumo sritims, atgrasyti nuo jų ir į juos reaguoti; ragina valstybes nares visapusiškai dalytis įrodymais ir žvalgybos duomenimis, kad būtų galima sudaryti kibernetinių sankcijų sąrašus; ragina šiuo klausimu aktyviau koordinuoti veiksmus su NATO dalyvaujant kibernetinėse pratybose ir bendruose mokymuose, pvz., lygiagrečiose ir suderintose pratybose (PACE);

37. pripažįsta, kad ES ir NATO turėtų koordinuoti veiksmus tais atvejais, kai priešiški veikėjai kelia grėsmę euroatlantiniams saugumo interesams; reiškia susirūpinimą dėl sistemingo agresyvaus elgesio, kurį pademonstravo Kinija, Rusija ir Šiaurės Korėja kibernetinėje erdvėje, įskaitant nemenką skaičių kibernetinių išpuolių prieš valdžios institucijas ir privačias bendroves; mano, kad ES ir NATO bendradarbiavimas turėtų būti sutelktas į problemas kibernetinių, hibridinių, besiformuojančių ir perversminių technologijų, kosmoso, ginklų kontrolės ir ginklų neplatinimo srityje; primygtinai ragina ES ir NATO bendradarbiauti užtikrinant atsparius, įperkamus ir saugius didelės spartos tinklus, atitinkančius ES ir nacionalinius saugumo standartus, kuriais būtų apsaugomi nacionaliniai ir tarptautiniai informacijos tinklai, galintys užšifruoti neskelbtinus duomenis ir ryšius;

38. teigiamai vertina CERT-EU ir NATO reagavimo į kompiuterinius incidentus tarnybos (NCIRC) susitarimą, kuriuo siekiama užtikrinti gebėjimą reaguoti į grėsmes tikruoju laiku, gerinant kibernetinių incidentų prevenciją, aptikimą ir reagavimą į juos tiek ES, tiek NATO; taip pat pabrėžia, kad svarbu didinti kibernetinės gynybos mokymo pajėgumus IT ir kibernetinių sistemų srityse bendradarbiaujant su NATO bendros kibernetinės gynybos kompetencijos centru (CCD COE) ir NATO ryšių ir informacijos (NCI) akademija;

39. ragina ES ir NATO toliau bendradarbiauti, visų pirma kibernetinės gynybos sąveikumo

reikalavimų srityje, ieškant galimo papildomumo ir abipusiai naudingo pajėgumų stiprinimo, siekiant atitinkamų BSGP struktūrų priskyrimo NATO federalinių misijų tinklui bei vengiant dubliavimosi ir pripažįstant atitinkamą jų atsakomybę; primygtinai ragina stiprinti ES PESCO ir NATO pažangiosios gynybos, jungtinių pajėgų iniciatyvą ir investicijų gynybos srityje įsipareigojimus ir skatinti išteklių telkimą ir dalijimąsi jais, siekiant kurti sąveiką ir efektyvumą tiekėjų ir galutinių naudotojų santykiuose; teigiamai vertina pažangą, kurią pasiekė ES ir NATO bendradarbiaudamos kibernetinės gynybos srityje, visų pirma keičiantis koncepcijomis ir doktrinomis, bendrai dalyvaujant kibernetinėse pratybose ir informaciniuose susirinkimuose, ypač krizių valdymo kibernetinio aspekto klausimu; siūlo sukurti bendrą ES ir NATO kibernetinių grėsmių informacijos centrą ir bendrą kibernetinio saugumo darbo grupę;

40. ragina valstybes nares, ES institucijas, NATO sąjungininkus, JT ir Europos saugumo ir bendradarbiavimo organizaciją (ESBO) glaudžiau koordinuoti kibernetinę gynybą; atsižvelgdamas į tai, ragina toliau skatinti ESBO pasitikėjimo kibernetinėje erdvėje stiprinimo priemones ir pabrėžia, kad reikia kurti veiksmingas tarptautinio bendradarbiavimo priemones, kuriomis būtų remiamas partnerių kibernetinių pajėgumų stiprinimas, taip pat plėtoti ir skatinti pasitikėjimo stiprinimo priemones ir įtraukų bendradarbiavimą su pilietine visuomene ir suinteresuotaisiais subjektais; teigiamai vertina 2021 m. balandžio 19 d. ES strategijoje dėl bendradarbiavimo Indijos ir Ramiojo vandenynų regione svarbą, teikiamą pasaulinei, atvirai, laisvai, stabiliai ir saugiai kibernetinei erdvei; ragina aktyviai plėtoti glaudesnius ryšius su panašiai mąstančiomis demokratinėmis šalimis Indijos ir Ramiojo vandenyno regione, tokiomis kaip JAV, Pietų Korėja, Japonija, Indija, Australija ir Taivanas, kad būtų galima keistis žiniomis ir patirtimi bei informacija kovojant su kibernetine grėsme; taip pat pabrėžia bendradarbiavimo su kitomis šalimis, ypač artimiausiose ES kaimyninėse šalyse, siekiant padėti stiprinti jų pajėgumus gintis nuo kibernetinio saugumo grėsmių, svarbą; teigiamai vertina Komisijos paramą kibernetinio saugumo programoms Vakarų Balkanuose ir Rytų partnerystės šalyse; pabrėžia, kad reikia nedelsiant taikyti tarptautinę teisę, įskaitant JT chartiją visa jos apimtimi, taip pat plačiu mastu pripažintą tarptautinę normatyvinę atsakingo valstybių elgesio kibernetinėje erdvėje sistemą, ir prisidėti prie JT vykstančių diskusijų dėl tarptautinės teisės taikymo elektroninėje erdvėje sąlygų;

41. pabrėžia tvirtos partnerystės kibernetinėje srityje su JK, kuri yra pirmaujanti valstybė pagal savo kibernetinės gynybos arsenalą, svarbą; ragina Komisiją išnagrinėti galimybę atnaujinti procesą, kuriuo siekiama ateityje sukurti oficialią ir struktūrizuotą bendradarbiavimo šioje srityje sistemą;

42. pabrėžia, kad būtina užtikrinti taiką ir stabilumą kibernetinėje erdvėje; ragina visas valstybes nares ir ES būti lyderėmis JT remiamose diskusijose ir iniciatyvose, be kita ko, pasiūlant veiksmų programą, siekiant taikyti iniciatyvų požiūrį kuriant tarptautiniu mastu pripažintą bendrą reglamentavimo sistemą ir padėti iš tikrųjų skatinti atskaitomybę, laikytis naujų normų, užkirsti kelią piktnaudžiavimui skaitmeninėmis technologijomis ir skatinti atsakingą valstybių elgesį kibernetinėje erdvėje, remiantis JT Generalinės Asamblėjos patvirtintomis JT vyriausybių ekspertų grupės bendro sutarimo ataskaitomis; teigiamai vertina neribotos sudėties darbo grupės galutinėje ataskaitoje pateiktas rekomendacijas, visų pirma dėl veiksmų programos sukūrimo; ragina JT skatinti valstybių, mokslo tyrimų pareigūnų, akademinės bendruomenės, pilietinės visuomenės organizacijų, humanitarinės pagalbos subjektų ir privačiojo sektoriaus dialogą, kad būtų užtikrinti įtraukūs politikos formavimo procesai dėl naujų tarptautinių nuostatų; ragina paspartinti visas esamas daugiašales pastangas, kad technologinė plėtra

ir nauji karybos metodai nebūtų vystomi sparčiau nei atnaujinamos norminės ir reglamentavimo sistemos; ragina modernizuoti ginklų kontrolės struktūrą siekiant išvengti skaitmeninės pilkosios zonos atsiradimo; ragina stiprinti JT taikos palaikymo misijas kibernetinės gynybos pajėgumais, atsižvelgiant į veiksmingą jų įgaliojimų įgyvendinimą;

43. dar kartą primena savo poziciją dėl visiškai autonominių ginklų kūrimo, gamybos ir naudojimo, kurie suteiktų galimybę vykdyti atakas be reikšmingo žmogaus įsikišimo; ragina Komisijos pirmininko pavaduotoją ir Sąjungos vyriausiąjį įgaliotinį, valstybes nares ir Europos Vadovų Tarybą priimti bendrą poziciją dėl autonominių ginklų sistemų, kuri užtikrintų prasmingą žmogaus vykdomą tokių ginklų sistemų ypatingos svarbos funkcijų kontrolę; prašo pradėti tarptautines derybas dėl teisiškai privalomos priemonės, kuria būtų uždrausti visiškai autonominiai ginklai;

44. pabrėžia bendradarbiavimo su nacionaliniais parlamentais keičiantis geriausia patirtimi kibernetinės gynybos srityje svarbą;

°

° °

45. paveda Pirmininkui perduoti šią rezoliuciją Europos Vadovų Tarybai, Tarybai, Komisijai, Komisijos pirmininko pavaduotojui ir Sąjungos vyriausiajam įgaliotiniui užsienio reikalams ir saugumo politikai, ES gynybos ir kibernetinio saugumo srities agentūroms, NATO generaliniam sekretoriui ir valstybių narių vyriausybėms bei parlamentams.