Europos Sąjungos
Taryba

Briuselis, 2021 m. kovo 9 d.
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

PRANEŠIMAS DĖL „I/A“ PUNKTO

nuo:	Tarybos generalinio sekretoriato
kam:	Nuolatinių atstovų komitetui / Tarybai
Dalykas:	Tarybos išvadų dėl Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategijos projektas

1. 2020 m. gruodžio 16 d. Komisija ir Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai paskelbė bendrą komunikatą Europos Parlamentui ir Tarybai „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“[1]. Šios naujos kibernetinio saugumo strategijos tikslas – remti Europos kolektyvinį atsparumą kibernetinėms grėsmėms ir užtikrinti, kad visi piliečiai ir įmonės galėtų visapusiškai naudotis sąžiningai teikiamų ir patikimų paslaugų ir skaitmeninių priemonių teikiama nauda.

[1] Dok. 14133/20.

2. Šį bendrą komunikatą Komisija ir EIVT pristatė 2020 m. gruodžio 17 d. ir 2021 m. sausio 12 d. vykusiose neformaliose Kibernetinių klausimų horizontaliosios darbo grupės vaizdo konferencijose. 2020 m. gruodžio 17 d. neformalioje Kibernetinių klausimų horizontaliosios darbo grupės vaizdo konferencijoje pirmininkausianti Portugalija pranešė ketinanti parengti Tarybos išvadų dėl Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategijos projektą.

3. Pirmąjį Tarybos išvadų projektą pirmininkaujanti valstybė narė pateikė neformalioje Kibernetinių klausimų horizontaliosios darbo grupės vaizdo konferencijoje 2021 m. vasario 2 d. Vėliau šios išvados buvo aptartos 2021 m. vasario 9 d., 2021 m. vasario 19 d. ir 2021 m. kovo 1 d. ir 9 d. vykusiose neformaliose Kibernetinių klausimų horizontaliosios darbo grupės vaizdo konferencijose.

4. Atsižvelgiant į tai, kad išvadų projekte taip pat yra nuoroda į ES gynybos politiką (30 punktas), su ja susijęs punktas buvo aptartas 2021 m. vasario 10 d. įvykusiame Politinės ir karinės grupės posėdyje.

5. Daug punktų yra susiję su bendra užsienio ir saugumo politika (1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 ir 33 punktai), todėl jie buvo pateikti Politiniam ir saugumo komitetui; Komitetas patvirtino šiuos punktus 2021 m. kovo 4 d. posėdyje.

6. 2021 m. kovo 9 d. neformalioje vaizdo konferencijoje Kibernetinių klausimų horizontalioji darbo grupė susitarė dėl Tarybos išvadų projekto, išdėstyto dok. 6722/21.

7. Atsižvelgiant į tai, kas išdėstyta pirmiau, Nuolatinių atstovų komiteto prašoma pateikti Tarybai priede išdėstytą Tarybos išvadų projektą ir rekomenduoti jai priimti šį projektą darbotvarkės A punktu.

PRIEDAS

Tarybos išvadų dėl Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategijos projektas

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“[2],

– interneto valdymo[3],

– 2017 m. lapkričio 20 d. bendro komunikato Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“[4],

– kibernetinio saugumo pajėgumų ir gebėjimų stiprinimo ES[5],

– 5G svarbos Europos ekonomikai ir poreikio mažinti su 5G susijusią saugumo riziką[6],

– aukšto skaitmeninimo lygio Europos ateities po 2020 m. „Skaitmeninio ir ekonominio konkurencingumo visoje Sąjungoje ir skaitmeninės sanglaudos stiprinimas“[7],

– papildomų pastangų siekiant didinti atsparumą ir kovoti su hibridinėmis grėsmėmis[8],

– Europos skaitmeninės ateities kūrimo[9],

---

2 Dok. 12109/13.
3 Dok. 16200/14.
4 Dok. 14435/17 + COR 1.
5 Dok. 7737/19.
6 Dok. 14517/19.
7 Dok. 9596/19.
8 Dok. 14972/19.
9 Dok. 8711/20.

– skaitmeninės diplomatijos[10],

– atsparumo didinimo ir kovos su hibridinėmis grėsmėmis, įskaitant dezinformaciją COVID-19 pandemijos kontekste[11],

– kibernetinio saugumo diplomatijos[12],

– ES koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes[13],

– bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos („Kibernetinio saugumo diplomatijos priemonių rinkinio“)[14],

– ES išorės kibernetinių pajėgumų stiprinimo gairių[15],

– perėjimą prie dinamiškesnės, atsparesnės ir konkurencingesnės Europos pramonės spartinančio ekonomikos gaivinimo[16],

– prijungtųjų įrenginių kibernetinio saugumo[17],

– Europos kibernetinio atsparumo sistemos stiprinimo ir kibernetinio saugumo pramonės konkurencingumo ir novatoriškumo skatinimo[18],

– taip pat Tarybos rezoliuciją dėl šifravimo „Saugumas naudojant šifravimą ir saugumas nepaisant šifravimo“[19],

---

10 Dok. 12804/20.
11 Dok. 14064/20.
12 Dok. 6122/15 + COR 1.
13 Dok. 10086/18.
14 Dok. 10474/17.
15 Dok. 10496/18.
16 Dok. 13004/20.
17 Dok. 13629/20.
18 Dok. 14540/16.
19 Dok. 13084/1/20 REV 1.

– ir 2020 m. spalio 15 d. bendrą valstybių narių deklaraciją „Naujos kartos debesijos, skirtos ES įmonėms ir viešajam sektoriui, kūrimas“,

PRIMINDAMA 2020 m. spalio 1–2 d. Europos Vadovų Tarybos išvadas dėl COVID-19, bendrosios rinkos, pramonės politikos, skaitmeninių klausimų ir išorės santykių[20] ir 2019 m. birželio 20 d. išvadas dėl dezinformacijos bei hibridinių grėsmių ir naujos 2019–2024 m. strateginės darbotvarkės[21],

PRIMINDAMA 2016 m. birželio 28 d. paskelbtą Visuotinę Europos Sąjungos užsienio ir saugumo politikos strategiją „Bendra vizija, bendri veiksmai: stipresnė Europa“,

PRIMINDAMA Europos Komisijos 2020 m. gruodžio 19 d. komunikatą dėl Europos skaitmeninės ateities formavimo[22] ir 2020 m. liepos 24 d. komunikatą dėl ES saugumo sąjungos strategijos[23],

PRIMINDAMA 2020 m. gruodžio 2 d. bendrą Europos Komisijos ir vyriausiojo įgaliotinio komunikatą dėl naujos ES ir JAV pasaulinių pokyčių darbotvarkės[24],

1. AKCENTUOJA tai, kad kibernetinis saugumas yra itin svarbus norint sukurti atsparią, žalią ir skaitmeninę Europą, ir PALANKIAI VERTINA bendrą komunikatą Europos Parlamentui ir Tarybai „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“, kuriame išdėstomas naujas ES veiksmų atsparumo, technologinio suverenumo ir lyderystės srityje pagrindas, kuriuo taip pat siekiama apsaugoti jos žmones, įmones ir institucijas nuo kibernetinių incidentų ir grėsmių, kartu didinant asmenų ir organizacijų pasitikėjimą ES gebėjimu remti saugias ir patikimas tinklų ir informacines sistemas, infrastruktūrą ir junglumą, taip pat propaguoti ir apsaugoti globalią, atvirą, laisvą, stabilią ir saugią kibernetinę erdvę, grindžiamą žmogaus teisėmis, pagrindinėmis laisvėmis, demokratija ir teisine valstybe.

---

20 Dok. EUCO 13/20.
21 Dok. EUCO 9/19.
22 Dok. COM(2020) 67 final, 2020 02 19.
23 Dok. COM(2020) 605 final, 2020 07 24.
24 Dok. JOIN(2020) 22 final, 2020 12 02.

2. PRIPAŽĮSTA, kad dėl COVID-19 pandemijos poreikis pasitikėti informacinių ir ryšių technologijų (IRT) priemonėmis bei sistemomis ir jų saugumu atsirado tarp svarbiausių mūsų kasdienio gyvenimo prioritetų. PABRĖŽIA, kad kibernetinis saugumas ir globalus bei atviras internetas yra gyvybiškai svarbūs tiek nacionalinio, tiek ES lygmens viešojo administravimo įstaigų ir institucijų veikimui, taip pat mūsų visuomenei ir visai ekonomikai apskritai.

3. AKCENTUOJA, kad reikia dar labiau didinti informuotumą kibernetiniais klausimais politiniame ir strateginiame sprendimų priėmimo lygmenyse, sprendimų priėmėjams suteikiant atitinkamų žinių ir informacijos, ir PABRĖŽIA, kad reikia didinti plačiosios visuomenės informuotumą ir propaguoti kibernetinę higieną.

4. RAGINA propaguoti ir saugoti pagrindines ES vertybes: demokratiją, teisinę valstybę, žmogaus teises ir pagrindines laisves, įskaitant teisę į saviraiškos laisvę ir informacijos laisvę, teisę į susirinkimų ir asociacijų laisvę ir teisę į privatumą kibernetinėje erdvėje. Šiuo atžvilgiu PALANKIAI VERTINA tolesnes nenutrūkstamas pastangas apsaugoti žmogaus teisių gynėjus, pilietinę visuomenę ir akademinę bendruomenę, dirbančius tokiais klausimais kaip kibernetinis saugumas, duomenų privatumas, sekimas ir cenzūra internete, teikiant tolesnes praktines gaires, propaguojant geriausią praktiką ir intensyvinant ES pastangas užkirsti kelią žmogaus teisių pažeidimams ir piktnaudžiavimui besiformuojančiomis technologijomis, visų pirma prireikus naudojant diplomatines priemones ir vykdant tokių technologijų eksporto kontrolę. Šiame kontekste PABRĖŽIA ES 2020–2024 m. veiksmų plano žmogaus teisių ir demokratijos srityje ir ES žmogaus teisių gairių dėl saviraiškos laisvės internete ir realiame gyvenime svarbą.
5. AKCENTUOJA, kad strateginio savarankiškumo užtikrinimas, kartu išsaugant atvirą ekonomiką, yra vienas iš pagrindinių Sąjungos tikslų siekiant patiems nusistatyti ekonomikos kelią ir interesus. Tuo tikslu, be kita ko, reikia stiprinti gebėjimą savarankiškai priimti sprendimus kibernetinio saugumo srityje, siekiant stiprinti ES skaitmeninę lyderystę ir jos strateginius pajėgumus. PRIMENA, kad tai apima strateginės priklausomybės nustatymą ir mažinimą ir jautriausių pramonės ekosistemų ir konkrečių sričių atsparumo didinimą. PABRĖŽIA, kad šie veiksmai, be kita ko, gali apimti gamybos ir tiekimo grandinių įvairinimą, investicijų ir gamybos skatinimą ir pritraukimą Europoje, alternatyvių sprendimų bei žiedinių modelių tyrinėjimą ir plataus masto valstybių narių bendradarbiavimo pramonės srityje skatinimą.

6. Atsižvelgdama į tai, kad darbuotojams trūksta skaitmeninių ir kibernetinio saugumo įgūdžių, PABRĖŽIA, jog svarbu patenkinti kvalifikuotų darbuotojų paklausą skaitmeninio ir kibernetinio saugumo srityje, visų pirma ugdant, išlaikant ir pritraukiant geriausius specialistus, pavyzdžiui, pasitelkiant švietimą ir mokymą, kad mūsų visuomenę skaitmenizuoti būtų galima kibernetiškai saugiu būdu. RAGINA moteris ir mergaites aktyviau rinktis studijuoti gamtos mokslų, technologijų, inžinerijos ir matematikos (STEM) dalykus ir kelti savo kvalifikaciją bei persikvalifikuoti, kad įgytų skaitmeninių įgūdžių ir galėtų dirbti su IRT susijusį darbą, nes tai yra viena iš priemonių skaitmeninei lyčių atskirčiai mažinti.

7. 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 savo įsipareigojimą tarptautinius ginčus kibernetinės erdvės klausimais spręsti taikiomis priemonėmis ir tai, kad prioriteto tvarka visomis ES diplomatinėmis pastangomis turėtų būti siekiama propaguoti saugumą ir stabilumą kibernetinėje erdvėje pasitelkiant tarptautinį bendradarbiavimą ir mažinti klaidingo suvokimo, eskalacijos ir konfliktų, galinčių kilti dėl IRT incidentų, pavojų, ir PRITARIA tam, kad būtų toliau kuriamos ir įgyvendinamos regioninio ir tarptautinio lygmens pasitikėjimo stiprinimo priemonės. PAKARTOJA bendru sutarimu parengtą Jungtinių Tautų Generalinės Asamblėjos raginimą JT valstybėms narėms vadovautis JT Vyriausybių ekspertų grupių ataskaitų rekomendacijomis, susijusiomis su naudojimusi IRT, ir DAR KARTĄ PATVIRTINA, kad kibernetinėje erdvėje taikoma tarptautinė teisė, o pirmiausia – visa apimtimi – JT Chartija.

8. DAR KARTĄ PATVIRTINA, jog norint, kad besiformuojančių technologijų ir techninės bei loginės infrastruktūros, būtinos bendram viešųjų šerdinių interneto elementų prieinamumui ir neliečiamumui užtikrinti, srityse tarptautinės normos ir standartai būtų praktiškai formuluojami taip, kad atitiktų visuotines bei ES vertybes, ir taikant įvairių suinteresuotųjų šalių bendradarbiavimu grindžiamą požiūrį, būtina toliau plėtoti normas ir standartus pačioje Sąjungoje. Taip bus užtikrinta, kad internetas išliktų globalus, atviras, laisvas, stabilus ir saugus ir kad naudojant ir plėtojant skaitmenines technologijas būtų gerbiamos žmogaus teisės, o tų technologijų naudojimas būtų teisėtas, saugus ir etiškas. ATKREIPIA DĖMESĮ į būsimą standartizacijos strategiją ir ĮSIPAREIGOJA proaktyviai ir koordinuotai vykdyti informavimo veiklą, kuria tarptautiniu lygmeniu būtų propaguojama ES lyderystė ir ES tikslai, be kita ko, ją vykdant įvairiose tarptautinėse standartizacijos įstaigose ir bendradarbiaujant su panašiai mąstančiais partneriais, pilietine visuomene, akademine bendruomene ir privačiuoju sektoriumi.

9. TVIRTAI REMIA įvairių suinteresuotųjų šalių bendradarbiavimu grindžiamo modelio taikymą interneto valdymo ir kibernetinio saugumo srityje ir įsipareigoja stiprinti reguliarų ir struktūrintą keitimąsi informacija su suinteresuotaisiais subjektais, įskaitant privatųjį sektorių, akademinę bendruomenę ir pilietinę visuomenę, tarptautiniuose forumuose, be kita ko, pagal Paryžiaus kvietimą užtikrinti pasitikėjimą ir saugumą kibernetinėje erdvėje. RAGINA užtikrinti visuotinę, įperkamą ir lygiateisę prieigą prie interneto, taip mažinant skaitmeninę atskirtį, ir visų pirma užtikrinti moterų ir mergaičių bei pažeidžiamoje ar marginalizuotoje padėtyje esančių asmenų įgalėjimą tiek formuojant politiką, tiek naudojantis internetu.

10. PABRĖŽIA, kad artimiausiais metais į skaitmeninės srities investicijas ir iniciatyvas reikia įtraukti kibernetinį saugumą ir kad reikia palaipsniui prisidėti prie vienodų sąlygų užtikrinimo kibernetinio saugumo srityje, ir ATKREIPIA DĖMESĮ į Komisijos planus didinti viešąsias išlaidas kibernetinio saugumo srityje ir į ją pritraukti privačiojo sektoriaus investicijų. AKCENTUOJA mažųjų ir vidutinių įmonių (MVĮ) svarbą kibernetinio saugumo ekosistemoje ir PRIPAŽĮSTA, kad turima tinkamų finansinių priemonių itin kryptingam orientavimuisi į kibernetinį saugumą remti vykdant skaitmeninę transformaciją 2021–2027 m. daugiametės finansinės programos (DFP) laikotarpiu ir Ekonomikos gaivinimo ir atsparumo didinimo priemonės kontekste.

11. TIKISI, kad bus greitai įgyvendintas Reglamentas dėl Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro ir Nacionalinių koordinavimo centrų tinklo (CCCN), be kita ko, kad Europos kibernetinio saugumo kompetencijos centras Bukarešte bus greitai įkurtas ir pradės veikti. Greitas šio centro darbotvarkės priėmimas padės kuo labiau padidinti investicijų poveikį, siekiant stiprinti Sąjungos lyderystę ir strateginį savarankiškumą kibernetinio saugumo srityje ir remti technologinius pajėgumus bei įgūdžius, taip pat siekiant didinti Sąjungos konkurencingumą pasaulyje, prisidedant kibernetinio saugumo srities pramonei ir akademinėms bendruomenėms, įskaitant MVĮ ir mokslinių tyrimų centrus, kuriems bus naudingas sistemingesnis, įtraukesnis ir strategiškesnis bendradarbiavimas, dėmesį skiriant Sąjungos ir visų jos valstybių narių sanglaudai.

12. PALANKIAI VERTINA ENISA kartu su valstybėmis narėmis ir suinteresuotaisiais subjektais vykdomą darbą Europos Sąjungoje rengiant IRT produktų, paslaugų ir procesų sertifikavimo schemas, kurios turėtų padėti didinti bendrą kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Todėl LAUKIA tęstinės Sąjungos darbo programos, kad būtų parengtos ES kibernetinio saugumo sertifikavimo schemos pagal Kibernetinio saugumo aktą. Šiame kontekste PRIPAŽĮSTA itin svarbų ES vaidmenį siekiant parengti standartus, kurie galėtų formuoti kibernetinio saugumo aplinką ir kurie padėtų užtikrinti sąžiningą konkurenciją ES ir pasaulinėje arenoje, taip skatinant patekimą į rinką ir šalinant saugumo riziką, kartu užtikrinant ES teisės aktų sistemos taikomumą.

13. PAKARTOJA, kad svarbu įvertinti poreikį ilguoju laikotarpiu priimti horizontaliuosius teisės aktus, kuriais, be kita ko, būtų apibrėžtos būtinos pateikimo rinkai taisyklės, kad būtų atsižvelgta į visus atitinkamus prijungtųjų įrenginių kibernetinio saugumo aspektus, pavyzdžiui, prieinamumą, vientisumą ir konfidencialumą. Šiuo atžvilgiu PALANKIAI VERTINA diskusiją, skirtą išnagrinėti tokių teisės aktų taikymo sritį ir jų sąsajas su kibernetinio saugumo sertifikavimo sistema, kaip apibrėžta Kibernetinio saugumo akte, siekiant padidinti saugumo lygį bendrojoje skaitmeninėje rinkoje. PABRĖŽIA, kad kibernetinio saugumo reikalavimai turėtų būti apibrėžti laikantis atitinkamų Sąjungos teisės aktų, įskaitant Kibernetinio saugumo aktą, naująją teisės aktų sistemą, Reglamentą dėl Europos standartizacijos ir galimus būsimus horizontaliuosius teisės aktus, kad būtų išvengta teisės aktų dviprasmiškumo ir fragmentiškumo.

14. PRIPAŽĮSTA, kad svarbu taikyti visapusišką ir horizontalų požiūrį į kibernetinį saugumą Sąjungoje, kartu visapusiškai atsižvelgiant į valstybių narių kompetenciją ir poreikius, ir kad norint stiprinti valstybių narių pajėgumus svarbu nuolat remti techninę pagalbą ir bendradarbiavimą. Atsižvelgdama į pakitusį kibernetinių grėsmių spektrą, ATKREIPIA DĖMESĮ į naują pasiūlymą dėl direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, grindžiamą TIS direktyva, ir pakartoja remianti nacionalinių kibernetinio saugumo sistemų stiprinimą ir derinimą bei nenutrūkstamą valstybių narių bendradarbiavimą. Be to, PABRĖŽIA, kad šioje srityje reikia suderinti sektorinius teisės aktus ir užtikrinti jų nuoseklumą.

15. ATKREIPIA DĖMESĮ į Komisijos pasiūlymą padėti valstybėms narėms steigti ir stiprinti saugumo operacijų centrus (SOC) siekiant visoje ES sukurti SOC tinklą, kad būtų atidžiau stebimi išpuolių prieš tinklus signalai ir tam būtų iš anksto pasirengta. Šiame kontekste LAUKIA išsamių Komisijos planų dėl SOC tinklo, kartu gerbiant valstybių narių kompetenciją. PRIMENA ES remiamas valstybių narių pastangas įsteigti sektorines, nacionalines ir regionines reagavimo į kompiuterių saugumo incidentus tarnybas (CSIRT) ir nacionalinius arba europinius keitimosi informacija ir jos analizės centrus (ISAC), kurie yra veiksmingo kibernetinio saugumo partneryščių tinklo Sąjungoje dalis. TIKISI, kad bus išnagrinėtas šio tinklo potencialas stiprinti SOC, taip pat šių centrų papildomumą ir koordinavimą su esamais tinklais ir subjektais (visų pirma CSIRT tinklu), kad būtų skatinama veiksminga, saugi ir patikima dalijimosi informacija kultūra. PABRĖŽIA, kad šis procesas bus grindžiamas darbu, atliekamu įgyvendinant dirbtinio intelekto ir našiosios kompiuterijos iniciatyvas, ir Europos skaitmeninių inovacijų centrų atliekamu darbu.

16. PAŽYMI, kad gali būti plėtojama saugi junglumo sistema, grindžiama Europos kvantinės komunikacijos infrastruktūra (EuroQCI) ir Europos Sąjungos vyriausybiniu palydoviniu ryšiu (GOVSATCOM), ir PRIPAŽĮSTA, kad bet koks galimas plėtojimas ateityje turėtų būti grindžiamas tvirta kibernetinio saugumo sistema, atsižvelgiant į visą elektroninių ryšių infrastruktūrą, pavyzdžiui, kosmoso, sausumos ir povandeninių tinklų sistemas.

17. LAUKIA diskusijų su Komisija, ENISA, dviem ES šakninių DNS (domenų vardų sistemos) serverių operatoriais ir įvairiais suinteresuotaisiais subjektais, kad būtų įvertintas dviejų ES šakninių DNS serverių operatorių vaidmuo užtikrinant, kad internetas išliktų prieinamas ir nesuskaidytas visame pasaulyje. PALANKIAI VERTINA tolesnes diskusijas dėl Komisijos ketinimo sukurti alternatyvią Europos prieigos prie pasaulinio interneto paslaugą (iniciatyva „DNS4EU“), grindžiamą skaidriu modeliu, atitinkančiu naujausius pritaikytojo ir integruotojo saugumo, pritaikytosios ir standartizuotosios duomenų apsaugos ir integruotosios ir standartizuotosios privatumo apsaugos standartus ir taisykles siekiant prisidėti prie didesnio atsparumo, kartu išlaikant ir stiprinant visų valstybių narių tarptautinį junglumą.

18. PRIPAŽĮSTA, kad Komisija ir valstybės narės turi bendrai dėti pastangas, kad paspartintų pagrindinių interneto standartų, įskaitant šeštąją interneto protokolo versiją (IPv6), ir plačiai pripažintų interneto saugumo standartų taikymą, nes jie yra itin svarbūs keliant bendrą pasaulinio interneto saugumo, atsparumo, atvirumo ir sąveikumo lygį, kartu didinant ES pramonės, o visų pirma – interneto infrastruktūros operatorių, konkurencingumą.

19. PABRĖŽIA koordinuoto požiūrio svarbą, taip pat veiksmingų priemonių kūrimą ir įgyvendinimą nacionaliniu lygmeniu norint sustiprinti 5G tinklų kibernetinį saugumą. PRITARIA tolesniems veiksmams, kurių reikia imtis užtikrinant 5G tinklų kibernetinį saugumą, kaip nurodyta ES kibernetinio saugumo strategijos priedėlyje ir remiantis Komisijos rekomendacijos dėl 5G tinklų saugumo poveikio ataskaitos rezultatais, pavyzdžiui, kiek tai susiję su ilgalaikio ir visapusiško požiūrio nustatymu apimant visą 5G vertės grandinę ir ekosistemą. Siekiant toliau stiprinti koordinuotą požiūrį į 5G tinklų saugumą, RAGINA valstybes nares, ES institucijas ir kitus atitinkamus suinteresuotuosius subjektus toliau periodiškai vertinti padėtį, taip pat keistis informacija ir geriausios praktikos pavyzdžiais TIS bendradarbiavimo grupėje atliekant darbą pagal specialią 5G kibernetinio saugumo kryptį ir reguliariai informuoti Tarybą apie padarytą pažangą. PABRĖŽIA, kartu akcentuodama valstybių narių atsakomybę už nacionalinį saugumą, kad yra tvirtai įsipareigojusi taikyti ir greitai baigti įgyvendinti ES 5G rinkinio priemones ir toliau dėti pastangas, kad būtų užtikrintas 5G tinklų saugumas ir plėtojami naujos kartos tinklai. Glaudus valstybių narių, Komisijos ir ENISA bendradarbiavimas 5G tinklų saugumo srityje galėtų būti pavyzdys sprendžiant kitus kibernetinio saugumo srities klausimus, kartu gerbiant valstybių narių kompetenciją ir subsidiarumo bei proporcingumo principus.

20. PRIPAŽĮSTA, kad svarbu geriau integruoti kibernetinį saugumą į ES reagavimo į krizes mechanizmus ir išbandyti tai atitinkamose pratybose, ir PABRĖŽIA, kad svarbu stiprinti įvairių kibernetinės srities bendruomenių bendradarbiavimą ir dalijimąsi informacija ES ir susieti esamas iniciatyvas, struktūras ir procedūras (pvz., ES integruotą politinio atsako į krizes mechanizmą (IPCR), CSIRT tinklą, TIS bendradarbiavimo grupę, Ryšių palaikymo dėl kibernetinių krizių organizacinį tinklą (CyCLONe), Europos kovos su elektroniniu nusikalstamumu centrą, ES žvalgybos ir situacijų centrą (ES INTCEN) ir kitas atitinkamas ES įstaigas) didelio masto ir tarpvalstybinių kibernetinių incidentų ir grėsmių atveju. ATSIŽVELGDAMA į šioje srityje jau padarytą pažangą, LAUKIA Komisijos pasiūlymo dėl bendro kibernetinio saugumo padalinio (BKSP) nustatymo proceso, orientyrų ir terminų, kad būtų teikiama pridėtinė vertė, skiriamas aiškus dėmesys ir supaprastinta ES kibernetinio saugumo krizių valdymo sistema, be kita ko, pasitelkiant pasirengimą, bendrą informuotumą apie padėtį, koordinuoto atsako ir pratybų stiprinimą – skaidriai ir laipsniškai, kartu vengiant dubliavimosi ir dalinio sutapimo ir gerbiant valstybių narių kompetenciją.

21. PABRĖŽIA, kad svarbu skatinti atitinkamų kibernetinio saugumo subjektų ir kompetentingų institucijų, pvz., teisėsaugos ir teisminių institucijų, bendradarbiavimą ir keitimąsi informacija saugumo ir baudžiamosios teisenos srityje ir kad reikia plėsti ir gerinti šių institucijų gebėjimus tirti kibernetinius nusikaltimus ir vykdyti baudžiamąjį persekiojimą už juos, taip pat kad reikia skatinti tarptautines derybas ir propaguoti ES taisykles dėl tarpvalstybinės prieigos prie elektroninių įrodymų. Nepriklausomai nuo atitinkamo meto technologinės aplinkos, itin svarbu išsaugoti kompetentingų saugumo ir baudžiamosios teisenos srities institucijų įgaliojimus, suteikiant joms teisėtą prieigą, kad jos galėtų vykdyti savo užduotis, kaip nustatyta ir leidžiama įstatymu. Tokiais įstatymais, kuriuose numatyti vykdymo užtikrinimo įgaliojimai, visada turi būti visapusiškai paisoma tinkamo proceso ir kitų apsaugos priemonių, taip pat pagrindinių teisių, visų pirma teisės į tai, kad būtų gerbiamas privatus gyvenimas bei komunikacijos slaptumas, ir teisės į asmens duomenų apsaugą.

22. Dar KARTĄ PATVIRTINA remianti patikimo šifravimo, kuris yra būtina asmenų, vyriausybių, pramonės ir visuomenės pagrindinių teisių apsaugos ir skaitmeninio saugumo užtikrinimo priemonė, kūrimą, diegimą ir naudojimą, ir kartu PRIPAŽĮSTA, jog reikia užtikrinti, kad kompetentingos saugumo ir baudžiamosios teisenos srities institucijos, pvz., teisėsaugos ir teisminės institucijos, galėtų naudotis savo teisėtais įgaliojimais tiek internete, tiek realiame gyvenime, kad būtų apsaugotos mūsų visuomenės ir piliečiai. Kompetentingos institucijos turi turėti galimybę teisėtai ir tikslingai susipažinti su duomenimis, visapusiškai gerbiant pagrindines teises ir laikantis atitinkamų duomenų apsaugos įstatymų, kartu užtikrinant kibernetinį saugumą. PABRĖŽIA, kad imantis bet kokių veiksmų šie interesai turi būti kruopščiai derinami su būtinumo, proporcingumo ir subsidiarumo principais.

23. REMIA ir PROPAGUOJA Budapešto konvenciją dėl elektroninių nusikaltimų ir šiuo metu atliekamą darbą rengiant šios konvencijos antrąjį papildomą protokolą. Be to, toliau daugiašaliu lygmeniu keičiasi informacija apie kibernetinius nusikaltimus, be kita ko, procesuose, susijusiuose su Europos Taryba, Jungtinių Tautų narkotikų kontrolės ir nusikalstamumo prevencijos biuru (UNODC) ir Nusikalstamumo prevencijos ir baudžiamosios justicijos komisija, siekiant užtikrinti tvirtesnį tarptautinį bendradarbiavimą kovos su kibernetiniais nusikaltimais srityje, įskaitant keitimąsi geriausios praktikos pavyzdžiais ir techninėmis žiniomis, ir remti gebėjimų stiprinimą, kartu gerbiant, propaguojant ir saugant žmogaus teises ir pagrindines laisves.

24. Nors kiekviena valstybė narė išimtinai lieka atsakinga už savo nacionalinį saugumą, PRIPAŽĮSTA strateginės žvalgybos bendradarbiavimo kibernetinių grėsmių ir veiklos srityje svarbą ir PRAŠO valstybių narių per savo kompetentingas institucijas toliau prisidėti prie ES žvalgybos ir situacijų centro (EU INTCEN), kuris yra ES informuotumo apie padėtį ir grėsmių vertinimo kibernetinėje srityje centras, atliekamo darbo ir išnagrinėti pasiūlymą dėl galimo valstybių narių kibernetinės žvalgybos darbo grupės įsteigimo, kad būtų sustiprinti INTCEN tiksliniai pajėgumai šioje srityje, grupės veiklą grindžiant savanoriškais valstybių narių įnašais žvalgybos srityje, nedarant poveikio valstybių narių kompetencijai.

25. PABRĖŽIA tvirtos ir nuoseklios saugumo sistemos svarbą norint apsaugoti visą ES personalą, duomenis, ryšių tinklus bei informacines sistemas ir sprendimų priėmimo procesus, grindžiamus išsamiomis, nuosekliomis ir vienalytėmis taisyklėmis. Visų pirma tai turėtų būti daroma didinant ES atsparumą kibernetinėms grėsmėms ir gerinant jos saugumo kultūrą, susijusią su šiomis grėsmėmis, taip pat stiprinant įslaptintų ir neįslaptintų ES tinklų saugumą, kartu užtikrinant tinkamą valdymą ir suteikiant pakankamai išteklių ir pajėgumų, be kita ko, Europos institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) įgaliojimų stiprinimo kontekste. Šiomis aplinkybėmis PALANKIAI VERTINA vykstančias diskusijas dėl bendrų informacijos saugumo taisyklių nustatymo, deramai atsižvelgiant į Tarybos saugumo taisykles dėl ES įslaptintos informacijos apsaugos, taip pat dėl bendrų privalomų kibernetinio saugumo taisyklių nustatymo visoms ES institucijoms, įstaigoms ir agentūroms.

26. REMDAMASI ES kibernetinio saugumo srities diplomatijos pastangomis, ĮSIPAREIGOJA didinti Kibernetinio saugumo diplomatijos priemonių rinkinio veiksmingumą ir efektyvumą ir TIKISI pagilinti diskusijas dėl jo taikymo srities ir naudojimo, remiantis taikant šią priemonę iki šiol įgyta patirtimi. Šiomis diskusijomis turėtų būti prisidedama prie saugumo stiprinimo tarptautiniu lygmeniu, skatinant dialogą ir puoselėjant bendrą viziją kibernetinio saugumo klausimais, stiprinant prevenciją, stabilumą, bendradarbiavimą ir pasitikėjimą bei pajėgumus, o prireikus – taikant ribojamąsias priemones, kad būtų užkirstas kelias kibernetinei kenkimo veiklai, nukreiptai prieš ES ir jos valstybių narių vientisumą ir saugumą, nuo šios veiklos atgrasyti ir į ją reaguoti, taip prisidedant prie tarptautinio saugumo ir stabilumo ir stiprinant ES poziciją kibernetiniais klausimais, visapusiškai gerbiant nacionalinę kompetenciją ir prerogatyvas. Visų pirma ypatingas dėmesys turėtų būti skiriamas tam, kad būtų užkirstas kelias sisteminio poveikio kibernetiniams išpuoliams, kurie gali padaryti poveikį mūsų tiekimo grandinėms, ypatingos svarbos infrastruktūrai ir pagrindinėms paslaugoms, demokratinėms institucijoms ir procesams ir pakenkti mūsų ekonominiam saugumui, įskaitant intelektinės nuosavybės vagystes pasinaudojant kibernetine erdve, ir kovojama su šiais išpuoliais. Valstybės narės ir ES institucijos taip pat turėtų toliau svarstyti ES kibernetinio saugumo krizių valdymo sistemos, Kibernetinio saugumo diplomatijos priemonių rinkinio ir ES sutarties 42 straipsnio 7 dalies bei SESV 222 straipsnio nuostatų tarpusavio derinimą, visų pirma vykdydamos scenarijais grindžiamą darbą, kad būtų pasiektas bendras supratimas apie praktinę ES sutarties 42 straipsnio 7 dalies įgyvendinimo tvarką.

27. PRIPAŽĮSTA, kad svarbu stiprinti bendradarbiavimą su tarptautinėmis organizacijomis ir šalimis partnerėmis siekiant gerinti bendrą supratimą apie kibernetinių grėsmių aplinką, plėtoti dialogus ir bendradarbiavimo mechanizmus, nustatyti, kai tinkama, bendradarbiavimu grindžiamą diplomatinį atsaką, taip pat gerinti dalijimąsi informacija, be kita ko, pasitelkiant švietimą, mokymą ir pratybas. Visų pirma PABRĖŽIA, kad tvirta transatlantinė partnerystė kibernetinio saugumo srityje prisideda prie mūsų bendro saugumo, stabilumo ir gerovės, ir ATKREIPIA DĖMESĮ į ES ir JK prekybos ir bendradarbiavimo susitarimo nuostatas dėl bendradarbiavimo kibernetinio saugumo srityje. PRIMINDAMA pagrindinius ES ir NATO bendradarbiavimo kibernetinio saugumo srityje pasiekimus įgyvendinant 2016 m. Varšuvos ir 2018 m. Briuselio bendras deklaracijas, pakartoja, kad yra svarbus tvirtesnis abipusiškai stiprinantis ir naudingas bendradarbiavimas pasitelkiant švietimą, mokymą, pratybas ir koordinuotą atsaką į kibernetinę kenkimo veiklą, visapusiškai gerbiant abiejų pusių sprendimų priėmimo autonomiškumą ir procedūras, remiantis skaidrumo, abipusiškumo ir įtraukumo principais.

28. Siekdama prisidėti prie globalios, atviros, laisvos, stabilios ir saugios kibernetinės erdvės, kuri tampa vis svarbesnė nuolatiniam mūsų visuomenių klestėjimui, augimui, saugumui, gerbūviui, junglumui ir vientisumui, ĮSIPAREIGOJA nuolat dalyvauti normų nustatymo procesuose tarptautinėse organizacijose, ypač su JT Pirmuoju komitetu susijusiuose procesuose, skatindama tarptautinės teisės taikymo kibernetinėje erdvėje pripažinimą ir atsakingo valstybių elgesio kibernetinėje erdvėje normų, taisyklių ir principų laikymąsi ir prisidėdama prie šių procesų, be kita ko, skatindama greitą veiksmų programos dėl atsakingo valstybių elgesio kibernetinėje erdvėje gerinimo nustatymą, nes ši programa yra konstruktyvi, įtrauki ir bendru sutarimu grindžiama tolesnė veikla, susijusi tiek su JT Vyriausybių ekspertų grupės, tiek su neribotos sudėties darbo grupės įgyvendinamais procesais.

29. PRIMENA esanti tvirtai įsipareigojusi užtikrinti veiksmingą daugiašališkumą ir taisyklėmis grindžiamą pasaulinę tvarką, kurioje Jungtinėms Tautoms tenka pagrindinis vaidmuo, ir pasiryžusi stiprinti bendradarbiavimą ir koordinavimą su tarptautinėmis ir regioninėmis organizacijomis, t. y. JT sistema, NATO, Europos Taryba, ESBO, EBPO, Afrikos Sąjunga (AS), Amerikos valstybių organizacija (OAS), Pietryčių Azijos valstybių asociacija (ASEAN), ASEAN regioniniu forumu, Persijos įlankos bendradarbiavimo taryba (GCC) ir Arabų Valstybių Lyga (LAS), diskutuojant su kibernetine erdve susijusiais klausimais, taip pat tęsiant ir plečiant struktūrinius ES dialogus ir konsultacijas kibernetinės erdvės klausimais su trečiosiomis šalimis. PABRĖŽIA, kad aktyviai remia JT, visų pirma jos Darbotvarkę iki 2030 m., įskaitant darnaus vystymosi tikslus, ir PALANKIAI VERTINA JT Generalinio Sekretoriaus veiksmų gaires skaitmeninio bendradarbiavimo srityje ir JT Generalinio Sekretoriaus nusiginklavimo darbotvarkę, kuriomis skatinama atskaitomybė ir normų laikymasis kibernetinėje erdvėje ir prisidedama prie konfliktų, kylančių dėl kibernetinės kenkimo veiklos, prevencijos ir taikaus sprendimo. PALANKIAI VERTINA vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai pasiūlymą sukurti neformalų ES kibernetinės diplomatijos tinklą siekiant plėsti ES ir valstybių narių įsitraukimą ir praktinę patirtį sprendžiant tarptautinius kibernetinius klausimus, kad būtų stiprinama koordinuota informavimo veikla.

30. LAUKIA būsimo pasiūlymo dėl Kibernetinės gynybos politikos metmenų peržiūros ir ĮSIPAREIGOJA toliau dėti pastangas, kad sustiprintų kibernetinio saugumo ir kibernetinės gynybos aspektus, siekiant užtikrinti, kad jie būtų visapusiškai integruoti į platesnę saugumo ir gynybos erdvę, visų pirma darbo, susijusio su strateginiu kelrodžiu, kontekste. MANO, kad būsima karinė vizija ir strategija dėl kibernetinės erdvės kaip operacijų srities padės tęsti šias diskusijas. PALANKIAI VERTINA Europos gynybos agentūros (EGA) iniciatyvą skatinti karinių CERT bendradarbiavimą ir REMIA pastangas, dedamas civilinei ir karinei sinergijoms didinti ir kibernetinės gynybos bei kibernetinio saugumo koordinavimui gerinti, įskaitant su kosmosu susijusius aspektus, be kita ko, vykdant specialius PESCO projektus.

31. PALANKIAI VERTINA pasiūlymą parengti ES išorės kibernetinių pajėgumų stiprinimo darbotvarkę, pasiūlymą įsteigti ES kibernetinių pajėgumų stiprinimo tarybą ir ES kibernetinio tinklo (ES kibernetinių pajėgumų stiprinimo tinklo) sukūrimą ir įgyvendinimą, siekiant didinti kibernetinį atsparumą ir pajėgumus visame pasaulyje. Šiomis aplinkybėmis PALANKIAI VERTINA bendradarbiavimą su valstybėmis narėmis, taip pat su viešojo ir privačiojo sektorių partneriais, visų pirma Pasauliniu kibernetinių ekspertinių žinių forumu (GFCE) ir kitomis atitinkamomis tarptautinėmis institucijomis, kad būtų užtikrintas koordinavimas ir išvengta dubliavimosi. Ypač SKATINA bendradarbiavimą su partneriais Vakarų Balkanuose ir ES rytinėse ir pietinėse kaimyninėse šalyse.

32. Siekdama užtikrinti, kad visos šalys galėtų gauti socialinės, ekonominės ir politinės interneto ir naudojimosi technologijomis naudos, ĮSIPAREIGOJA padėti šalims partnerėms spręsti didėjančią kibernetinės kenkimo veiklos problemą, visų pirma veiklos, kuria kenkiama jų ekonomikos vystymuisi, visuomenei ir demokratinių sistemų vientisumui bei saugumui, be kita ko, atsižvelgdama į Europos demokratijos veiksmų plane numatytas pastangas.

33. Siekdama užtikrinti ES kibernetinio saugumo strategijoje pateiktų pasiūlymų rengimą, įgyvendinimą bei stebėseną ir atsižvelgdama į kai kurių iniciatyvų daugiametį pobūdį, RAGINA Komisiją ir vyriausiąjį įgaliotinį užsienio reikalams ir saugumo politikai parengti išsamų įgyvendinimo planą, kuriame būtų nustatyti planuojamų veiksmų prioritetai ir tvarkaraštis. STEBĖS pažangą įgyvendinant šias išvadas pagal veiksmų planą, kurį Taryba reguliariai peržiūrės ir atnaujins glaudžiai bendradarbiaudama su Europos Komisija ir vyriausiuoju įgaliotiniu.