Eiropas Savienības
Padome

Briselē, 2023. gada 22. maijā
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Saņēmējs:	delegācijas
Iepr. dok. Nr.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Temats:	Padomes secinājumi par ES kiberaizsardzības politiku

Pielikumā ir pievienoti Padomes secinājumi par ES kiberaizsardzības politiku, kurus Padome apstiprināja 2023. gada 22. maija sanāksmē.

Padomes secinājumi par ES kiberaizsardzības politiku

1. Pēc 2014. gada kiberaizsardzības politikas satvara un tā atjauninājuma 2018. gadā Padome kā turpinājumu atzinīgi vērtē vērienīgo kopīgo paziņojumu par ES kiberaizsardzības politiku, lai vēl vairāk ieguldītu mūsu mūsdienīgajos un sadarbspējīgajos bruņotajos spēkos, progresīvākajās tehnoloģijās, mūsdienīgās kiberaizsardzības spējās un stiprinātu partnerības kopīgu izaicinājumu pārvarēšanai. Kibertelpa ir kļuvusi par stratēģiskas konkurences lauku laikā, kad pieaug atkarība no digitālajām tehnoloģijām. Tāpēc ir būtiski saglabāt atvērtu, brīvu, stabilu un drošu kibertelpu. Tādu kiberoperāciju izmantošana, kas ir ļāvušas Krievijai īstenot tās neprovocēto un nepamatoto agresijas karu pret Ukrainu un kas ir norisinājušās līdztekus tam, ietekmē globālo stabilitāti un drošību, ir nozīmīgs eskalācijas risks un vēl vairāk papildina jau tā nopietno pēdējos gados vērojamo ļaunprātīgu kiberdarbību skaita pieaugumu ārpus bruņota konflikta.

2. Karš Ukrainā ir radījis jaunu stratēģisko kontekstu un apstiprinājis, ka ES, tās dalībvalstīm un to partneriem ir vēl vairāk jāstiprina ES noturība saskarei ar kiberapdraudējumiem un jāpalielina mūsu kopīgā kiberdrošība un kiberaizsardzība pret ļaunprātīgu rīcību un agresijas aktiem kibertelpā. Kopīgais paziņojums par ES kiberaizsardzības politiku pauž mūsu apņemšanos nodrošināt tūlītējus un ilgtermiņa pasākumus, lai nodrošinātu rīcības brīvību kibertelpā un reakciju uz draudu radītājiem aktoriem, kuri cita starpā tiecas iejaukties, traucēt vai sagraut ES un tās partneru tīklu un informācijas sistēmas. Šis kopīgais paziņojums papildina ES kiberdrošības stratēģiju un atbilstīgi Stratēģiskajam kompasam ir svarīgs solis virzībā uz ES pilna spektra pieeju noturībai, reaģēšanai, konfliktu novēršanai, sadarbībai un stabilitātei kibertelpā. Šajā sakarā Padome akcentē, ka ir vajadzīgas pienācīgas un saskaņotas atbildes reakcijas no ES, tās dalībvalstu un to partneru puses, un arī gaida, kad tiks pārskatītas ES kiberdiplomātijas rīkkopas īstenošanas pamatnostādnes, kas ir vēl viens svarīgs solis uz priekšu ES pozīcijas attīstībā kiberjautājumos.

3. Padome uzsver, ka arī nesenie kiberuzbrukumi Eiropas kritiskajai infrastruktūrai, strauji mainīgā kiberapdraudējumu aina un tehnoloģiskās attīstības ātrā gaita parāda, ka ir jāuzlabo civilā un militārā koordinācija un sadarbība, bet vienlaikus pasvītro, ka starp civilajām un militārajām aprindām nepastāv hierarhiskas attiecības.
ES kiberaizsardzības politika dod ES un tās dalībvalstīm iespējas stiprināt to spēju aizsargāt, atklāt, aizstāvēt un atturēt, pienācīgi izmantojot visu veidu aizsardzības iespējas, kas pieejamas civilajām un militārajām aprindām plašākas ES drošības un aizsardzības ietvaros, to darot saskaņā ar starptautiskajām tiesībām, tostarp starptautiskajām cilvēktiesībām un starptautiskajām humanitārajām tiesībām.

4. Kaut gan, kā norādīts LES 4. panta 2. punktā, nacionālā drošība, arī kibertelpā, arvien paliek katras dalībvalsts pilnīgā pārziņā, Padome tomēr uzsver, ka individuāli un kopīgi ir būtiski jāinvestē noturības uzlabošanā un pilna uz aizsardzību vērstu kiberaizsardzības spēju spektra izvēršanā un efektīvi jāizmanto ES sadarbības satvari un finansiālie stimuli. Padome uzsver vajadzību pēc turpmākas stiprinošas dalībvalstu un ES iestāžu, struktūru un aģentūru (ESISA) rīcības, lai aizsargātu Savienību, mūsu pilsoņus, ESISA un KDAP misijas un operācijas kibertelpā. Turklāt tā uzsver, cik svarīga ir ES noturība kibertelpā, kas panākama, pilnveidojot kiberaizsardzības spējas un uzlabojot sadarbību ar uzticamu privātā sektora ekosistēmu.

I. **Darboties kopā stiprākas kiberaizsardzības vārdā**

5. Padome atkārtoti norāda, ka lielākas uzticēšanās panākšanai būtisks ir pakāpenisks, pārredzams un iekļaujošs process, – lielāka uzticēšanās ir kritiski svarīga ES kiberdrošības krīžu pārvarēšanas satvara turpmākai attīstībai, kas būtu panākams saskaņā ar Padomes izstrādāto kiberkrīžu pārvarēšanas ceļvedi. Padome atkārto, ka ir jāturpina uzlabot mūsu spēja aizsargāt no kiberuzbrukumiem, atklāt tos, aizstāvēt pret tiem un atturēt no tiem ar labāku situācijas apzināšanos, spēju veidošanu, apmācību, mācībām un lielāku noturību, kā arī, ar visiem atbilstīgajiem līdzekļiem stingri reaģējot uz kiberuzbrukumiem, kas vērsti pret ES, tās dalībvalstīm, ESISA, KDAP misijām un operācijām. Attiecīgi Padome mudina Augsto pārstāvi un Komisiju mazināt sarežģītību attiecībā uz kiberjomu, izvairīties no nevajadzīgas dublēšanās un nodrošināt sadarbību un sinerģiju ar jau esošajām iniciatīvām. Ir jāstiprina sadarbība un koordinācija kiberaizsardzības aktoru vidū ES un dalībvalstīs, starp militārajām un civilajām kiberaprindām un starp publisko un uzticamu privāto ekosistēmu. Šajā kontekstā dalībvalstis tiek mudinātas dziļāk izskatīt un stiprināt nacionālos civilmilitāros koordinācijas mehānismus, atvieglot kopējo brīvprātīgo informācijas apmaiņu, apmainīties gūtajām atziņām, veicināt sadarbspējīgu standartu pilnveidi un veikt riska novērtējumus un riska scenāriju izstrādi, kā arī īstenot kopīgas mācības, īpaši Eiropas līmenī, pilnībā ievērojot noteikumus Direktīvā, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību (TID 2 direktīva).

6. Atzīstot centienus vēl vairāk uzlabot Savienības noturību ar TID 2 direktīvu un Kritisko vienību noturības (KVN) direktīvu, Padome atkārto savu ieteikumu attiecībā uz ES mēroga koordinētu pieeju kritiskās infrastruktūras stiprināšanai [1]. Tā aicina veikt pasākumus vēl labākai kritisko vienību, infrastruktūras, digitālo produktu un pakalpojumu noturībai, vienlaikus atzīmējot, ka vissvarīgākais pasākums joprojām ir pienācīga TID 2 direktīvas īstenošana. Kaut arī par to pārsvarā atbildīgs ir civilais sektors, tas arī sekmē spēcīgāku kiberaizsardzību. Šajā kontekstā gan ESISA, gan dalībvalstis tiek mudinātas atbalstīt, ka tiek pilnveidoti un izvērsti jauni un esošie ES koordinācijas mehānismi, riska novērtējumi, izvērtējumi un scenāriji, kopējā brīvprātīgā informācijas apmaiņa un mācības – tā, lai tas radītu pievienoto vērtību un ļautu izvairīties no nevajadzīgas dublēšanās ar jau pastāvošām iniciatīvām.

7. Lai vēl vairāk stiprinātu uzticēšanos, konsolidētu sadarbību un sekmētu savlaicīgu informācijas apmaiņu par nozīmīgiem un liela mēroga kiberdrošības incidentiem, kuri ietekmē aizsardzības sistēmas, Padome atzinīgi vērtē iniciatīvu pilnveidot ES kiberdrošības komandieru konferenci, ko paredzēts organizēt katrai ES Padomes dalībvalstij ar Eiropas Aizsardzības aģentūras (EAA) atbalstu un piedaloties Eiropas Ārējās darbības dienestam (EĀDD). Padome mudina visas dalībvalstis piedalīties šajās sanāksmēs. Lai stiprinātu ES noturību pret liela mēroga kiberdrošības incidentiem, Padome aicina ES Kiberkrīžu sadarbības organizāciju tīklu (*EU-CyCLONe*) un ES kiberdrošības komandieru konferenci apzināt iespējamos veidus, kā sadarboties un gūt labumu no kopīgas militāras un civilas perspektīvas.

[1] Priekšlikums – Padomes Ieteikums par koordinētu Savienības pieeju kritiskās infrastruktūras noturības stiprināšanai, COM/2022/551.

8. Lai veicinātu stabilāku un koordinētāku ES līmeņa reaģēšanu, Padome atzinīgi vērtē to, ka ir izveidots ES militāro datorapdraudējumu reaģēšanas vienību operatīvais tīkls (*MICNET*), un gaida, ka līdz 2024. gada vidum tas sasniegs sākotnējās operatīvās spējas; tīkls izveidots nolūkā starp dalībvalstīm uzlabot tehniskās informācijas apmaiņu par kiberincidentiem, kas skar aizsardzības sistēmas. Padome mudina visas dalībvalstis piedalīties *MICNET*, lai nodrošinātu tīkla efektivitāti. Papildus tam Padome aicina dalībvalstis ņemt vērā saistībā ar datordrošības incidentu reaģēšanas vienībām (*CSIRT*) gūtās atziņas un stingri mudina starp abiem tīkliem pienācīgā laikā izveidot efektīvu sadarbības un koordinācijas mehānismu, pilnībā ievērojot katras vienības pārvaldības mehānismus un struktūru.

9. Ņemot vērā to, ka pieaug ļaunprātīgu kiberdarbību skaits, ko veic valsts un nevalstiski aktori pret ES KDAP misijām un operācijām, Padome aicina ES un tās dalībvalstis stiprināt savas spējas aizsargāt un padarīt drošas KDAP misijas un operācijas. Šajā sakarā Padome atzinīgi vērtē mērķus vēl vairāk attīstīt ES militāro tīklu un struktūru aizsardzību cita starpā saskaņā ar ES Militāro redzējumu un stratēģiju par kibertelpu kā operacionālo telpu [2].

[2] EEAS(2021) 706 REV4.

10. Padome atkārtoti uzsver Padomes 2022. gada maija secinājumus [3] un nepieciešamību ieguldīt mūsu savstarpējā palīdzībā saskaņā ar LES 42. panta 7. punktu un solidaritātes klauzulu LESD 222. pantā. Padome uzsver, cik svarīgi ir vēl vairāk padziļināt ES un tās dalībvalstu kopējo izpratni par 42. panta 7. punkta īstenošanu atbilstīgi attiecīgajiem starptautisko tiesību principiem, tostarp sarežģītos scenārijos, kuros iesaistīts kiberuzbrukums. Tā atzinīgi vērtē iespēju pēc attiecīgās dalībvalsts (attiecīgo dalībvalstu) skaidra pieprasījuma sniegt ES atbalstu kiberuzbrukuma gaitā, neskarot dažu dalībvalstu drošības un aizsardzības politikas īpašās iezīmes.

11. Padome uzsver progresu, kas panākts *PESCO* projektā "Kiberdrošības ātrās reaģēšanas vienības un savstarpēja palīdzība kiberdrošības jomā" (*CRRT*) un tā gatavību pēc pieprasījuma būt par spēju, ko izmanto dalībvalstu un ES vajadzībām KDAP misiju un operāciju atbalstam un palīdzības sniegšanai ES partneriem. Padome atzinīgi vērtē, ka ir pilnveidotas *PESCO CRRT* spējas, valstu vienības reaģēšanai uz kiberdraudiem un attiecīgos gadījumos papildu spējas reaģēšanai uz incidentiem, piemēram, Stratēģiskajā kompasā nākotnē iecerētās ES hibrīddraudu novēršanas ātrās reaģēšanas vienības, tostarp, veicinot to koordināciju un sadarbību ES līmenī.

[3] Padomes secinājumi par Eiropas Savienības pozīcijas kiberjautājumos izstrādi, 2022. gada 23. maijs, dok. 9364/22.

12. Padome atzinīgi vērtē *PESCO* projekta "Kibertelpas un informācijas telpas koordinācijas centrs" (*CIDCC*), kura mērķis ir nodrošināt militāras spējas vākt un analizēt informāciju, kas attiecas uz kopējo operacionālo kiberainu. Turklāt Padome atzinīgi vērtē priekšlikumu koncepcijas pierādījumu, ja tas sekmīgi darbosies kā informācijas koordinācijas centrs, no 2025. gada integrēt ES Kiberaizsardzības koordinācijas centrā (*EUCDCC*), uzlabojot koordināciju un situācijas apzināšanos, jo īpaši attiecībā uz ES KDAP misiju un operāciju komandieriem, kā arī stiprinot kopējo ES vadības un kontroles arhitektūru. Padome aicina Augsto pārstāvi nākt klajā ar koncepciju un ceļvedi *EUCDCC* izveidei, ņemot vērā pieredzi ar līdzīgām starptautiskām struktūrām, apzinot vajadzīgos resursus, izvairoties no nevajadzīgas dublēšanās un cenšoties panākt papildināmību ar kopējo ES kiberdrošības satvaru.

13. Padome uzsver, cik svarīga ir stratēģiska sadarbība izlūkošanas jomā saistībā ar kiberapdraudējumiem un darbībām, un aicina dalībvalstis ar savu kompetento iestāžu starpniecību turpināt sniegt ieguldījumu ES Izlūkošanas un situāciju centra (*INTCEN*), ES Militārā štāba (*EUMS*) Izlūkošanas direktorāta darbā un dalībvalstu darbā, kas notiek vienotās izlūkdatu analīzes procedūras (*SIAC*) ietvaros. Padome arī uzsver, cik svarīgi ir stiprināt mūsu kiberizlūkošanas spējas, lai uzlabotu mūsu kibernoturību un reaģēšanu un nodrošinātu efektīvu atbalstu mūsu civilajām un militārajām KDAP misijām un operācijām, kā arī mūsu bruņotajiem spēkiem un *SIAC* spējai kibertelpā, balstoties uz dalībvalstu brīvprātīgi sniegtu izlūkinformāciju un neskarot to kompetenci.

14. Padome pieņem zināšanai Eiropas Komisijas kibersituāciju un analīzes centru, kura mērķis ir uzlabot Komisijas situācijas apzināšanos. Padome uzsver, cik svarīgi ir izveidot savstarpēji izdevīgu sadarbību starp minēto centru un citām ESISA, jo īpaši *ENISA* un *CERT-EU*. Padome uzsver, cik svarīgi situācijas apzināšanās izveidē ir nodrošināt ciešu sadarbību ar ES sadarbības tīkliem un ievērot konfidencialitāti. Padome atzīmē, ka ir jāstiprina kopējā situācijas apzināšanās ES līmenī un jāturpina attīstīt ES kiberdrošības krīžu pārvarēšanas satvars, vienlaikus izvairoties no nevajadzīgas centienu dublēšanās.

15. Padome atgādina, ka ar kiberjomu saistīta izglītība, apmācība un mācības ir būtiska tam, lai nodrošinātu gatavību un efektivitāti, un atzinīgi vērtē valsts līmeņa darbības, kā arī darbības, ko nodrošina ES ar Eiropas Drošības un aizsardzības koledžas (EDAK), EAA, *ENISA* un aktuālo *PESCO* projektu starpniecību, tādu kā "Kiberpoligonu federācijas" un ES Kiberlietu akadēmija un inovācijas centrs" (*CAIH*) Lai šos centienus vēl vairāk pastiprinātu, Padome gaida EAA pamatprojekta *CyDEF-X* izveidi, lai sinhronizētu un atbalstītu mācības kiberaizsardzības jomā. Padome mudina EAA ciešā sadarbībā ar dalībvalstīm un EĀDD izpētīt, kā *CyDEF-X* varētu vēl vairāk atbalstīt tādas mācības kā *CYBER PHALANX*, tostarp saistībā ar LES 42. panta 7. punktā paredzēto savstarpējo palīdzību un LESD 222. panta solidaritātes klauzulu, kā arī sadarbībā ar Komisiju un *ENISA* attiecībā uz civilām mācībām. Turklāt Padome mudina *CyDef-X* ietvaros izmantot un pilnveidot esošās kiberaizsardzības testēšanas un mācību vides, piemēram kiberpoligonu federācijas. Lai nodrošinātu elastīgu un rezultatīvu lēmumu pieņemšanas procesu kiberkrīžu jomā, Padome uzsver, cik svarīgi ir rīkot regulāras teorētiskās mācības dalībvalstu lēmumu pieņēmējiem.

16. Padome pieņem zināšanai priekšlikumu kibersolidaritātes aktam un nodomu uzlabot spējas kiberapdraudējumu un incidentu atklāšanai un reaģēšanai uz tiem Eiropas Savienībā. Padome uzsver, ka priekšlikumi šajā jomā var būt efektīvi tikai tad, ja tie ir saskaņoti ar dalībvalstu krīžu pārvarēšanas satvariem un vajadzībām. Padome uzsver, cik svarīgi ir testēt kritiskās infrastruktūras iespējamās ievainojamības, – ja to atzīst par lietderīgu un tas ir valsts kompetencē, ņemot vērā pieejamos ES riska novērtējumus.

17. Padome pieņem zināšanai Komisijas priekšlikumu izveidot ārkārtas reaģēšanas mehānismu kiberdrošības jomā, kurš varētu atbalstīt tādu kiberdrošības pakalpojumu pieejamību, ko sniedz uzticami privātie pakalpojumu sniedzēji, lai pēc pieprasījuma palīdzētu dalībvalstīm liela mēroga kiberdrošības incidentu gadījumā, vienlaikus uzsverot, ka ir plašāk jāizvērš Eiropas kiberdrošības industrija ar *ECCC* atbalstu, kas būtu būtisks pīlārs šā mehānisma darbības nodrošināšanā. Padome uzsver, ka katrai dalībvalstij ir būtiska loma savu valsts līmeņa vajadzību uzraudzīšanā un novērtēšanā.

II. **Droša ES aizsardzības ekosistēma**

18. Padome atgādina, ka tā mudina dalībvalstis pilnveidot pašu spējas veikt kiberaizsardzības operācijas, tostarp attiecīgos gadījumos proaktīvus aizsardzības pasākumus nolūkā aizsargāt no kiberuzbrukumiem, atklāt tos, aizstāvēt pret tiem un atturēt no tiem. Tā kā TID 2 direktīva neattiecas uz publiskās pārvaldes struktūrām, kas savu darbību īsteno aizsardzības jomā, Padome aicina EAA ar Komisijas un attiecīgā gadījumā EĀDD atbalstu palīdzēt dalībvalstīm izstrādāt juridiski nesaistošus brīvprātīgus ieteikumus, kuru pamatā ir TID 2 direktīva, lai palielinātu kiberdrošību aizsardzības aprindās, un aicina visas dalībvalstis aktīvi iesaistīties šajos centienos. Šajos ieteikumos būtu jāņem vērā līdzīgs darbs, kas veikts citos satvaros.

19. Kā atzīts Stratēģiskajā kompasā, ES spēja rīkoties ir atkarīga no tā, vai tā varēs samazināt savas stratēģiskās atkarības tās kiberaizsardzības spējās un piegādes ķēdēs, kā arī izstrādāt un apgūt visprogresīvākās kiberaizsardzības tehnoloģijas. Tas ietver Eiropas aizsardzības tehnoloģiskās un industriālās bāzes (*EDITB*) stiprināšanu visā ES, kā arī tās spēju sadarboties ar līdzīgi domājošiem partneriem visā pasaulē uz savstarpības pamata, lai nodrošinātu abpusējus ieguvumus. Tāpēc Padome aicina kiberdrošības un kiberaizsardzības industrijas cieši sadarboties, lai veidotu sinerģijas nolūkā izveidot un īstenot pilnu kiberaizsardzības spēju spektru. Padome aicina Komisiju attiecīgā gadījumā ciešā sadarbībā ar *ECCC*, veicot turpmākas investīcijas un īstenojot politikas pasākumus, turpināt atbalstīt spēcīgas, elastīgas, globāli konkurētspējīgas un inovatīvas Eiropas kiberaizsardzības industriālās un tehnoloģiskās bāzes izveidi, kas ietver arī mazus un vidējus uzņēmumus (MVU).

20. Ņemot vērā to, cik svarīga kiberaizsardzības spējām ir sadarbspēja un kopība, tostarp attiecībā uz nākamās paaudzes kiberaizsardzības spēju sadarbīgu izstrādi, Padome aicina EAA un ES Militāro štābu strādāt pie ES kiberaizsardzības sadarbspējas prasību kopuma, kura pamatā būtu un kas būtu saderīgs ar esošajiem principiem, procesiem un standartiem, kas iedibināti jo īpaši Ziemeļatlantijas līguma organizācijas (NATO) satvarā. Turklāt Padome aicina dalībvalstis Eiropas Aizsardzības standartizācijas komitejas satvarā, cieši sadarbojoties ar visām attiecīgajām ieinteresētajām personām, tostarp attiecīgā gadījumā ar Eiropas standartizācijas organizācijām un NATO, izpētīt, vai varētu būt vajadzīgi specifiski brīvprātīgi standarti aizsardzības sistēmām.

21. Padome atzinīgi vērtē Komisijas centienus nākt klajā ar plānu nolūkā veicināt esošo standartu izmantošanu attiecībā uz civiliem kiberdrošības un kiberaizsardzības lietojumiem, kā arī jaunu brīvprātīgu standartu izstrādi. Padome uzsver, ka kiberdrošības un kiberaizsardzības standarti attiecīgā gadījumā ir jāsaskaņo. Padome atzīst, ka šādi brīvprātīgi standarti varētu būt lietderīgi ES kiberdrošības un kiberaizsardzības industrijām un mudina uz ciešāku sadarbību starp civilām un aizsardzības standartizācijas struktūrām.

22. Padome aicina ātri izstrādāt ieteikumus, kas balstīti uz esošo kibertelpas drošas komunikācijas rīku kartēšanu, ko veiktu Komisija un attiecīgās iestādes. Ieteikumiem pēc iespējas vajadzētu būt saskaņotiem ar esošām iniciatīvām saistībā ar informācijas apmaiņu, un tajos arī būtu jāņem vērā riski, ko pašreizējām šifrēšanas metodēm rada jaunas un revolucionāras tehnoloģijas.

23. Turklāt Padome atzinīgi vērtē sākotnējo darbu, kas ir paveikts saistībā ar risku izvērtēšanu, un scenārijus, ko šobrīd izstrādā (sākotnēji – attiecībā uz enerģētikas un telesakaru nozarēm) Komisija, Augstais pārstāvis un TID sadarbības grupa. Padome atzīst, ka šobrīd tiek gatavoti arī mērķorientēti kiberdrošības riska novērtējumi komunikācijas infrastruktūrai un tīkliem Eiropas Savienībā. Padome atkārtoti norāda, ka ārkārtīgi svarīga ir kopīga izpratne par kiberincidentu iespējamo ietekmi starp dalībvalstīm un arī ES iestādēm, struktūrām un aģentūrām. Tādējādi Padome aicina minētos aktorus nodrošināt, ka riska izvērtējumi, scenāriji un no tiem izrietošie ieteikumi tiek ņemti vērā, kad tiek definēti ES un attiecīgos gadījumos valstu līmeņa pasākumi un atbalsts un noteikta to prioritārā kārtība. Turklāt Padome aicina visus attiecīgos aktorus riska scenārijus ņemt vērā riska novērtēšanas procesos un kiberdrošības mācību izstrādē.

III. **Investēt kiberaizsardzības spējās**

24. Padome mudina dalībvalstis palielināt investīcijas nolūkā veidot, uzturēt un pilnveidot sadarbspējīgas kiberaizsardzības spējas. Padome atbalsta to, ka tiek izstrādāts brīvprātīgu saistību kopums attiecībā uz nacionālo kiberaizsardzības spēju izveidi, paturot prātā līdzīgus centienus, kas tiek īstenoti citos satvaros.

25. Padome aicina dalībvalstis un EAA izmantot iespēju, ko sniedz Spēju attīstības plāna pārskatīšana, lai nospraustu vērienīgus mērķus attiecībā uz sadarbīgas kiberaizsardzības izveidi ES līmenī. Tāpat Padome mudina dalībvalstis, par pamatu ņemot atjaunināto prioritāšu kopumu un to *PESCO* saistības, palielināt iesaistes līmeni sadarbīgos ES kiberaizsardzības spēju veidošanas projektos, atzīstot tiešos ieguvumus, ko ES līmeņa sadarbīgi projekti sniedz nacionālo kiberaizsardzības spēju veidošanas sekmēšanā.

26. Padome atzinīgi vērtē sadarbīgas pētniecības centienus ES līmenī, kas vērsti uz to, lai pētītu jaunu un revolucionāru tehnoloģiju iespējamos pielietojumus ar aizsardzību saistītās sistēmās, vienlaikus atzīmējot, ka ir jānodrošina, lai minētie tehnoloģiskie jauninājumi tiktu ātri integrēti esošajās un turpmākajās spējās. Padome mudina dalībvalstis un ES industriju pēc iespējas labāk izmantot ES līmeņa sadarbīgās pētniecības iespējas, piemēram, EAA satvarā, spēkā esošajos *PESCO* projektos (tādos kā "ES Kiberlietu akadēmija un inovācijas centrs" (*CAIH*)), Eiropas Aizsardzības fonda ietvaros un attiecīgos gadījumos programmu "Apvārsnis Eiropa" un "Digitālā Eiropa" divējāda lietojuma projektos. Turklāt Padome atzinīgi vērtē speciālo satvaru izmantošanu tam, lai atbalstītu inovāciju aizsardzības jomā, pārņemot jauninājumus no civilās jomas, īpaši ES aizsardzības inovācijas shēmu un Aizsardzības inovācijas centru. Tāpat Padome mudina Eiropas Kiberdrošības kompetenču centru (*ECCC*) un EAA izveidot darba mehānismu, kā atvieglot informācijas apmaiņu starp to darbiniekiem par prioritātēm attiecīgi civilo, divējāda lietojuma un aizsardzības tehnoloģiju jomā, lai radītu sinerģijas un izvairītos no dublēšanās.

27. Padome atzinīgi vērtē Komisijas nodomu sadarbībā ar EAA un *ECCC* saskaņā ar to attiecīgajām pilnvarām, ar dalībvalstīm un konsultējoties ar attiecīgajām ieinteresētajām personām, piemēram, industrijā, izstrādāt kritisko kibertehnoloģiju ceļvedi, kurš, identificējot kritiskās kibertehnoloģijas, kartējot tehnoloģisko attīstību un stratēģiskās atkarības, paredz veidus, kā tās mazināt, tā atbalstot ES stratēģisko autonomiju un tehnoloģisko suverenitāti, vienlaikus saglabājot atvērtu ekonomiku. Padome norāda, ka kritisko kibertehnoloģiju ceļvedis var ietekmēt ES finansēšanas instrumentu stratēģiskās prioritātes, vienlaikus ievērojot attiecīgo kārtību, kāda pastāv saistībā ar tiem. Padome atgādina, ka ES būtu jāīsteno vērienīga un pārliecināta Eiropas industriālā politika, lai radītu ilgtspējīgu, pievilcīgu un konkurencē balstītu uzņēmējdarbības vidi, kas arī var dot iespēju Eiropas kiberjomas struktūrām paplašināt darbību.

28. Padome ir gandarīta par nodomu risināt nozīmīgo prasmju trūkuma problēmu kiberdrošības jomā, piesaistot jaunus speciālistus, tostarp sievietes, īstenojot kvalifikācijas celšanas un pārkvalifikācijas pasākumus un investējot apmācībā un mācībās un tās rīkojot nolūkā veidot daudzveidīgu un iekļaujošu darbaspēku kiberjomā. Atzīstot izaicinājumus, ar ko ES saskaras saistībā ar cilvēkkapitālu kiberdrošības un kiberaizsardzības jomā, Padome atzinīgi vērtē Kiberdrošības prasmju akadēmijas iniciatīvu, kas varētu nest ieguvumus arī attiecībā uz kiberaizsardzības jomas darbaspēku.

29. Padome aicina dalībvalstis apmainīties ar informāciju par paraugpraksi kvalificētu kiberdrošības speciālistu prasmju pilnveidošanā, izmantojot sinerģijas starp militārām, civilām un tiesībaizsardzības iniciatīvām, un aicina EDAK ar EAA un *ENISA* atbalstu izskatīt iespējas uzlabot paraugprakses apmaiņu un rast vēl lielākas sinerģijas starp militāro un civilo jomu attiecībā uz apmācību un kiberjomai specifisku aizsardzības prasmju veidošanu.

30. Padome uzsver, cik svarīga ir kopīga izpratne par kiberdrošības jomas darbaspēka sastāvu un attiecīgajām prasmēm, lai apzinātu nepilnības kiberdrošības darba tirgū un pievērstos tām, kā arī nepieciešamība darbā iesaistīt visas ieinteresētās personas, tostarp dalībvalstis un industriju. Padome atzīst, ka rādītāju noteikšana kiberdrošības darba tirgus monitoringa nolūkos palīdzētu apzināt vajadzības saistībā ar kiberdrošības prasmēm un pienācīgi novirzīt finanšu līdzekļus, vienlaikus sekmējot ar politiku saistīto pienākumu (īpaši tādu, kas izriet no TID 2 direktīvas) izpildi. Padome atzinīgi vērtē priekšlikumu par kiberaizsardzības prasmju sertifikācijas satvaru un aicina Augsto pārstāvi, kurš ir EDAK vadītājs, to izstrādāt sadarbībā ar EĀDD, Komisiju un dalībvalstīm, lietderīgi izmantojot civilās iniciatīvas.

IV. **Veidot partnerības, lai stātos pretī kopīgiem izaicinājumiem**

31. Padome aicina Augsto pārstāvi un Komisiju stiprināt un virzīt uz priekšu to sadarbību un izskatīt savstarpēji izdevīgu un pielāgotu partnerību iespējas attiecībā uz kiberaizsardzības politiku, tostarp kiberaizsardzības spēju veidošanu, izmantojot Eiropas Miera mehānismu (EMM). Šajā nolūkā kiberaizsardzība būtu jāiekļauj kā jautājums ES dialogos un konsultācijās par kiberlietām un vispārējām drošības un aizsardzības konsultācijām ar partneriem. Turklāt būtu jāpastiprina dialogi un sadarbība ar privāto sektoru. Padome uzsver, ka starptautiska sadarbība kiberdrošības standartu un sertifikācijas jautājumos radītu pievienoto vērtību Eiropas industrijai. Tāpēc tā atzinīgi vērtē Komisijas apņemšanos šo aspektu padarīt par būtisku elementu ES kiberdialogos ar trešām valstīm un starptautiskām organizācijām.

32. Padome uzsver, cik svarīga ir starptautiskā sadarbība tam, lai novērstu vai mazinātu konflikta riskus kibertelpā, īpaši pilnveidojot un iedarbinot uzticības veicināšanas pasākumus reģionālā un starptautiskā līmenī, tostarp ANO, un vēl vairāk iedrošinot izmantot jau esošos uzticības veicināšanas pasākumus kiberjomā, piemēram, Eiropas Drošības un sadarbības organizācijā (EDSO), tostarp starptautiskas spriedzes laikā.
ES un tās dalībvalstis uzsver, ka esošās starptautiskās tiesības attiecas uz kibertelpu, un uzsver, cik svarīgi ir turpināt centienus atbalstīt un veicināt ANO sistēmu attiecībā uz valstu atbildīgu rīcību un strādāt pie tās īstenošanas, tostarp, izveidojot rīcības programmu valstu atbildīgas rīcības veicināšanai kibertelpā.

33. Atbilstīgi kopīgajām deklarācijām par ES un NATO sadarbību Padome aicina Augsto pārstāvi (tostarp EAA vadītāja statusā) un Komisiju vēl vairāk stiprināt, padziļināt un paplašināt partnerību kibertelpā ar NATO, pilnībā ievērojot iekļautības, savstarpības, abpusējas atklātības un pārredzamības principus, kā arī abu organizāciju lēmumu pieņemšanas autonomiju. Ņemot vērā nepieciešamību nodrošināt papildinošus un koordinētus centienus, maksimāli iesaistot dalībvalstis, kuras nav NATO dalībvalstis, un izvairīties no nevajadzīgas dublēšanās, Padome vienlaikus aicina veidot attiecīgā līmeņa saites starp ES un NATO saistībā ar apmācību, izglītību, situācijas apzināšanos, mācībām un pētniecības un izstrādes platformām un censties panākt iespējamas sinerģijas starp attiecīgajām brīvprātīgajām saistībām attīstīt nacionālās kiberaizsardzības spējas un krīzes pārvarēšanas satvarus, kritiskās infrastruktūras aizsardzību un uzlabotu apmaiņu situācijas apzināšanās jomā, koordinētu reakciju uz ļaunprātīgām kiberdarbībām, kā arī spēju veidošanas centienus trešās valstīs. Tas cita starpā ietver tehnisko vienošanos starp NATO Datorincidentu reaģēšanas spējām (*NCIRC*) un ES datorapdraudējumu reaģēšanas vienību (*CERT-EU*), kā arī ciešāku politisko dialogu par kiberaizsardzības jautājumiem visos līmeņos.

V. **Nobeigums**

34. Pamatojoties uz Padomes secinājumiem par ES kiberaizsardzības politiku, Padome aicina Augsto pārstāvi un Komisiju līdz 2023. gada otrajam ceturksnim dalībvalstu apstiprināšanai izstrādāt politikas īstenošanas plānu. Padome arī aicina dalībvalstis brīvprātīgi paziņot savu mērķu vērienīgumu un rīcību attiecībā uz kiberaizsardzību ES kiberaizsardzības politikas kontekstā un pilnvērtīgi izmantot juridiski nesaistošus brīvprātīgus ieteikumus un saistības pastiprināt savus nacionālos un starptautiskos kiberaizsardzības centienus nolūkā panākt maksimālu iedarbību ES līmenī. Augstais pārstāvis, Komisija un dalībvalstis tiek aicinātas līdz 2024. gada otrajam ceturksnim sākt ik gadus ziņot un apspriesties par progresu, kas panākts kopīgā paziņojuma un tā īstenošanas plāna elementu īstenošanā.