Eiropas Savienības
Padome

Briselē, 2024. gada 6. decembrī
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Saņēmējs:	delegācijas
Temats:	Padomes secinājumi par *ENISA*

Pielikumā ir pievienoti Padomes secinājumi par *ENISA*, kurus Padome apstiprināja 2024. gada 6. decembra sanāksmē.

PIELIKUMS

Projekts – Padomes secinājumi par *ENISA*

EIROPAS SAVIENĪBAS PADOME

1. UZSVER, ka izaicinājumi, ko rada globālā kibertelpa, nekad nav bijuši tik sarežģīti, daudzveidīgi un nopietni kā pašlaik, ņemot vērā jauno kiberdraudu sarežģītību, pastāvīgi mainīgo drošības vidi un pašreizējo ģeopolitisko spriedzi. Tāpēc ES un tās dalībvalstīm būtu jāturpina centieni kļūt noturīgākām nolūkā efektīvi apzināt pašreizējos un jaunos apdraudējumus un izaicinājumus un reaģēt uz tiem. UZSVER, ka darbs pie augstāka kibernoturības līmeņa būtu jāturpina, izmantojot visas sabiedrības pieeju. UZSVER, ka turpmākajos gados ES un tās dalībvalstīm būtu jākoncentrējas uz tādu leģislatīvu un neleģislatīvu iniciatīvu efektīvu īstenošanu, kas ir visu līdz šim šajā jomā veikto darbību pamatā un sekmē to īstenošanu.

2. ATGĀDINOT, ka valsts drošība paliek vienīgi katras dalībvalsts atbildībā, ATZĪST, ka ES un tās dalībvalstis pēdējos gados ir ļoti cieši sadarbojušās, lai kiberjomā izveidotu nepieciešamo institucionālo struktūru un sadarbības veidus gan valstu, gan ES līmenī. ATZINĪGI VĒRTĒ dažādās leģislatīvās un neleģislatīvās iniciatīvas, kas ES un tās dalībvalstīm ir nodrošinājušas spēcīgu un stabilu satvaru šajā jomā, palielinot Savienības vispārējo kibernoturību. Šis satvars ir attīstījies, lai aptvertu vairākus kiberjomas aspektus: drošību, diplomātiju, tiesībaizsardzību un aizsardzību. NORĀDA, ka liels skaits aktoru, tostarp dalībvalstu kiberdrošības iestādes, TID sadarbības grupa (TID SG), *CSIRT* tīkls, Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*), Nacionālo koordinācijas centru tīkls (*NCC*), Eiropas Kiberdrošības sertifikācijas grupa (*ECCG*), Komisija, Eiropas Ārējās darbības dienests (EĀDD), Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), Eiropas Kiberdrošības kompetenču centrs (*ECCC*), *CERT-EU*, Eiropas Aizsardzības aģentūra (EAA) un Eiropola Eiropas Kibernoziedzības apkarošanas centrs (*EC3*), ir daļa no ES kiberdrošības ekosistēmas, un katrs no šiem aktoriem veic savu daļu ES mēroga kiberdrošības satvara īstenošanā.

3. ATZĪST – pēdējo divdesmit gadu laikā *ENISA* ir pierādījusi, ka ir nenovērtējama vienība Eiropas kiberdrošības ekosistēmā un tai ir izšķiroša nozīme, aktīvi atbalstot dalībvalstis un ES iestādes, struktūras, birojus un aģentūras (*EUIBA*) kiberdrošības politikas īstenošanā un izstrādē, spēju veidošanā un sagatavotībā, sadarbībā un kiberdrošības izpratnes un sertifikācijas veicināšanā.

VISPĀRĪGI POLITIKAS IETEIKUMI

4. AICINA Komisiju izmantot **Kiberdrošības akta izvērtēšanu** kā iespēju izpētīt, kā tas var palīdzēt vienkāršot sarežģīto kiberekosistēmu, tādējādi uzlabojot resursu efektivitāti un lietderīgu izmantošanu. Tādēļ AICINA Komisiju nodrošināt, ka *ENISA* pilnvaras atbalstīt dalībvalstis un ES iestādes, struktūras, birojus un aģentūras (*EUIBA*) ir mērķtiecīgas un skaidri definētas ar konkrētiem stratēģiskiem mērķiem un prioritāriem uzdevumiem, kā arī precīzāku uzdevumu un kompetenču sadalījumu attiecībā uz citiem aktoriem. Šajā sakarā AICINA Komisiju izskatīt un vēl vairāk stiprināt *ENISA* lomu operatīvās sadarbības atbalstīšanā ES līmenī un starp dalībvalstīm, lai uzlabotu kibernoturību, ņemot vērā dalībvalstu kompetenci šajā jomā. Turklāt AICINA Komisiju stiprināt *ENISA* padomdevējas lomu, lai tā varētu sniegt ekspertu un uz pierādījumiem balstītus norādījumus un ieteikumus attiecībā uz pašreizējo un turpmāko ES leģislatīvo un neleģislatīvo iniciatīvu īstenošanu, vienlaikus nodrošinot saskaņotu ES kiberdrošības satvaru.

5. Tādā pašā garā MUDINA Komisiju apsvērt iespēju racionalizēt *ENISA* lomu attiecībā uz uzdevumiem, kuri nav tās pilnvaru pamatā. UZSVER, ka *ENISA* **pienākumi ir ievērojami paplašināti** ar nesenajām leģislatīvajām iniciatīvām, tostarp TID 2, Kibernoturības aktu un Kibersolidaritātes aktu. ATZĪMĒ, ka dažu šo iniciatīvu rezultātā *ENISA* ir saņēmusi papildu resursus, taču UZSVER, ka *ENISA* pienākumu paplašināšanās un kiberdraudu un izaicinājumu pieaugošās sarežģītības dēļ tās uzdevumu apjoms ir ievērojami pieaudzis, kas būtu jāatspoguļo **atbilstošos resursos** – cilvēkresursos, finanšu un tehniskajos resursos –, lai aģentūra varētu pilnībā veikt visus tās kompetencē esošos uzdevumus, neapsteidzot sarunas par daudzgadu finanšu shēmu. Šajā nolūkā AICINA Komisiju, sagatavojot Savienības vispārējā budžeta projektu, par prioritāriem noteikt pasākumus un uzdevumus, kas saistīti ar atbalstu dalībvalstīm kibernoturības un operatīvās sadarbības stiprināšanā un Savienības tiesību aktu izstrādē un īstenošanā.

ENISA **ATBALSTS POLITIKAS IZSTRĀDEI UN ĪSTENOŠANAI**

6. ATGĀDINA, ka saskaņā ar pašreizējo kiberdrošības tiesisko regulējumu *ENISA* ir uzticēti vairāki svarīgi atbalsta un padomdevējas pienākumi visā ES. Šajā sakarā ATZINĪGI VĒRTĒ *ENISA* lomu saistībā ar**palīdzības** sniegšanu **dalībvalstīm** leģislatīvu un neleģislatīvu iniciatīvu efektīvā īstenošanā. AICINA *ENISA* ciešā sadarbībā ar TID SG un Komisiju turpināt sniegt vispārēju ieskatu un analīzi par pašreizējo tiesisko vidi kiberdrošības jomā. MUDINA *ENISA* regulāri un strukturēti apmainīties ar tehniskiem norādījumiem un paraugpraksi un aktīvi tos popularizēt, tādējādi palīdzot dalībvalstīm īstenot kiberdrošības politiku un tiesību aktus.

7. ATZĪST *ENISA* būtisko lomu **Eiropas kiberdrošības sertifikācijas shēmu** izstrādē, ar ko tiek nostiprināta uzticēšanās IKT produktiem, pakalpojumiem un procesiem, kā arī pārvaldītiem drošības pakalpojumiem, ņemot vērā gaidāmo Kiberdrošības akta mērķorientēto grozījumu. UZSVER, ka dalībvalstis un nozare ir nobažījušās par ilgo kiberdrošības sertifikācijas shēmu atlases, izstrādes un pieņemšanas procesu; tāpēc MUDINA Komisiju izmantot Kiberdrošības akta izvērtēšanas iespēju, lai rastu veidus, kā panākt vienkāršāku, uz risku balstītu, kā arī pārredzamāku un ātrāku pieeju ES kiberdrošības sertifikācijas shēmu izstrādei, un vienlaikus UZSVER dalībvalstu svarīgo lomu šajā procesā. Turklāt UZSVER, cik svarīgi ir skaidri noteikt atbildību par katras sertifikācijas shēmas uzturēšanu. Turklāt ATGĀDINA, ka *ENISA*, sagatavojot kandidātshēmas, būtu oficiālā, atklātā, pārredzamā un iekļaujošā procesā savlaicīgi jāapspriežas ar visām attiecīgajām ieinteresētajām personām un ka Komisijai, novērtējot pieņemto shēmu efektivitāti un izmantošanu, būtu jāapspriežas atklātā, pārredzamā un iekļaujošā veidā. MUDINA *ENISA* vēl vairāk stiprināt sadarbību ar datu aizsardzības kopienu, jo īpaši attiecīgā gadījumā ar Eiropas Datu aizsardzības kolēģiju, un valstu kompetentajām iestādēm, īpašu uzmanību pievēršot sinerģiju veicināšanai saistībā ar turpmāko Eiropas kiberdrošības sertifikācijas shēmu izstrādi.

8. Lai novērstu nevajadzīgu administratīvo slogu, ko varētu radīt sarežģīta ziņošanas sistēma, AICINA *ENISA* sadarbībā ar Komisiju turpināt apmaināties ar informāciju ar dalībvalstīm par ziņošanas procedūras praktiskajiem aspektiem, vienkāršošanu un racionalizēšanu. Turklāt ATGĀDINA savu aicinājumu Komisijai ar *ENISA* un citu attiecīgo ES vienību atbalstu sagatavot kartējumu par attiecīgajiem ziņošanas pienākumiem, kas noteikti attiecīgajos ES tiesību aktos kiberjomā un digitālajā jomā. ATGĀDINA, ka informācijas apmaiņa starp *ENISA* un dalībvalstīm ir balstīta uz attiecībām, kuru pamatā ir uzticēšanās un kurās drošība un konfidencialitāte ir garantēta saskaņā ar Kiberdrošības aktu un attiecīgajiem noteikumiem un protokoliem, un tā būtu jāierobežo līdz tādai, kas ir atbilstīga un samērīga ar apmaiņas mērķi. UZSVER, ka dati un informācija ir jāapstrādā ar pienācīgu rūpību.

9. UZSVER, ka *ENISA* ir atbildīga par **vienotās ziņošanas platformas** izveidi un uzturēšanu **saskaņā ar Kibernoturības aktu**, kurai būs konkrēta operatīvā pievienotā vērtība, jo īpaši attiecībā uz aktīvi izmantotām ievainojamībām un nopietniem incidentiem, kas ietekmē produktu ar digitāliem elementiem drošību. Ņemot vērā šo horizontālo tiesību aktu plašo darbības jomu, vienotajai ziņošanas platformai vajadzētu būt efektīvam un drošam instrumentam, kas atvieglo informācijas apmaiņu starp valstu *CSIRT* un *ENISA*. Tāpēc MUDINA *ENISA* papildus pietiekamu cilvēkresursu piešķiršanai paātrināt platformas izveidi kā vienu no galvenajām prioritātēm, lai nodrošinātu tās gatavību Kibernoturības aktā noteiktajā termiņā.

10. ATZĪST *ENISA* lomu **Eiropas ievainojamību datubāzes** izveidē, kuras mērķis ir nodrošināt labāku pārredzamību attiecībā uz ievainojamību atklāšanu, vienlaikus nodrošinot sensitīvu datu pienācīgu apstrādi. Ņemot vērā TID 2 direktīvas transponēšanas perioda beigas, MUDINA *ENISA* pastiprināt visu nepieciešamo darbu, lai nodrošinātu šīs datubāzes netraucētu darbību. Vienlaikus AICINA TID SG ar *ENISA* palīdzību turpināt publiskot norādījumus, politiku un procedūras attiecībā uz ievainojamību atklāšanu.

11. ATZĪST ieguvumus, ko sniedz *ENISA* īstenotā **kiberdrošības atbalsta darbība**, kas kalpo kā kiberdrošības pakalpojumu kopums, kurš pieejams dalībvalstīm, lai papildinātu to centienus, kā arī *ENISA* pieredzi, kas gūta tās īstenošanā. Šajā sakarā UZSVER, ka *ENISA* vajadzētu uzņemties galveno lomu ES kiberdrošības rezerves pārvaldībā un darbības nodrošināšanā. AICINA *ENISA* nekavējoties pēc Kibersolidaritātes akta stāšanās spēkā sākt nepieciešamo pakalpojumu un to pieejamības kartēšanu, lai ES kiberdrošības rezervi padarītu pēc iespējas lietderīgāku un pielāgotāku lietotāju vajadzībām visās dalībvalstīs. AICINA *ENISA* – tiklīdz tai šis uzdevums tiks uzticēts – agrīnā ES kiberdrošības rezerves izveides procesā iesaistīt dalībvalstis, jo īpaši, apkopojot informāciju par nepieciešamajiem kritērijiem un informējot par gaidāmajiem konkursiem. AICINA *ENISA* – tiklīdz tai šis uzdevums tiks uzticēts – nodrošināt, lai uzticamu pārvaldītu drošības pakalpojumu sniedzēju atlases process būtu pārredzams, atklāts un godīgs un lai pakalpojumu sniedzēji no visām dalībvalstīm varētu tajā piedalīties neatkarīgi no to lieluma. Turklāt ATGĀDINA, ka *ENISA* bez liekas kavēšanās ir jāizdod sadarbspējas pamatnostādnes pārrobežu kibercentriem.

12. UZSVER, ka **ar jaunām tehnoloģijām saistīto tendenču uzraudzībai** strauji mainīgā jomā, tādā kā kiberjoma, ir izšķiroša nozīme, lai saglabātu un vēl vairāk stiprinātu mūsu pozīciju kiberjomā. ATZĪST *ENISA* paveikto darbu, kas vērsts uz to, lai pievērstu sabiedrības uzmanību riskiem un iespējām, ko rada tādas tehnoloģijas kā mākslīgais intelekts un kvantu datošana, tādējādi veicinot labāku izpratni par pašreizējiem izaicinājumiem. MUDINA *ENISA* turpināt sniegt ieguldījumu šo uzdevumu izpildē, aktīvi iestāties par tās ieteikumu īstenošanu un attiecīgā gadījumā konsultēt *ECCC* un sadarboties ar to.

***ENISA* ATBALSTS DALĪBVALSTĪM KIBERNOTURĪBAS UN OPERATĪVĀS SADARBĪBAS UZLABOŠANĀ**

13. UZSVER, ka *ENISA* ir svarīga loma **kā divu ES līmeņa dalībvalstu virzītu kibersadarbības tīklu – *CSIRT* tīkla un *EU-CyCLONe* – sekretariātam**. UZSVER *ENISA* vērtīgo dalību TID SG, jo īpaši, tai aktīvi iesaistoties un sniedzot tehnisku ieguldījumu dažādos darba virzienos. MUDINA *ENISA* arī turpmāk atbalstīt šo tīklu darbību un sadarbību, jo tie nodrošina būtiskus kanālus dalībvalstu sadarbībai dažādos līmeņos.

14. ATKĀRTOTI NORĀDA, ka ES līmenī ir jāuzlabo **kopīga situācijas apzināšanās**, kas veicina ES pozīciju kiberjomā saistībā ar kiberdrošības incidentu atklāšanu, novēršanu un reaģēšanu uz tiem. Šajā sakarā UZSVER, cik svarīgas ir *ENISA* prognozēšanas darbības, regulāri ziņojumi un draudu novērtējumi, kas palīdz uzlabot situācijas apzināšanos. MUDINA *ENISA* cieši sadarboties ar dalībvalstīm, lai palīdzētu veidot situācijas apzināšanos ES līmenī. Šajā sakarā ATZĪST svarīgo lomu, kāda ir *ENISA* kopā ar *CERT-EU* un Eiropolu, atbalstot Padomi ar informatīviem ziņojumiem par situāciju saistībā ar kiberdiplomātijas rīkkopu, kas papildina situācijas apzināšanos, kuru nodrošina vienotā izlūkdatu analīzes procedūra (*SIAC*), un UZSVER, ka ir jāveido visaptveroša apdraudējuma aina, pamatojoties uz dažādiem avotiem, tostarp privāto sektoru. Šajā sakarā MUDINA pilnveidot *ENISA* sadarbību ar EĀDD un jo īpaši ar *INTCEN*, pilnībā ievērojot to attiecīgās pilnvaras.

15. UZSVER, ka Komisijas Kibersituāciju un analīzes centrs veic iekšēju funkciju Komisijā un tam palīdz sadarbība ar *ENISA* un *CERT-EU*. Lai radītu maksimālu potenciālu sinerģijām un mazinātu sarežģītību ES kiberekosistēmā, AICINA Komisiju ņemt vērā Kiberdrošības akta izvērtēšanas rezultātus, kā arī diskusijas par Kiberdrošības plāna izvērtēšanu, lai racionalizētu Komisijas Kibersituāciju un analīzes centra uzdevumus un ar to saistītos *ENISA* uzdevumus. MUDINA Komisiju izvairīties no nevajadzīgas uzdevumu dublēšanās un vienlaikus aizsargāt centrālo lomu, kuru *ENISA* pilda, palīdzot veidot kopīgu situācijas apzināšanos Savienības līmenī dalībvalstu atbalstam, pienācīgi ņemot vērā valstu kompetenci.

16. UZSVER, ka kopīgas situācijas apzināšanās veidošana ir priekšnoteikums savlaicīgai un efektīvai krīzes pārvarēšanai visā Savienībā. UZSVER, ka ES līmenī **reaģēšanā uz liela mēroga kiberdrošības incidentiem** ir iesaistīti dažādi nozīmīgi aktori un ka šādu incidentu gadījumā dalībvalstu efektīvas sadarbības pamatā galvenokārt ir *CSIRT* tīkls un *EU-CyCLONe*. *ENISA* kā *CSIRT* tīkla un *EU-CyCLONe* sekretariātam ir svarīga loma kiberkrīžu pārvaldībā. AICINA Komisiju izmantot Kiberdrošības plāna izvērtēšanu, lai tajā pienācīgi atspoguļotu papildu uzdevumus un pienākumus palīdzēt izstrādāt sadarbīgu reakciju uz liela mēroga pārrobežu kiberdrošības incidentiem vai krīzēm, kā arī lomu, kas *ENISA* noteikta kā *CSIRT* tīkla un *EU-CyCLONe* sekretariātam un ar jaunākajiem kiberdrošības tiesību aktiem.

17. UZSVER, ka ir svarīgi organizēt regulāras **kiberdrošības mācības**, kas ievērojami palielina ES gatavību reaģēt uz incidentiem un krīzēm. ATZĪST, ka *ENISA* ir apkopojusi vērtīgu un plašu pieredzi šajā jomā, sniedzot atbalstu dalībvalstīm. ATZĪST *ENISA* svarīgo lomu kiberdrošības mācību plānošanas, sagatavošanas, izpildes un novērtēšanas posmos un UZSVER, ka tai arī turpmāk vajadzētu būt vienam no galvenajiem aktoriem ES līmenī, paturot prātā, ka šādas mācības būtu jāveic, pamatojoties uz strukturētiem satvariem un kopīgu terminoloģiju. AICINA *ENISA*, *CSIRT* tīklu un *EU-CyCLONe* pēc iespējas efektīvāk izmantot esošās regulārās mācības, lai pārbaudītu un uzlabotu ES satvaru reaģēšanai krīzes situācijās, un nodrošināt gūtās pieredzes maksimālu izmantošanu.

ENISA **SADARBĪBA AR CITIEM AKTORIEM KIBEREKOSISTĒMĀ**

18. ATKĀRTOTI UZSVER, ka **sadarbība starp visiem aktoriem dalībvalstu un Savienības līmenī** ir ļoti svarīga kiberdrošības horizontālā rakstura dēļ, un tādēļ PASVĪTRO, ka vispārējās kibernoturības palielināšanai Eiropas līmenī ir vajadzīgs arī *ENISA* un citu attiecīgo kiberjomas vienību kopīgs darbs.

19. UZSVER, ka *EUIBA* spēja saglabāt kiberdrošību ir svarīga vispārējai ES līmeņa kibernoturībai, kurā nenovērtējama ir *CERT-EU* loma. Šajā sakarā ATZINĪGI VĒRTĒ izveidoto strukturēto sadarbību starp *CERT-EU* un *ENISA* un MUDINA tās turpināt ciešo sadarbību nākotnē.

20. Pateicoties iegūtajai finansiālajai autonomijai, *ECCC* saskaņā ar tā pilnvarām būtiski veicinās spēcīgas Eiropas pētniecības, rūpniecības un tehnoloģiju ekosistēmas izveidi kiberjomā, tostarp darbaspēka attīstībai vajadzīgās prasmes. MUDINA *ENISA* un *ECCC* turpināt ciešo sadarbību, jo īpaši attiecībā uz pētniecības un inovācijas vajadzībām un prioritātēm, kā arī kiberprasmēm, lai palielinātu Savienības kiberdrošības nozares konkurētspēju. AICINA Komisiju izpētīt, kā varētu vēl vairāk optimizēt sinerģijas *ENISA* un *ECCC* darbā un kā labāk racionalizēt darbības saskaņā ar to attiecīgajām pilnvarām.

21. UZSVER, ka informācijas par apdraudējuma ainu regulāra atjaunināšana palīdz labāk noteikt, kādi pasākumi un instrumenti ir vajadzīgi, lai efektīvi apkarotu kibernoziedzību. UZSVER pievienoto vērtību, ko sniedz ES kopīgās kibernovērtēšanas (*J-CAR*) ziņojumi, kuri ir *ENISA*, Eiropola *EC3* un *CERT-EU* kopīgās sadarbības rezultāts un kuri jau ir snieguši vērtīgu ieguldījumu dažādu problēmu risināšanā, tostarp cīņā pret kibernoziedzību. AICINA *ENISA* un Eiropolu turpināt strukturētu sadarbību nākotnē.

22. UZSVER, ka kiberaizsardzība ir svarīgs un pastāvīgi mainīgs elements kibertelpas radīto draudu novēršanā. UZSVER, ka *ENISA* ir jāsadarbojas ar EĀDD un Komisiju gadījumos, kad *ENISA* piedalās atbalstā ES kiberaizsardzības politikas īstenošanai, cieši sadarbojoties ar EAA, *ECCC* un kiberaizsardzības kopienu. UZSVER *ENISA* kā civilas aģentūras lomu. UZSVER, cik svarīgi ir padziļināt un racionalizēt civilmilitāro sadarbību kiberjomā ES, tostarp skaidri sadalīt uzdevumus un pienākumus starp abām kopienām un starp ES un NATO, pilnībā ievērojot iekļaušanas, savstarpības, abpusējas atklātības un pārredzamības principus, kā arī abu organizāciju lēmumu pieņemšanas autonomiju. MUDINA *ENISA* turpināt īstenot darba vienošanos ar NATO Sakaru un informācijas aģentūru.

23. MUDINA ES turpināt popularizēt mūsu kopīgās vērtības un kopīgos centienus globālos forumos, lai nodrošinātu brīvu, globālu, atvērtu un drošu kibertelpu. UZSVER, ka kiberdraudu un incidentu pārrobežu rakstura dēļ ir vajadzīga cieša un efektīva sadarbība ne tikai ES līmenī, bet arī **ar starptautiskām organizācijām un partneriem**. NORĀDA, ka saskaņā ar ES kopējo ārpolitiku un drošības politiku *ENISA* starptautiskajai iesaistei būtu jākoncentrējas uz stratēģiskiem partneriem un ES kandidātvalstīm. UZSVER, ka starptautiskajā iesaistē *ENISA* būtu jārīkojas saskaņā ar savām pilnvarām un attiecīgajiem Kiberdrošības akta noteikumiem. ATZĪST, ka saskaņā ar attiecīgajām procedūrām ir jāprecizē *ENISA* starptautiskā iesaiste, jo īpaši, nodrošinot, ka tās valde tiek pienācīgi un laikus informēta par saistītajām darbībām. MUDINA *ENISA* iesaistīties attiecīgos starptautiskās kiberdrošības sadarbības satvaros, tostarp tādās organizācijās kā NATO un EDSO.

24. ATKĀRTOTI NORĀDA, ka ES un tās dalībvalstis bieži ir uzsvērušas **kiberdrošības prasmju** trūkumus. ATGĀDINA, ka Komisija un *ENISA* ir ieviesušas plašu un visaptverošu satvaru norādījumu sniegšanai visām ieinteresētajām personām, piemēram, Eiropas kiberdrošības prasmju satvaru, paziņojumu par Kiberdrošības prasmju akadēmiju un katru gadu organizēto Eiropas Kiberprasmju konferenci, un MUDINA Komisiju un *ENISA* balstīties uz šīm iniciatīvām, īpaši ņemot vērā notiekošās diskusijas par Eiropas digitālās infrastruktūras konsorciju (*EDIC*). Šajā nolūkā AICINA Komisiju sadarboties ar dalībvalstīm, kuras ir ieinteresētas izveidot *EDIC*. ATZĪST, ka gan *ENISA*, gan *ECCC* ir pilnvarotas veicināt prasmes visā Savienībā. AICINA *ENISA* par prioritāti noteikt atbalstu dalībvalstu centieniem prasmju un izglītības jomā un sabiedrības informētības pastiprināšanu un attiecīgā gadījumā sadarboties ar *ECCC*.

25. ATZĪST, ka *ENISA* pēdējos gados ir izveidojusi **sadarbību ar privāto sektoru**. ATGĀDINA – tā kā privātais sektors nepārtraukti uzrauga kiberdraudu ainu, nozares apkopotā informācija varētu palīdzēt uzlabot kopīgu situācijas apzināšanos. Tādēļ MUDINA *ENISA* ciešā sadarbībā ar dalībvalstīm un ES vienībām stiprināt sadarbību ar privāto sektoru.

26. AICINA Komisiju un *ENISA* apsvērt veidus, kā uzlabot sadarbību starp *ENISA* un Eiropas **standartizācijas** iestādēm. UZSVER, ka *ENISA* ir jāuzlabo savas speciālās zināšanas par Eiropas kiberdrošības standartizāciju, cita starpā sekojot līdzi standartizācijas darbībām un piedaloties tajās.

27. MUDINA Komisiju un *ENISA* izpētīt, kā vēl vairāk optimizēt ES kiberdrošības satvara darbību, ņemot vērā šajos secinājumos sniegtos ieteikumus un priekšlikumus. Pastāvīga sadarbība, prioritāšu noteikšana attiecībā uz uzdevumiem un resursiem, kā arī sarežģītās kibervides vienkāršošana būs būtiski elementi pašreizējo un turpmāko izaicinājumu pārvarēšanai.