Eiropas Savienības
Padome

Briselē, 2018. gada 19. novembrī
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

DARBA REZULTĀTI

Sūtītājs:	Padomes Ģenerālsekretariāts
Datums:	2018. gada 19. novembris
Saņēmējs:	delegācijas
Temats:	ES kiberaizsardzības politikas satvars (2018. gada atjauninājums)

Pielikumā pievienots ES kiberaizsardzības politikas satvars (2018. gada atjauninājums), ko Padome pieņēma 3652. sanāksmē 2018. gada 19. novembrī.

PIELIKUMS

ES KIBERAIZSARDZĪBAS POLITIKAS SATVARS

(2018. GADA ATJAUNINĀJUMS)

Darbības joma un mērķi

Lai reaģētu uz mainīgajiem drošības izaicinājumiem, ES un tās dalībvalstīm ir jāstiprina kibernoturība un jāattīsta spēcīgas kiberdrošības un kiberaizsardzības spējas.

Ar ES kiberaizsardzības politikas satvaru (KPS) atbalsta ES dalībvalstu kiberaizsardzības spēju attīstību, kā arī ES drošības un aizsardzības infrastruktūras kiberaizsardzības stiprināšanu, neskarot dalībvalstu tiesību aktus un ES tiesības, tostarp kiberaizsardzības tvērumu, ja tāds ir noteikts.

Kibertelpa līdztekus zemes, jūras, gaisa un kosmosa jomām ir operāciju piektā joma, un ES misiju un operāciju sekmīga īstenošana arvien vairāk ir atkarīga no nepārtrauktas piekļuves drošai kibertelpai, un tāpēc ir nepieciešamas spēcīgas un noturīgas operatīvās kiberspējas.

Atjauninātā KPS mērķis ir turpināt attīstīt ES kiberaizsardzības politiku, ņemot vērā relevantas norises citos relevantos forumos un politikas jomās un KPS īstenošanu kopš 2014. gada. KPS ir apzinātas kiberaizsardzības prioritārās jomas un precizētas dažādu Eiropas dalībnieku lomas, vienlaikus pilnībā respektējot Savienības dalībnieku un dalībvalstu pienākumus un kompetences, kā arī ES iestāžu sistēmu un tās lēmumu pieņemšanas autonomiju.

Konteksts

Eiropadomes 2013. gada secinājumos par KDAP, kā arī Padomes 2013. gada novembra secinājumos par KDAP tika pausts aicinājums izstrādāt ES kiberaizsardzības politikas satvaru, pamatojoties uz priekšlikumu, ko Augstā pārstāve sagatavojusi sadarbībā ar Eiropas Komisiju un Eiropas Aizsardzības aģentūru (EAA). ES kiberaizsardzības politikas satvaru (KPS) Padome pieņēma 2014. gada 18. novembrī [1], un kopš tā laika KPS īstenošanas gaitā gūtie konkrētie rezultāti ir devuši ieguldījumu, lai būtiski nostiprinātu dalībvalstu kiberaizsardzības spējas. Saistībā ar 2017. gada ziņojumu par ES kiberaizsardzības politikas satvara īstenošanu [2] un ņemot vērā ES iniciatīvas drošības un aizsardzības jomā, jo īpaši Koordinēto ikgadējo pārskatu par aizsardzību (*CARD*), Pastāvīgo strukturēto sadarbību (*PESCO*), Eiropas Aizsardzības fondu (EAF), civilās KDAP paktu, kā arī 2018. gadā notikušo Spēju attīstības plāna (*CDP*) pārskatīšanu un Civilo spēju attīstības plānu (*CCDP*), dalībvalstis aicināja atjaunināt ES kiberaizsardzības politikas satvaru.

Kiberdrošība ir Globālās ES ārpolitikas un drošības politikas stratēģijas prioritāte, un tā ir ES mērķu vērienīguma daļa [3]. Globālajā stratēģijā uzsvērts, ka ir jāstiprina spējas aizsargāt ES un tās pilsoņus un reaģēt uz ārējām krīzēm. Globālajā stratēģijā uzsvērta vajadzība stiprināt ES kā drošības kopienu. Šajā sakarā ar drošības un aizsardzības centieniem būtu arī jāpalielina ES stratēģiskā loma un tās spēja rīkoties autonomi, kad un kur vien nepieciešams un, kad vien iespējams, kopā ar partneriem. Šo mērķu sasniegšanai nepieciešams vairāk sadarboties spēju attīstības jomā, ar ko sekmētu rezultātā izveidoto civilo un militāro spēju efektivitāti un savietojamību.

---

1 Padomes dokuments 15585/14, 18.11.2014.
2 Padomes dokuments 15870/17, 19.12.2017.
3 Padomes secinājumi par ES globālās stratēģijas īstenošanu drošības un aizsardzības jomā, 14.11.2016.

Vienotais priekšlikumu kopums Eiropadomes priekšsēdētāja, Eiropas Komisijas priekšsēdētāja un Ziemeļatlantijas līguma organizācijas ģenerālsekretāra 2016. gada 8. jūlijā parakstītās kopīgās deklarācijas īstenošanai [4] ietver konkrētas darbības, ar kurām paredzēts paplašināt ES un NATO sadarbību kiberdrošības un kiberaizsardzības jomā, tostarp saistībā ar misijām un operācijām, kā arī attiecībā uz kiberaizsardzības spēju attīstību, pētniecību un tehnoloģijām, apmācību, izglītību, mācībām un kiberjomas aspektu iekļaušanu krīžu pārvarēšanā. Šī sadarbība notiek, pilnībā respektējot atklātības, pārredzamības, iekļautības, savstarpības un ES lēmumu pieņemšanas autonomijas principus. 2016. gada februārī parakstītā tehniskā vienošanās starp ES Datorapdraudējumu reaģēšanas vienību (*CERT-EU*) un NATO Datorincidentu reaģēšanas spēju vienību (*NCIRC*) atvieglo tehniskās informācijas apmaiņu, kas ļauj abās organizācijās uzlabot kiberincidentu novēršanu, atklāšanu un reaģēšanu uz tiem.

Būtu jāatgādina, ka vairākas ES politikas sekmē šajā dokumentā izklāstīto kiberaizsardzības politikas mērķu sasniegšanu, un šajā satvarā arī ir ņemts vērā attiecīgais regulējums, politika un tehnoloģiskais atbalsts civilajā sektorā. Piemēram, 2016. gada jūlijā Eiropas Parlaments un Padome pieņēma Tīklu un informācijas drošības direktīvu [5] (*NIS*), kas palielinās ES dalībvalstu vispārējo gatavību vērsties pret kiberdraudiem un pastiprinās ES mēroga sadarbību. Šajā direktīvā ir paredzēti pasākumi ar mērķi Savienībā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību tā, lai uzlabotu iekšējā tirgus darbību. Direktīvas transponēšanas termiņš ir 2018. gada 9. maijs.

---

4 Padomes secinājumi par Eiropadomes priekšsēdētāja, Eiropas Komisijas priekšsēdētāja un Ziemeļatlantijas līguma organizācijas ģenerālsekretāra kopīgās deklarācijas īstenošanu (2016. gada 6. decembris, dok. 15283/16; 2017. gada 5. decembris, dok. 14802/17).

5 Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā, OV L 194, 19.7.2016., 1. lpp.

2017. gada septembra ES kiberdrošības akta priekšlikumā ir ietverts jauns ES kiberdrošības aģentūras (*ENISA*) mandāts un paredzēta ES mēroga sertifikācijas satvara izveide. Tiklīdz sertifikācijas satvars būs ieviests, tam būtu jāatbalsta augsti standarti IKT procesiem, produktiem un pakalpojumiem, tam vajadzētu būt konkurences priekšrocību avotam un būtu jāpalielina patērētāju un pircēju uzticēšanās. Bez tam 2017. gada septembrī Komisija spēra vēl vienu soli, lai ES sagatavotu plašapmēra pārrobežu kiberdrošības incidentiem ("plāns"), un pašlaik tā ar dalībvalstīm un citām iestādēm, aģentūrām un struktūrām strādā pie Eiropas kiberdrošības krīžu sadarbības attīstīšanas, ieviešot visu attiecīgo dalībnieku, procesu un procedūru praktisku īstenojamību un dokumentāciju saistībā ar esošajiem ES krīzes un katastrofu pārvarēšanas mehānismiem, jo īpaši integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem.

Padomes 2016. gada novembra secinājumos par Eiropas kibernoturības stiprināšanu izklāstīts kopīgais mērķis sekmēt Eiropas stratēģisko autonomiju, kā minēts Padomes secinājumos par Globālo Eiropas Savienības ārpolitikas un drošības politikas stratēģiju,– arī kibertelpā. Šo vēstījumu Eiropadome atkārtoti apstiprināja 2018. gada jūnijā un arī uzsvēra vajadzību stiprināt spējas pret kiberdrošības apdraudējumiem, kuru izcelsme ir ārpus ES.

Padome 2017. gadā pieņēma satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopumu") [6]. Tiek sagaidīts, ka minētais satvars sekmēs sadarbību, veicinās draudu mazināšanu un ilgtermiņā ietekmēs potenciālo agresoru uzvedību. Lai novērstu ļaunprātīgas kiberdarbības un reaģētu uz tām, satvarā paredzēts izmantot KDAP pasākumus, tostarp ierobežojošus pasākumus. Ļaunprātīgu kiberdarbību subjekti par savām darbībām ir jāsauc pie atbildības, un ES dalībvalstis tiek mudinātas koordinēti un atbilstoši kiberdiplomātijas instrumentu kopumam turpināt attīstīt spējas reaģēt uz ļaunprātīgām kiberdarbībām. Valstīm nevajadzētu veikt vai apzināti atbalstīt tādas ar informācijas un komunikācijas tehnoloģijām (IKT) saistītas darbības, kas ir pretrunā to pienākumiem saskaņā ar starptautiskajām tiesībām, un tām nevajadzētu apzināti ļaut izmantot savu teritoriju ar IKT lietojumu saistītu starptautisku prettiesisku darbību veikšanai.

Komisija un AP/PV 2017. gada septembrī nāca klajā ar kopīgu paziņojumu [7] par kiberdrošību, kura nolūks ir mazināt riskus, kas izriet no jaunās drošības apdraudējuma ainas. Tajā kiberaizsardzība ietverta kā viena no galvenajām darbības jomām, un KPS ir viens no tās konkrētas īstenošanas pīlāriem [8].

Padomes 2017. gada novembra secinājumos atzīts, ka saikne starp kiberdrošību un aizsardzību kļūst arvien ciešāka, un aicināts pastiprināt sadarbību kiberaizsardzības jomā, tostarp, mudinot izvērst sadarbību starp civilajām un militārajām incidentu reaģēšanas kopienām. Tajos arī ir uzsvērts, ka īpaši nopietns kiberincidents vai krīze varētu būt pietiekams pamatojums tam, lai dalībvalsts iedarbinātu ES solidaritātes klauzulu un/vai savstarpējās palīdzības klauzulu.

---

[6] Padomes secinājumi par satvaru vienotai ES diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām ("kiberdiplomātijas instrumentu kopums"), dok. 9916/17, 2017. gada 7. jūnijs.

[7] Kopīgs paziņojums Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" (2017. gada 13. septembris, JOIN(2017) 450 *final*).

[8] Padomes secinājumi par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" (2017. gada 20. novembris, 14435/17).

2017. gada 11. decembrī tika sākta Pastāvīgā strukturētā sadarbība (*PESCO*). Šo vērienīgo, saistošo un iekļaujošo sadarbības satvaru izveidoja 25 dalībvalstis, un tajā ir iekļauta apņemšanās pastiprināt centienus sadarboties kiberaizsardzības jomā, kā arī citi saistīti *PESCO* projekti. Pirmajā *PESCO* projektu kārtā, kurus dalībvalstis apzināja 2017. gadā, ir iekļauti divi ar kiberaizsardzību saistīti projekti: "Kiberdrošības ātrās reaģēšanas vienības un savstarpēja palīdzība kiberdrošības jomā" un "Kiberdraudu un kiberincidentu reaģēšanas informācijas apmaiņas platforma". Ir plānotas arī turpmākas *PESCO* projektu kārtas. *PESCO* ietvaros paredzēts attīstīt kiberaizsardzības spējas un tādējādi stiprināt iesaistīto dalībvalstu sadarbību un palielināt sadarbspēju.

EAA valdes 2018. gada jūnijā apstiprinātajā ES Spēju attīstības plānā (*CDP*) kiberaizsardzība ir apzināta kā izšķirīgs elements un atzīta vajadzība jebkādā operatīvajā kontekstā izvērst aizsardzības rakstura kiberoperācijas, kuru pamatā ir rafinēta kibertelpas pašreizējās situācijas un prognozētās turpmākās situācijas apzināšanās, tostarp spēja kombinēt lielus datu apjomus un no dažādiem avotiem nākušus izlūkdatus, tādējādi atbalstot lēmumu ātru pieņemšanu un datu vākšanas, analīzes un lēmumu atbalsta procesa pastiprinātu automatizāciju. 2018. gada *CDP* ir identificētas kiberaizsardzības prioritātes šādās jomās: sadarbība un sinerģijas ar attiecīgajiem visas kiberaizsardzības un kiberdrošības jomas dalībniekiem; kiberaizsardzības pētniecības un tehnoloģiju darbības; sistēmu inženierijas satvari kiberoperāciju vajadzībām; izglītība, apmācība, mācības un izvērtēšana (*ETEE*); pievēršanās kiberaizsardzības izaicinājumiem gaisa, kosmosa, jūras un zemes jomās.

Visbeidzot, pēdējo gadu laikā ir izkristalizējusies vajadzība starptautiskajai sabiedrībai novērst konfliktus, sadarboties un stabilizēt kibertelpu. ES ciešā sadarbībā ar citām starptautiskajām organizācijām, jo īpaši ANO, EDSO un *ASEAN* Reģionālo forumu, veicina kibertelpas konfliktu novēršanas, sadarbības un stabilitātes stratēģisko satvaru, kas aptver – i) starptautisko tiesību, jo īpaši ANO Statūtu kopumā, piemērošanu kibertelpā; ii) universālu nesaistošu valsts atbildīgas uzvedības normu, noteikumu un principu respektēšanu; iii) reģionālu uzticības veicināšanas pasākumu (UVP) attīstību un īstenošanu. Arī Kiberaizsardzības politikas satvaram (KPS) būtu jāatbalsta šie centieni.

Prioritātes

Atjauninātajā KPS ir identificētas sešas prioritārās jomas. Primāri šajā politikas satvarā pievēršas kiberaizsardzības spēju attīstīšanai, kā arī ES KDAP sakaru un informācijas tīklu aizsardzībai. Citas prioritārās jomas ir šādas: apmācība un mācības, pētniecība un tehnoloģijas, civilmilitārā sadarbība un starptautiskā sadarbība. Apmācību jomā galvenais uzsvars ir likts uz dalībvalstu kiberaizsardzības apmācības un KDAP komandķēdes kiberapzināšanās apmācības stiprināšanu. Tāpat mācībās kiberdimensijai ir svarīgi pievērst pienācīgu uzmanību, lai, uzlabojot lēmumu pieņemšanas procedūru un informācijas pieejamību, kāpinātu ES spējas KDAP kontekstā reaģēt uz kiberkrīzēm un hibrīdkrīzēm. Kibertelpa ir joma, kas strauji attīstās, un gan civilajā, gan militārajā jomā ir jāatbalsta jauni tehnoloģiski risinājumi. Civilmilitārā sadarbība kiberjomā ir izšķirīga, lai nodrošinātu saskanīgu reaģēšanu uz kiberdraudiem. Visbeidzot, tomēr ne mazāk svarīgi, – pastiprināta sadarbība ar starptautiskajiem partneriem varētu palīdzēt uzlabot kiberdrošību Eiropas Savienībā un plašākā mērogā un sekmētu ES principus un vērtības.

Šajā satvarā ir izklāstīti priekšlikumi un iespējas koordinēt attiecīgo ES iestāžu, struktūru un aģentūru darbību. Tajā arī ir atspoguļota būtiskā loma, kas kiberdrošības un kiberaizsardzības tehnoloģiju attīstībā ir privātajam sektoram.

Turklāt ar KPS atbalsta turpmāku kiberaizsardzības integrāciju Savienības krīzes pārvarēšanas mehānismos, kad, lai risinātu kiberkrīzes sekas, var būt piemērojami ES līguma un Līguma par Eiropas Savienības darbību [9] attiecīgie noteikumi.

1. Atbalsta sniegšana dalībvalstu kiberaizsardzības spēju attīstīšanai

Kiberaizsardzības spēju un tehnoloģiju izstrādē būtu jāpievēršas visiem spēju veidošanas aspektiem, tostarp doktrīnai, vadībai, organizācijai, personālam, apmācībai, nozarei, tehnoloģijām, infrastruktūrai, loģistikai un sadarbspējai. Šajā nolūkā dalībvalstīm būtu jāpastiprina centieni gūt sekmes efektīvu kiberaizsardzības spēju izveidē. EĀDD, Komisijai un EAA būtu jāsadarbojas un jāatbalsta šie centieni.

Ir nepieciešams nepārtraukti veikt vājo vietu novērtēšanu tajās informācijas infrastruktūrās, ar kurām atbalsta KDAP misijas un operācijas, vienlaikus nodrošinot, ka gandrīz reālā laikā var apzināties, cik efektīva ir aizsardzība. No operatīvā viedokļa raugoties, viena no galvenajām kiberaizsardzības darbību jomām, kurai būtu jāpievērš uzmanība, būs uzturēt KDAP sakaru un informācijas tīklu pieejamību, integritāti un konfidencialitāti, ja vien operāciju vai misiju pilnvarojumā nav noteikts citādi. Bez tam EĀDD sadarbībā ar dalībvalstīm kiberspējas vēl vairāk integrēs KDAP misijās un operācijās.

Ļaunprātīgo kiberdarbību subjekti par savām darbībām ir jāsauc pie atbildības. Ir būtiski, lai dalībvalstis ar EĀDD atbalstu stiprinātu savstarpējo sadarbību nolūkā reaģēt uz ļaunprātīgām kiberdarbībām. Kiberdiplomātijas instrumentu kopums ir izstrādāts, lai palīdzētu nodrošināt šādu savstarpēju reaģēšanu. EĀDD un EAA, pamatojoties uz kiberdiplomātijas instrumentu kopumu, rīkos regulāras mācības, kurās dalībvalstis to varēs praktizēt.

[9] LESD 222. pants un LES 42. panta 7. punkts, pienācīgi ņemot vērā LES 17. pantu.

Ņemot vērā to, ka dalībvalstu, kā arī ES tiesību aktos kiberaizsardzības tvērums, ja tas vispār ir noteikts, ir plašs un diversificēts, ir jāattīsta kopēja vienota izpratne par kiberaizsardzības tvērumu.

Tā kā KDAP militārās operācijas balstās uz vadības, kontroles, sakaru un datoru (*C4*) infrastruktūru, ko nodrošina dalībvalstis, tad, plānojot kiberaizsardzības prasības informācijas infrastruktūrām, ir nepieciešama noteikta līmeņa stratēģiskā konverģence.

Balstoties uz EAA kiberaizsardzības projekta grupas darbu, lai attīstītu kiberaizsardzības spējas, EAA un dalībvalstis:

- izmantos *CDP* un citus instrumentus, piemēram, *CARD*, kuri atvieglo un sniedz atbalstu sadarbībai starp dalībvalstīm, lai uzlabotu konverģences līmeni dalībvalstu kiberaizsardzības prasību stratēģiskā līmeņa plānošanā, jo īpaši attiecībā uz pārraudzību, situācijas apzināšanos, novēršanu, atklāšanu un aizsardzību, informācijas apmaiņu, kriminālistikas un ļaunprogrammatūras analīzes spēju, gūto pieredzi, bojājumu ierobežošanu, dinamiskām atkopes spējām, dalītu datu glabāšanu un datu rezerves kopijām;
- atbalstīs pašreizējos un turpmākos ar kiberaizsardzību saistītos militāro operāciju resursu apvienošanas un koplietošanas projektus (piemēram, tādās jomās kā kriminālistika, sadarbspējas attīstīšana, standartu noteikšana);
- izmantojot pašreizējo ES mērogā gūto pieredzi, izstrādās mērķu un prasību standarta kopumu, kurā būs noteikts minimālais kiberdrošības un uzticības līmenis, kas jāpanāk dalībvalstīm.

EĀDD un dalībvalstis:

- atvieglos apmaiņu starp dalībvalstīm attiecībā uz valstu kiberaizsardzības doktrīnām, kā arī uz kiberaizsardzību vērstām personāla rekrutēšanas, saglabāšanas un rezervistu programmām.

EAA:

- izpētīs dažādos kiberaizsardzības militāro prasību tvērumus dalībvalstu tiesību aktos un paraugprakses. Galvenais šīs izpētes mērķis būs attīstīt kiberaizsardzības korporatīvo arhitektūru, tajā iekļaujot šajā jomā dalībvalstu lietoto tvērumu, funkcijas un prasības atbilstoši valstu un ES tiesību aktiem.

Dalībvalstis brīvprātīgi:

- uzlabos sadarbību starp to datorapdraudējumu reaģēšanas vienībām (*CERT*), lai uzlabotu incidentu novēršanu un risināšanu;
- izmantos *PESCO*, lai turpinātu pastiprināt sadarbību kiberaizsardzības jomā, tostarp attiecībā uz jauniem projektiem;
- izmantos Eiropas Aizsardzības fondu, lai kopīgi attīstītu kiberaizsardzības spējas;
- veidos kopēju izpratni par savstarpējās palīdzības klauzulas piemērošanu kiberjomā, vienlaikus saglabājot tās elastību;
- izstrādās kiberaizsardzības pamatprasības informācijas infrastruktūrai;
- Ņemot vērā, ka kiberaizsardzības spēju uzlabojumi zināmā mērā ir atkarīgi no civilajām tīklu un informācijas drošības (TID) ekspertu zināšanām, izmantos ekspertu zināšanas, ko piedāvā *ENISA*, TID sadarbības grupā sanākušās dalībvalstu iestādes un citas iespējamas struktūras ES līmenī, kurām ir zinātība civilās kiberdrošības jomā.

Dalībvalstis, EĀDD/ES Militārais štābs, EDAK un EAA:

- apsvērs kiberaizsardzības apmācības izstrādāšanu, gatavojoties ES kaujas grupu sertifikācijai.

Komisija sadarbībā ar dalībvalstīm:

- apsvērs kiberaizsardzību Eiropas aizsardzības rūpniecības attīstības programmas un Eiropas Aizsardzības fonda programmās.

2. ES struktūru izmantoto KDAP sakaru un informācijas sistēmu aizsardzības uzlabošana

Neskarot nozīmi, kāda ir ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienībai (*CERT-EU*) – galvenajai ES struktūrai, kas koordinē reaģēšanu uz kiberincidentiem attiecībā uz visām Savienības iestādēm, struktūrām un aģentūrām, – un saskaņā ar relevantajiem noteikumiem, kas attiecas uz Savienības budžetu, EĀDD izstrādās adekvātu un autonomu izpratni par drošības un tīklu aizsardzības jautājumiem un attīstīs pati savas IT drošības spējas. Tās mērķis būs uzlabot EĀDD KDAP tīklu noturību, koncentrējoties uz novēršanu, atklāšanu, reaģēšanu uz incidentiem, situācijas apzināšanos, informācijas apmaiņu un agrīnas brīdināšanas mehānismiem.

EĀDD sakaru un informācijas sistēmu aizsardzību un informācijas tehnoloģiju (IT) drošības spēju attīstīšanu vada EĀDD Budžeta un administrācijas ģenerāldirektorāts (BA). Papildu īpašos resursus un atbalstu sniegs arī Eiropas Savienības Militārais štābs (ESMŠ), Krīžu pārvarēšanas un plānošanas direktorāts (*CMPD*) un Civilās plānošanas un īstenošanas centrs (*CPĪC*). Šīs IT drošības spējas attieksies gan uz klasificētām, gan neklasificētām sistēmām un būs pašreizējo operatīvo vienību integrāla daļa.

Ir nepieciešams racionalizēt arī informācijas sistēmu drošības noteikumus, kurus nodrošinājuši dažādi ES institucionālie dalībnieki, vadot KDAP misijas un operācijas. Šajā sakarā būtu jāapsver vienotas komandķēdes izveide ar mērķi uzlabot saistībā ar KDAP izmantoto tīklu noturību.

Lai nodrošinātu labāku koordināciju un pastiprinātu KDAP sakaru un informācijas sistēmu un tīklu aizsardzību un noturību, 2017. gadā EĀDD ģenerālsekretāra pakļautībā tika izveidota EĀDD Kiberpārvaldības padome.

EĀDD/BA:

- pastiprinās EĀDD IT drošības spējas, balstoties uz esošajām tehniskajām spējām un procedūrām un koncentrējoties uz novēršanu, atklāšanu, reaģēšanu uz incidentiem, situācijas apzināšanos, informācijas apmaiņu un agrīnas brīdināšanas mehānismu. Vēl vairāk tiks uzlabota sadarbības stratēģija ar *CERT-EU* un esošajām ES kiberdrošības spējām.

EĀDD/BA kopā ar ESMŠ, MPĪC, *CMPD* un CPĪC:

- lai panāktu konverģenci attiecībā uz noteikumiem, politikām un organizāciju, izstrādās saskaņotu IT drošības politiku un pamatnostādnes, ņemot vērā arī kiberaizsardzības tehniskās prasības saistībā ar KDAP attiecībā uz struktūrām, misijām un operācijām, paturot prātā esošās sadarbības sistēmas un politiku Eiropas Savienībā.

EĀDD / vienotā izlūkdatu analīzes procedūra (*SIAC*):

- balstoties uz esošajām struktūrām, nostiprinās kiberdraudu novērtēšanas un izlūkošanas spējas, lai identificētu jaunus kiberriskus un sniegtu regulārus riska novērtējumus, kas balstīti uz stratēģisko draudu novērtējumu un gandrīz reāllaikā gūtu informāciju par incidentiem, ko koordinē attiecīgās ES struktūras un ko dara pieejamus dažādos klasifikācijas līmeņos.

EĀDD/*SIAC* un *CERT-EU*:

- veicinās reāllaika kiberdraudu informācijas apmaiņu starp dalībvalstīm un attiecīgajām ES struktūrām. Šajā sakarībā starp attiecīgajām valsts un Eiropas iestādēm attīstīs informācijas apmaiņas mehānismus un uzticības veidošanas pasākumus, izmantojot brīvprātīgu pieeju, kas balstās uz esošo sadarbību.

EĀDD/ESMŠ un MPĪC:

- vēl vairāk attīstīs un kiberaizsardzības koncepciju KDAP militārajām misijām un operācijām un integrēs to stratēģiskajā plānošanā;
- sadarbībā ar operāciju štābu izstrādās vispārēju operatīvā līmeņa standarta darbības procedūru kiberjomai.

EĀDD/CPĪC un *CMPD*:

- vēl vairāk attīstīs kiberaizsardzības koncepciju KDAP civilajām misijām un integrēs to stratēģiskajā plānošanā;
- stiprinās KDAP civilo misiju kiberaizsardzības spējas, pamatojoties uz esošo infrastruktūru un veicinot to tehnoloģiju standartizāciju un harmonizāciju, ko izmanto KDAP misijās un operācijās, attiecīgā gadījumā izmantojot *CERT-EU*, *ENISA* un EAA speciālo zināšanu priekšrocības;
- civilās KDAP stiprināšanas procesā vēl vairāk izskatīs iespējas civilajām KDAP misijām atbalstīt uzņēmējvalstis attiecībā uz kiberdrošību.

EĀDD:

- vēl vairāk attīstīs kopējās prasības attiecībā uz KDAP militārajām un civilajām misijām un operācijām;
- izmantojot pašreizējo ES mērogā gūto pieredzi, uzlabos kiberaizsardzības koordināciju, lai īstenotu mērķus, kas saistīti ar to tīklu aizsardzību, kurus izmanto ES iestāžu dalībnieki, kas atbalsta KDAP;
- apspriežoties ar dalībvalstīm un citām ES iestādēm, regulāri pārskatīs prasības attiecībā uz resursiem un citus relevantus politikas lēmumus, kas balstīti uz mainīgo draudu vidi.

3. Civilmilitārās sadarbības veicināšana

Kibertelpa ir joma, kas strauji attīstās, un tāpēc tehnoloģiju attīstība ir jāstiprina ar drošības sistēmām gan civilajā, gan militārajā jomā. Gadījumos, kad līdzīga tehnoloģiju attīstība rada risinājumus civilam un militāram izmantojumam, cik vien iespējams, būtu jāparedz koordinācija starp civilo un militāro jomu. Citos gadījumos militārās spējas un ieroču sistēmas ir tik specifiskas, ka nepastāv iespēja koplietojumam ar civilajām tehnoloģijām. Neskarot dalībvalstu iekšējo organizāciju un tiesību aktus, civilmilitāro sadarbību kiberjomā var apsvērt *inter alia* apmaiņai ar paraugpraksi, informācijas apmaiņai un agrīnas brīdināšanas mehānismiem, reaģēšanas uz incidentiem riska novērtējumiem un informētības uzlabošanai, un apmācībai un mācībām.

Civilās kiberdrošības uzlabošana ir būtisks faktors, kas veicina tīklu un informācijas drošības kopējo izturētspēju. Direktīva par tīklu un informācijas drošību palielina gatavību valstu līmenī un stiprina gan stratēģisko, gan operatīvo sadarbību starp dalībvalstīm Savienības līmenī. Šajā sadarbībā ir iesaistītas gan valstu iestādes, kuras pārrauga kiberdrošības politiku, gan valstu *CERT* un *CERT-EU*. Būtu jāpastiprina sadarbība starp civilajām un militārajām *CERT*, pienācīgi ņemot vērā šīs norises. Jaunā Eiropas kiberdrošības akta mērķis ir uzlabot Eiropas noturību pret kiberuzbrukumiem un paredzēt kiberdrošības sertifikācijas satvaru produktiem un pakalpojumiem, tādējādi palielinot uzticēšanos civilajai digitālajai sfērai.

EAA, Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*), Eiropas Kibernoziedzības centrs (*EC3*) un *CERT-EU* kopā ar citām attiecīgajām ES struktūrām un aģentūrām to attiecīgā pilnvarojuma ietvaros un nedublējot dalībvalstu kompetenci, kā arī dalībvalstis tiek aicinātas vēl vairāk uzlabot savu sadarbību šādās jomās:

- izstrādāt kopējus kiberdrošības un aizsardzības kompetenču profilus, pamatojoties uz starptautisko paraugpraksi un ES iestāžu, struktūru un aģentūru izmantoto sertifikāciju, ņemot vērā arī privātā sektora sertifikācijas standartus;
- palīdzēt vēl vairāk attīstīt un pielāgot publiskā sektora kiberdrošības un aizsardzības organizatoriskos un tehniskos standartus izmantošanai aizsardzības un drošības jomā. Vajadzības gadījumā par pamatu izmantot *ENISA* un EAA notiekošo darbu;
- izveidot un tālāk attīstīt darba mehānismus un režīmus paraugprakses apmaiņai, jo īpaši attiecībā uz izglītību, apmācību un mācībām, kā arī uz pētniecību un tehnoloģiju un citām jomām, kas nodrošina civilmilitāras sinerģijas;
- kibernoziegumu novēršanā, izmeklēšanas un kriminālistikas spējās un to plašākā izmantošanā kiberaizsardzības spēju izstrādē smelties no esošās ES pieredzes.

Dalībvalstis brīvprātīgi:

- stiprinās sadarbību starp civilajām un militārajām *CERT* starp dalībvalstīm.

EĀDD, Komisija un dalībvalstis:

- iekļaus kiberaizsardzību ES krīzes un katastrofu pārvarēšanas procedūrās (izmantojot plāna procesu).

4. Pētniecība un tehnoloģijas

Gan civiliem, gan aizsardzības nolūkiem paredzētas infrastruktūras un informācijas un komunikācijas tehnoloģiju (IKT) operatori saskaras ar līdzīgiem kiberdrošības pārbaudījumiem; tas izriet no kopējām tehnoloģijas un operatīvo spēju prasībām. Sagaidāms, ka kopējas pētniecības un tehnoloģiju vajadzības un kopējas sistēmu prasības uzlabos sistēmu sadarbspēju ilgtermiņā, kā arī samazinās risinājumu izstrādes izmaksas. Apjomradītu ietaupījumu sasniegšana ir nepieciešama, lai vērstos pret arvien pieaugošo draudu un ievainojamības gadījumu skaitu. Tam savukārt vajadzētu veicināt konkurētspējīgas kiberaizsardzības nozares saglabāšanu un izaugsmi Eiropā.

Kiberaizsardzības spēju attīstībai ir būtisks pētniecības un tehnoloģiju aspekts. Saistībā ar Kiberaizsardzības pētniecības programmu (*CDRA*) EAA ir nodrošinājusi stabilu pamatu tam, ka turpmākam pētniecības un tehnoloģiju izdevumu finansējumam starpvaldību satvarā tiek piešķirta prioritāte. Stratēģiskajā pētniecības programmā, ko pēc tam izstrādāja attiecīgā EAA *ad hoc* darba grupa, paredzēta pamatota prioritāšu piešķiršana attiecībā uz kiberjomas tehnoloģijām, kas nepieciešamas militārām vajadzībām, vienlaikus apzinot iespējas divējāda izmantojuma centieniem un investīcijām valstu, multinacionālā vai ES finansētā kontekstā.

Lai mazinātu draudus un ievainojamību, ir būtiski Eiropā attīstīt tehniskās spējas. Galvenais ar kiberaizsardzību saistītas tehnoloģijas un inovācijas virzītājs joprojām būs industrija. Dažas no jomām, kurām ir jāpievēršas, ietver kriptogrāfiju, drošas iegultās sistēmas, ļaunprogrammatūras atklāšanu, simulācijas un vizualizācijas paņēmienus, tīkla un sakaru sistēmu aizsardzību un identifikācijas un autentifikācijas tehnoloģijas. Svarīgi ir arī veicināt konkurētspējīgu Eiropas industriālo kiberdrošības apgādes ķēdi, atbalstot iesaisti ar maziem un vidējiem uzņēmumiem (MVU).

Tas, vai Eiropa varēs sacensties ar starptautiskiem konkurentiem kibertehnoloģijas spēju ziņā, ir atkarīgs arī no mūsu spējas veicināt revolucionāru inovāciju, izmantojot gan valsts, gan ES instrumentus, piemēram, Eiropas Inovācijas padomi.

Lai sekmētu civilmilitāru sadarbību kiberaizsardzības spēju veidošanā, stiprinātu Eiropas aizsardzības tehnoloģisko un rūpniecisko bāzi [10] un vairotu ES stratēģisko autonomiju arī kibertelpā, kad un ja tas nepieciešams un, kad vien iespējams, ar partneriem,

EAA, Komisija un dalībvalstis:

- tieksies rast sinerģijas starp militārās nozares pētniecības un tehnoloģiju centieniem un civilajām pētniecības un izstrādes programmām, jo īpaši tādām, kas attiecas uz revolucionāru inovāciju, un, īstenojot sagatavošanas darbības attiecībā uz pētniecību, ņems vērā kiberdrošības un aizsardzības aspektu;
- dalīsies ar kiberdrošības pētniecības programmām (piemēram, Eiropas Aizsardzības aģentūras Stratēģisko pētniecības programmu attiecībā uz kiberdrošību), kā arī no tām izrietošajiem ceļvežiem un darbībām; šajā nolūkā, cieši sadarbojoties ar Komisiju un dalībvalstīm, tiks izstrādāta starpnozaru kiberaizsardzības pētniecības programma;
- palīdzēs uzlabot kiberdrošības un kiberaizsardzības aspektu integrēšanu programmās, kurām ir divējāda lietojuma drošības un aizsardzības dimensija, piemēram, Eiropas vienotās gaisa telpas gaisa satiksmes pārvaldības (*ATM*) pētniecības programmā (*SESAR*).

[10] Paziņojums "Ceļā uz konkurētspējīgāku un efektīvāku aizsardzības un drošības nozari", COM(2013) 542.

Komisija:

- apsvērs iespēju izveidot Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru ar valstu koordinācijas centru tīklu, lai atbalstītu kiberdrošības tehnoloģiskās un industriālās spējas un palielinātu Savienības kiberdrošības industrijas konkurētspēju, nodrošinot papildināmību un izvairoties no dublēšanās kiberdrošības kompetenču centru tīklā un ar citām ES aģentūrām. Centram *inter alia* būtu jāuzlabo sadarbība starp civilām un aizsardzības tehnoloģijām un pielietojumiem, cieši un pilnībā papildinoši sadarbojoties ar Eiropas Aizsardzības aģentūru kiberaizsardzības jomā;
- atbalstīs tādu industriālo ekosistēmu un inovācijas kopu attīstību, kuras aptver visu vērtības veidošanas ķēdi drošības jomā, izmantojot akadēmiskās zināšanas, MVU inovāciju un rūpniecisko ražošanu.

Komisija sadarbībā ar dalībvalstīm:

- apsvērs kiberaizsardzības jautājumus uzaicinājumos iesniegt priekšlikumus par sagatavošanas darbībām attiecībā uz pētniecību aizsardzības jomā;
- apsvērs kiberaizsardzību jautājumos, kas saistīti ar Eiropas Aizsardzības fonda uzaicinājumiem iesniegt priekšlikumus;
- atbalstīs ES politikas saskaņotību ar mērķi nodrošināt, lai ES kiberaizsardzības politikas un tehniskajiem aspektiem arī turpmāk būtu prioritāte tehnoloģiju inovācijā un lai tie būtu saskaņoti visā ES (kiberdraudu analīzes un izvērtēšanas spējas, integrētās drošības iniciatīvas, atkarības pārvaldība attiecībā uz piekļuvi tehnoloģijām u. c.).

5. Uzlabot izglītības, apmācības un mācību iespējas

Lai uzlabotu gatavību kiberdraudu novēršanai un attīstītu kopēju kiberaizsardzības kultūru visā ES, kas dotu labumu arī ES misijām un operācijām, ir jāuzlabo un jāpaplašina kiberaizsardzības apmācības iespējas. Ir ļoti svarīgi, lai izglītībai un apmācībai paredzētie budžeti tiktu izmantoti lietderīgi, vienlaikus nodrošinot vislabāko iespējamo kvalitāti. Kiberaizsardzības izglītības un apmācības resursu apvienošana un koplietošana Eiropas mērogā būs ļoti svarīga.

Eiropas Drošības un aizsardzības koledža (EDAK), EĀDD, EAA, Komisija un dalībvalstis:

- pamatojoties uz EAA kiberaizsardzības apmācības vajadzību analīzi un pieredzi, kas gūta kiberdrošības apmācībā saistībā ar EDAK, izveidos KDAP apmācību un izglītību dažādām mērķauditorijām, tostarp EĀDD, personālam no KDAP misijām un operācijām un dalībvalstu amatpersonām; tajā būtu jāpievēršas arī jautājumiem par kvalificēta personāla saglabāšanu īstermiņā, vidējā termiņā un ilgtermiņā;
- attiecībā uz apmācības standartiem un sertifikāciju ierosinās izveidot kiberaizsardzības jautājumu dialogu ar dalībvalstīm, ES iestādēm, trešām valstīm un citām starptautiskām organizācijām, kā arī ar privāto sektoru;
- sadarbosies ar Eiropas privātā sektora apmācības nodrošinātājiem, kā arī ar akadēmiskām iestādēm, lai uzlabotu KDAP misijās un operācijās iesaistītā personāla kompetences un prasmes.

EDAK:

- vēl vairāk attīstīs EDAK izveidoto kiberjomas izglītības, apmācības, izvērtēšanas un mācību platformu (kiberjomas *ETEE* platforma);
- radīs sinerģijas ar citu ieinteresēto personu – piemēram, *ENISA*, Eiropola, Eiropas Policijas akadēmijas (*CEPOL*) un NATO Kopējā kiberaizsardzības izcilības centra – apmācības programmām;
- izpētīs iespēju veidot kopējas EDAK un NATO kiberaizsardzības apmācības programmas, kas būtu pieejamas visām ES dalībvalstīm, ar mērķi veicināt kopīgu kiberaizsardzības kultūru.

Komisija:

- izvērtēs variantus, kā paplašināt apmācības un izglītības iespējas dalībvalstīs, kas identificētas kiberjomas *ETEE* platformā.

EAA:

- sadarbībā ar EDAK izstrādās papildu EAA kursus, lai izpildītu dalībvalstu prasības kiberaizardzības izglītības, apmācības un mācību jomā;
- atbalstīs kiberjomas *ETEE* platformu, *inter alia* pakāpeniski integrējot kiberjomas izglītības, apmācības, izvērtēšanas un mācību moduļus, kas izstrādāti EAA satvarā.

EĀDD un dalībvalstis:

- ievēros jau izveidotos apmācības programmu EDAK sertifikācijas mehānismus, cieši sadarbojoties ar attiecīgajiem ES iestāžu, struktūru un aģentūru dienestiem un pamatojoties uz pastāvošajiem standartiem un zināšanām; apsvērs iespēju izveidot konkrēti ar kiberdrošību saistītus moduļus militārās jomas "*Erasmus*" iniciatīvas ietvaros.

Kiberaizsardzības mācību iespējas militāriem un civiliem KDAP dalībniekiem ir jāizlabo. Kopīgas mācības ir instruments, lai attīstītu kopējas zināšanas un izpratni par kiberaizsardzību. Tas valstu spēkiem dos iespēju uzlabot savu gatavību darboties daudznacionālā vidē. Kopīgu kiberaizsardzības mācību rīkošana arī sekmēs sadarbspēju un uzticību.

EĀDD, EAA, *CERT-EU* un dalībvalstis koncentrēsies uz kiberaizsardzības elementu veicināšanu KDAP un citās mācībās:

- kiberaizsardzības aspektu integrēs pastāvošajos mācību scenārijos, kas paredzēti *MILEX* un *MULTILAYER*;
- regulāri organizēs tādas stratēģiskas/politiskas mācības kā *CYBRID 2017*, koordinējot tās ar ES vadītajām paralēlajām un koordinētajām mācībām (*PACE*), un tādas tehniski operatīvās mācības kā *DEFNET*;
- attiecīgā gadījumā izstrādās īpašas ES KDAP kiberaizsardzības mācības un izpētīs iespējamu koordināciju ar Eiropas mēroga kiberjomas mācībām, piemēram, *CyberEurope*, ko organizē *ENISA*;
- turpinās piedalīties citās daudznacionālās kiberaizsardzības mācībās, piemēram, *Locked Shields*;
- saskaņā ar ES mācību politikas satvaru uz mācībām aicinās attiecīgus starptautiskos partnerus, piemēram, NATO;
- organizēs regulāras mācības, pamatojoties uz kiberdiplomātijas instrumentu kopumu, kurās ES dalībvalstis var trenēties reaģēt uz ļaunprātīgām kiberdarbībām.

6. Sadarbības uzlabošana ar attiecīgajiem starptautiskajiem partneriem

Saistībā ar starptautisko sadarbību ir jānodrošina dialogs ar starptautiskajiem partneriem, sevišķi NATO un citām starptautiskām organizācijām, lai veicinātu efektīvu kiberaizsardzības spēju attīstību. Lai virzītu uz priekšu stratēģisku satvaru konfliktu novēršanai, sadarbībai un stabilitātei kibertelpā, būtu jātiecas panākt ciešāku iesaisti ar darbu, kas tiek veikts Eiropas Drošības un sadarbības organizācijā (EDSO) un Apvienoto Nāciju Organizācijā (ANO).

Eiropas Savienībā ir politiska griba vēl vairāk sadarboties ar NATO attiecībā uz kiberaizsardzību, veidojot spēcīgas un noturīgas kiberaizsardzības spējas, kā prasīts kopīgajā deklarācijā, ko 2016. gada 8. jūlijā Varšavā parakstīja Eiropadomes priekšsēdētājs, Eiropas Komisijas priekšsēdētājs un Ziemeļatlantijas līguma organizācijas ģenerālsekretārs. Regulāras konsultācijas pušu personāla līmenī, savstarpēji informēšanas pasākumi, kā arī iespējamas Politisku un militāru jautājumu grupas un attiecīgo NATO komiteju tikšanās atbilstīgi minētajam satvaram palīdzēs izvairīties no nevajadzīgas dublēšanās un nodrošinās centienu saskaņotību un papildināmību.

EĀDD un EAA kopā ar dalībvalstīm turpinās attīstīt ES un NATO sadarbību kiberaizsardzības jomā, pienācīgi ņemot vērā attiecīgo organizāciju institucionālo sistēmu un lēmumu pieņemšanas autonomiju:

- palielinās intensitāti esošajās darbībās, kas saistītas ar Eiropadomes priekšsēdētāja, Eiropas Komisijas priekšsēdētāja un Ziemeļatlantijas līguma organizācijas ģenerālsekretāra kopīgās deklarācijas īstenošanu;
- apmainīsies ar paraugpraksi krīžu pārvarēšanā, kā arī attiecībā uz militārajām un civilajām misijām un operācijām kiberaizsardzības jomā;
- strādās pie tā, lai kiberaizsardzības spēju prasību izstrādē rezultāti būtu saskaņoti jomās, kur tās pārklājas, it īpaši attiecībā uz ilgtermiņa kiberaizsardzības spēju attīstību;
- plašāk izmantos EAA sadarbības satvaru ar NATO Kopējo kiberaizsardzības izcilības centru kā sākotnēju platformu ciešākai sadarbībai daudznacionālos kiberaizsardzības projektos, pamatojoties uz attiecīgiem izvērtējumiem.

EDAK, EĀDD un EAA:

- stiprinās sadarbību attiecībā uz kiberaizsardzības apmācības un izglītības, kā arī mācību koncepcijām;
- nodrošinās savstarpīgu personāla dalību mācībās atbilstoši saskaņotajam satvaram.

***CERT-EU*:**

- vēl vairāk izmantos tehnisko vienošanos starp *CERT-EU* un *NCIRC* (NATO Datorincidentu reaģēšanas spējas), lai uzlabotu situācijas apzināšanos, informācijas apmaiņu, agrīnas brīdināšanas mehānismus un paredzētu draudus, kas varētu skart abas organizācijas.

Attiecībā uz citām starptautiskām organizācijām un attiecīgajiem ES starptautiskajiem partneriem EĀDD un dalībvalstis attiecīgos gadījumos:

- sekos stratēģiskajām norisēm un ar starptautiskiem partneriem (starptautiskām organizācijām un trešām valstīm) apspriedīsies par kiberaizsardzības jautājumiem;
- izpētīs iespējas sadarboties kiberaizsardzības jautājumos, cita starpā ar trešām valstīm, kas piedalās KDAP misijās un operācijās;
- attiecīgajās starptautiskajās organizācijās, un jo īpaši ANO, EDSO un *ASEAN* Reģionālajā forumā, sekmēs to, ka kibertelpā tiek piemērotas esošās starptautiskās tiesības, jo īpaši ANO Statūti pilnā apmērā, un ka tiek izstrādātas un īstenotas vispārējas nesaistošas normas attiecībā uz valstu atbildīgu rīcību, kā arī īstenoti reģionāli uzticības veicināšanas pasākumi, lai vairotu pārredzamību un mazinātu pārpratumu risku valstu rīcībā.

Komisija un EĀDD:

- attiecīgos gadījumos atbalstīs ES partneru kiberspēju veidošanu, izmantojot grozīto Stabilitātes un miera veicināšanas instrumentu (*IcSP*).

Turpmāki pasākumi

Lai izvērtētu Kiberaizsardzības politikas satvara īstenošanu (un šā satvara īstenošanas koordināciju veic EĀDD), EĀDD/EAA/Komisijai būtu jāsniedz ikgadējs progresa ziņojums par sešām iepriekš aprakstītajām jomām un ar to jāiepazīstina Politisku un militāru jautājumu grupa, piedaloties Kiberjautājumu horizontālās darba grupas locekļiem, kā arī Politikas un drošības komiteja. Reizi sešos mēnešos tiks sniegts arī mutisks ziņojums.

Ir būtiski, lai jaunas kiberaizsardzības prasības tiktu identificētas, tiklīdz parādās jauni kiberdraudi, un tad tās tiktu iekļautas Kiberaizsardzības politikas satvarā. Nākamā KPS pārskatīšana būtu jāiesniedz ne vēlāk kā 2022. gada vidū, cieši apspriežoties ar dalībvalstīm.