EIROPAS
KOMISIJA

Briselē, 24.7.2019.
COM(2019) 353 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, EIROPADOMEI UN PADOMEI

Deviņpadsmitais progresa ziņojums virzībā uz efektīvu un patiesu drošības savienību

I. IEVADS

Šis ir deviņpadsmitais ziņojums par turpmāko progresu, kas gūts efektīvas un patiesas drošības savienības izveidē, un tajā ir aplūkotas norises, kuras atbilst diviem galvenajiem pīlāriem, proti, proti, cīņai pret terorismu un organizēto noziedzību un līdzekļiem, kas tos atbalsta, un mūsu aizsardzības pasākumu stiprināšanai un noturības veidošanai pret šiem draudiem.

Eiropas iedzīvotāji ir tiesīgi sagaidīt, ka Savienība gādā par viņu drošību. Ž. K. Junkera vadītā Komisija jau no pirmās dienas drošību ir izvirzījusi par vienu no galvenajām prioritātēm. Eiropadomes jaunajā stratēģiskajā programmā 2019.–2024. gadam mērķis "aizsargāt pilsoņus un brīvības" ir minēts pirmajā vietā starp četrām Savienības galvenajām prioritātēm[1]. Eiropadome arī paziņoja, ka tā pilnveidos un stiprinās Savienības centienus cīņā pret terorismu un pārrobežu noziedzību, tostarp uzlabojot sadarbību un informācijas apmaiņu un turpinot izstrādāt kopīgus instrumentus.

Pateicoties ciešai sadarbībai starp Eiropas Parlamentu, Padomi un Komisiju, ES ir daudz paveikusi kopīgajā darbā virzībā uz efektīvu un patiesu drošības savienību, pieņemot vairākas prioritāras likumdošanas iniciatīvas un īstenojot visdažādākos neleģislatīvos pasākumus, lai atbalstītu dalībvalstis un uzlabotu drošību visiem iedzīvotājiem[2]. Savienība ir izlēmīgi rīkojusies, lai slēgtu telpu, kurā darbojas teroristi un noziedznieki, liedzot teroristiem līdzekļus uzbrukumu veikšanai, aizliedzot iegādāties un izmantot konkrētus šaujamieročus un sprāgstvielas un ierobežojot piekļuvi finansējumam. ES ir arī pastiprinājusi informācijas apmaiņu starp dalībvalstīm un novērsusi informācijas nepilnības un neredzamās zonas, vienlaikus apkarojot radikalizāciju, aizsargājot Eiropas iedzīvotājus tiešsaistē, novēršot kiberdraudus un kiberiespējotus draudus, pastiprinot Savienības ārējo robežu pārvaldību un stiprinot starptautisko sadarbību drošības jomā.

Tajā pašā laikā drošības savienībā vēl joprojām ir vairākas prioritāras iniciatīvas, kuras abi likumdevēji vēl nav pieņēmuši. Pēc tam, kad 2019. gada 2. jūlijā darbu sāka Eiropas Parlamenta 9. sasaukums, šajā ziņojumā:

- izklāstīts, kādos gadījumos abiem likumdevējiem ir jārīkojas, lai novērstu tūlītēju apdraudējumu. Īpaši steidzami jārīkojas, lai **apkarotu teroristu propagandu un radikalizāciju tiešsaistē**;
- izklāstītas nepabeigtās prioritārās iniciatīvas drošības savienībā, kurām ir vajadzīga abu likumdevēju turpmāka rīcība, lai uzlabotu **kiberdrošību** un atvieglotu piekļuvi **elektroniskiem pierādījumiem**, un pabeigtu darbu pie spēcīgākām un viedākām drošības, robežu un migrācijas pārvaldības informācijas sistēmām;
- atjaunināta informācija par kopīgo un steidzamo darbu, kas tika uzsākts 2019. gada martā, lai novērtētu un stiprinātu **5G tīklu drošību**, pamatojoties uz valsts riska novērtējumiem, ko dalībvalstis iesniedza līdz 2019. gada 15. jūlijā;
- risināts jautājumu kopums, ko veido četri ziņojumi saistībā ar **nelikumīgi iegūtu līdzekļu legalizācijas novēršanu** un ko Komisija pieņēma 2019. gada 24. jūlijā, kuros analizēti pašreizējie riski un neaizsargātība nelikumīgi iegūtu līdzekļu legalizācijas jomā, kā arī novērtēts, kā attiecīgais ES tiesiskais regulējums tiek piemērots privātajā un publiskajā sektorā;
- sniegta jaunākā informācija par progresu, kas kopš 2019. gada marta[3] panākts tiesību aktu īstenošanā drošības savienības ietvaros, ņemot vērā to, ka informācijas sistēmu sadarbspēja ir

---

1 https://www.consilium.europa.eu/media/39931/a-new-strategic-agenda-2019-2024-lv.pdf

2 Pārskata iegūšanai skatīt faktu lapu "Drošības savienība: Eiropa, kas aizsargā" (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) un Astoņpadsmito progresa ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2019) 145 final (20.3.2019.)).

3 Sk. Astoņpadsmito progresa ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2019) 145 final (20.3.2019.)).

viena no galvenajām prioritātēm ātrai un pilnīgai īstenošanai dalībvalstīs;

- aplūkots pašreizējais darbs, ko veic, lai nepieļautu dezinformāciju un aizsargātu vēlēšanas pret kiberiespējotiem draudiem, kā arī centieni uzlabot sagatavotību un aizsardzību pret drošības apdraudējumiem un sadarbība ar starptautiskajiem partneriem drošības jautājumos.

II. LIKUMDOŠANAS PRIORITĀŠU ĪSTENOŠANA

1. Radikalizācijas novēršana tiešsaistē un kopienās

Radikalizācijas novēršana ir ES uzmanības centrā, reaģējot uz terorismu gan tiešsaistē, gan mūsu kopienās.

Šausminošais uzbrukums Jaunzēlandes pilsētā Kraistčērčā 2019. gada 15. martā bija drausmīgs atgādinājums par to, kā internetu var izmantot terorisma nolūkos, neatkarīgi no tā, vai tos ir veicinājuši džihādisti, labējais ekstrēmisms vai jebkura cita ekstrēmisma ideoloģija. Ātrums un mērogs, kādā straumētais Kraistčērčas uzbrukuma video izplatījās interneta platformās, skaidri parādīja, cik svarīgi ir tas, ka interneta platformām ir piemēroti pasākumi, lai apturētu šāda satura strauju izplatīšanos.

Reaģējot uz to, dažu dalībvalstu un trešo valstu vai to valdību vadītāji, priekšsēdētājs Ž. K. Junkers un tiešsaistes platformas 2019. gada 15. maijā atbalstīja **Kraistčērčas aicinājumu rīkoties**[4], kurā tika izklāstītas kopējas darbības ar mērķi izskaust teroristisku un vardarbīgu ekstrēmistisku saturu tiešsaistē. Turpmākas saistības šajā sakarībā uzņēmās G7[5] un G20[6].

Uz pašreizējo acīmredzamo apdraudējumu, ko rada teroristisks saturs tiešsaistē, Komisija jau reaģēja ar **tiesību akta priekšlikumu**, par kuru priekšsēdētājs Ž. K. Junkers paziņoja savā 2018. gada runā par stāvokli Savienībā, ierosinot skaidru un saskaņotu tiesisko regulējumu, lai novērstu mitināšanas pakalpojumu sniedzēju ļaunprātīgu izmantošanu teroristiska satura izplatīšanai tiešsaistē[7]. Ierosinātie pasākumi noteiktu, ka interneta platformām ir obligāti vienas stundas laikā jāizņem teroristisks saturs, saņemot jebkuras dalībvalsts kompetentas iestādes pieprasījumu par tā dzēšanu. Turklāt, ja platforma tiek ļaunprātīgi izmantota, lai izplatītu teroristisku saturu, tai būtu pienākums veikt proaktīvus pasākumus, lai noteiktu šo saturu un novērstu tā atkārtotu parādīšanos, paredzot skaidrus noteikumus un aizsardzības pasākumus. Dalībvalstu iestādēm būtu jānodrošina, ka īpašām tiesībaizsardzības iestādēm ir nepieciešamie resursi, lai efektīvi atklātu teroristisku saturu un izdotu dzēšanas rīkojumus.

Tas ļaus izveidot ātru un efektīvu Savienības mēroga sistēmu un ieviesīs stingrus aizsardzības pasākumus, tostarp efektīvus sūdzību iesniegšanas mehānismus un tiesiskās aizsardzības līdzekļus. Ierosinātie pasākumi palīdzēs garantēt netraucētu digitālā vienotā tirgus darbību, vienlaikus palielinot drošību un paaugstinot uzticamību tiešsaistē, kā arī pastiprinot pasākumus vārda un informācijas brīvības aizsardzībai.

Padomē tieslietu un iekšlietu ministri 2018. gada decembrī vienojās par vispārēju nostāju par priekšlikumu. Eiropas Parlaments 2019. gada aprīlī pieņēma savu nostāju pirmajā lasījumā. **Komisija aicina abus likumdevējus pēc iespējas drīz sākt iestāžu sarunas par šo prioritāro iniciatīvu izņemt teroristisku saturu tiešsaistē**, lai panāktu ātru vienošanos par ES tiesisko regulējumu ar

---

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. Francijas prezidents Emanuels Makrons un Jaunzēlandes premjerministre Džasinda Arderna 2019. gada 15. maijā uzaicināja līderus un tiešsaistes platformas uz Parīzi, lai uzsāktu šo iniciatīvu.

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

6 G20 sanāksmē Osakā 2019. gada 28. un 29. jūnijā līderi vēlreiz apstiprināja savu apņemšanos rīkoties, lai aizsargātu cilvēkus pret to, ka terorisms un vardarbīgais ekstrēmisms, kas veicina terorismu, izmanto internetu saviem mērķiem (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final (12.9.2018).

skaidriem noteikumiem un aizsardzības pasākumiem.

Vienlaikus Komisija **ES Interneta foruma**[8] ietvaros turpina sadarbību ar tiešsaistes platformām. Kā Parīzes 2019. gada 15. maija sanāksmē saistībā ar Kraistčērčas aicinājumu rīkoties paziņoja Komisijas priekšsēdētājs Ž. K. Junkers, Komisija kopā ar Eiropolu ir sākusi izstrādāt **ES krīzes protokolu**, lai ļautu valdībām un interneta platformām ātri un saskaņoti reaģēt uz teroristiska satura izplatīšanu tiešsaistē, piemēram, tūlīt pēc teroristu uzbrukuma. Šis darbs ir daļa no pasākumiem starptautiskā līmenī, lai īstenotu Kraistčērčas aicinājumu rīkoties. Papildus turpmākām sarunām ar dalībvalstīm un nozares pārstāvjiem un 2019. gada septembrī plānotajām teorētiskās modelēšanas mācībām, lai simulētu ārkārtas situāciju, Komisija 2019. gada 7. oktobrī sasauks ES Interneta foruma ministru līmeņa sanāksmi, lai apstiprinātu ES krīzes protokolu.

Turklāt Komisija turpina centienus **atbalstīt dalībvalstis un vietējos dalībniekus radikalizācijas novēršanā un apkarošanā** vietējās kopienās visā Eiropā. Tam nepieciešami ilgtspējīgi un ilgstoši centieni, iesaistot visus attiecīgos dalībniekus vietējā, valsts un ES līmenī. **Koordinācijas padome attiecībā uz Savienības darbībām radikalizācijas novēršanai un apkarošanai**, kas 2018. gada augustā tika izveidota, lai konsultētu Komisiju par to, kā stiprināt ES politikas reakciju šajā jomā, 2019. gada 17. jūnijā rīkoja savu otro sanāksmi, lai izpētītu turpmākās darbības tādās prioritārās jomās kā radikalizācija cietumos un ekstrēmistu ideoloģiju apkarošana. Tā kā praksē strādājošie un vietējie speciālisti bieži vien var vislabāk identificēt agrīnas radikalizācijas brīdinājuma pazīmes un veidus, kā to novērst, ES finansētais **Radikalizācijas izpratnes tīkls**[9] turpina sniegt palīdzību praksē strādājošajiem dalībniekiem un apvieno aptuveni 5000 praktiķus no pilsoniskās sabiedrības, skolām un policijas, kā arī valstu koordinatorus un politikas veidotājus.

Nesenā sadarbība starp praksē strādājošajiem darbiniekiem tīkla ietvaros ļāva padziļināt izpratni par problēmām, kas saistītas ar galēji labējo ekstrēmismu. Šogad Radikalizācijas izpratnes tīkls publicēs faktu lapas, lai palīdzētu politikas veidotājiem un praktiķiem noteikt galēji labējā un islāma ekstrēmisma galvenās formas un izpausmes, piemēram, galvenos vēstījumus, valodu, veidus, simbolus, tipoloģijas un stratēģijas. Visbeidzot, tā kā vietējie dalībnieki un **pilsētas** ir vadošajās pozīcijās radikalizācijas novēršanā un apkarošanā, Komisija atbalsta pilsētu ierosinātas iniciatīvas radikalizācijas novēršanai. Pēc 2019. gada 26. februārī notikušās konferences "ES pilsētas pret radikalizāciju" pēc Strasbūras mēra uzaicinājuma 2019. gada 8. jūlijā notika pirmā aptuveni 20 pilsētu pilotgrupas sanāksme, lai palielinātu paraugprakses apmaiņu un uzlabotu pilsētu centienus šajā jomā.

Paralēli tiek turpināts darbs, lai atbalstītu partnervalstis cīņā pret radikalizāciju — tostarp cietumos —, kas var novest pie terorisma.

Lai novērstu draudus, ko rada teroristisks saturs tiešsaistē, Komisija aicina Eiropas Parlamentu un Padomi:

- sākt sarunas par tiesību akta priekšlikumu, lai novērstu **teroristiska satura** izplatīšanu **tiešsaistē**, nolūkā ātri panākt vienošanos par ES tiesisko regulējumu, paredzot skaidrus noteikumus un aizsardzības pasākumus.

2. Kiberdrošības uzlabošana

[8] **ES Interneta forums**, kuru izveidoja 2015. gadā, pulcē ES iekšlietu ministrus, interneta nozares pārstāvjus un citas ieinteresētās personas, lai brīvprātīgā partnerībā strādātu ar mērķi novērst interneta ļaunprātīgu izmantošanu, ko veic teroristu grupējumi, un aizsargātu iedzīvotājus.

[9] Komisija 2011. gadā izveidoja **Radikalizācijas izpratnes tīklu**, lai pulcinātu vienkopus praksē strādājošos un vietējos speciālistus. Komisija 2015. gadā nostiprināja tīklu, izveidojot Radikalizācijas izpratnes tīkla izcilības centru, lai izstrādātu ieinteresētajām personām dalībvalstīs paredzētas mērķtiecīgākas norādes, atbalstu un konsultāciju pakalpojumus un palielinātu dažādu dalībnieku zināšanas un prasmes. Plašāku informāciju par Radikalizācijas izpratnes tīkla darbību skatīt: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

Kiberdrošība joprojām ir viens no galvenajiem drošības jautājumiem. ES ir panākusi jūtamu progresu[10] cīņā pret "klasiskajiem" kiberdraudiem, kuru mērķis ir sistēmas un dati, īstenojot pasākumus, kas izklāstīti 2017. gada septembra kopīgajā paziņojumā[11] "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību". Šie pasākumi ietver ES kiberdrošības tiesību aktu[12], kas Eiropas Savienības Kiberdrošības aģentūrai piešķir pastāvīgas pilnvaras, stiprina tās lomu un izveido ES kiberdrošības sertifikācijas regulējumu. Komisija ir pievērsusies arī nozarei specifiskām prasībām, piemēram, 2019. gada 3. aprīlī pieņemot Ieteikumu par kiberdrošību enerģētikas nozarē[13]. Taču ļaunprātīgu personu nepārtraukta darbības palielināšanās attiecībā uz dažādiem mērķiem un upuriem nozīmē to, ka centieni apkarot kibernoziedzību un uzlabot kiberdrošību joprojām ir ES rīcības prioritāte.

Eiropas Parlamentam un Padomei joprojām ir jāpanāk vienošanās par Komisijas prioritāro iniciatīvu attiecībā uz **Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu**[14]. Priekšlikuma mērķis ir atbalstīt kiberdrošības tehnoloģiskās un industriālās spējas un palielināt Savienības kiberdrošības nozares konkurētspēju. Abi likumdevēji 2019. gada martā pieņēma savas sarunu pilnvaras. Tā kā iestāžu sarunas nebija iespējams pabeigt pirms Eiropas Parlamenta iepriekšējā pilnvaru termiņa beigām, Eiropas Parlaments oficiāli pieņēma savu nostāju pirmajā lasījumā. Tikmēr Padomē turpinās diskusijas starp dalībvalstīm, īpašu uzmanību pievēršot mijiedarbībai starp ierosināto regulu, ar ko izveido Kiberdrošības kompetences centru un tīklu, no vienas puses, un programmām "Apvārsnis Eiropa" un "Digitālā Eiropa", no otras puses. **Komisija aicina abus likumdevējus atsākt un ātri pabeigt iestāžu sarunas par šo prioritāro iniciatīvu kiberdrošības uzlabošanai.**

Tikmēr Komisija turpina **atbalstīt pētniecību un inovācijas**, kas saistītas ar kiberdrošību, pašreizējās daudzgadu finanšu shēmas ietvaros darot pieejamus 135 miljonus EUR projektiem tādās jomās kā kritisko infrastruktūru kiberdrošība, inteliģentā drošības un privātuma pārvaldība un īpaši iedzīvotājiem un mazajiem un vidējiem uzņēmumiem paredzēti instrumenti[15]. Komisija 2019. gada jūlijā izsludināja jaunu uzaicinājumu iesniegt priekšlikumus Eiropas infrastruktūras savienošanas instrumenta programmas ietvaros, darot pieejamus 10 miljonus EUR ES finansējumam, kas paredzēts galvenajiem dalībniekiem, kuri noteikti Tīklu un informācijas drošības direktīvā (TID direktīva)[16], piemēram, Eiropas datordrošības incidentu reaģēšanas vienības, pamatpakalpojumu sniedzēji (piemēram, bankas, slimnīcas, komunālo pakalpojumu sniedzēji, dzelzceļi, aviosabiedrības, domēna nosaukumu sniedzēji) un dažādas valsts iestādes. Pirmo reizi Eiropas kiberdrošības sertifikācijas iestādes arī ir tiesīgas pieteikties šai programmai, lai tās varētu īstenot ES Kiberdrošības aktu.

2019. gada 17. maijā Padome pieņēma **sankciju režīmu**, kas Eiropas Savienībai ļauj piemērot mērķtiecīgus, ierobežojošus pasākumus, ar kuriem novērst kiberuzbrukumus un reaģēt uz tādiem kiberuzbrukumiem, kas rada ārēju apdraudējumu ES un tās dalībvalstīm. Jaunais sankciju režīms ir daļa no **ES kiberdiplomātijas instrumentu kopuma**[17], kas ir satvars vienotai ES diplomātiskajai

---

10 Sīkāku informāciju skatīt brošūrā "Spēcīgas kiberdrošības veidošana Eiropas Savienībā: noturība, atturēšana, aizsardzība" vietnē: https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

11 JOIN(2017) 450 final (13.9.2017.).

12 ES Kiberdrošības akts (2019. gada 17. aprīļa Regula (ES) 2019/881) pirmo reizi ievieš ES mēroga noteikumus attiecībā uz produktu, procesu un pakalpojumu kiberdrošības sertifikāciju. Turklāt Kiberdrošības aktā ir arī noteiktas jaunas pastāvīgas pilnvaras ES Kiberdrošības aģentūrai, kā arī noteikts, ka Aģentūras mērķu sasniegšanai jāatvēl vairāk līdzekļu. Plašāku informāciju par uzaicinājumu iesniegt priekšlikumus skatīt: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

13 C(2019) 2400 final (3.4.2019.) un SWD(2019) 1240 final (3.4.2019.).

14 COM(2018) 630 final (12.9.2018).

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Direktīva (ES) 2016/1148 (6.7.2016.).

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/lv/pdf

reakcijai uz ļaunprātīgām kiberdarbībām[18], kurš ES ļauj pilnībā izmantot kopējās ārpolitikas un drošības politikas pasākumus, lai novērstu ļaunprātīgas kiberdarbības un reaģētu uz tām.

Papildus kiberdraudiem, kas vērsti pret sistēmām un datiem, ES arī strādā, lai risinātu sarežģītas un daudzšķautņainas **hibrīddraudu**[19] radītās problēmas. Eiropadome savos 2019. gada 21. jūnija secinājumos[20] uzsvēra, ka "*ES ir jānodrošina koordinēta reakcija uz hibrīddraudiem un kiberdraudiem un jāstiprina sadarbība ar attiecīgiem starptautiskiem rīcībspēkiem*". Komisija atzinīgi vērtē to, ka hibrīddraudu apkarošana ir arī Padomes prezidentvalsts Somijas prioritāte un ka tieslietu un iekšlietu ministru neformālajā sanāksmē Helsinkos 2019. gada 18. un 19. jūlijā notika uz scenārijiem balstīta politikas diskusija par hibrīddraudiem. Līdzīgas ES aizsardzības jomas politikas vadītāju uz scenārijiem balstītas diskusijas par hibrīddraudiem notika 2019. gada 7. un 8. jūlijā un ES politisko vadītāju diskusijas – 2019. gada 9. un 10. jūlijā, un to rezultātus ārlietu un aizsardzības ministri paziņos kopīgā neoficiālā sesijā 2019. gada 29. un 30. augustā.

Lai uzlabotu kiberdrošību, Komisija aicina Eiropas Parlamentu un Padomi:
• panākt drīzu vienošanos par tiesību akta priekšlikumu par **Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu**.

3. Labāka tiesībaizsardzības iestāžu piekļuve elektroniskajiem pierādījumiem

ES ir veikusi turpmākus pasākumus, lai liegtu teroristiem un noziedzniekiem līdzekļus, ar ko rīkoties, apgrūtinot tiem piekļuvi sprāgstvielu prekursoriem[21], darbību finansēšanu[22] un ceļošanu bez iespējas tikt atklātiem[23].

Sarunas par Komisijas 2018. gada aprīļa priekšlikumiem uzlabot tiesībaizsardzības iestāžu piekļuvi **elektroniskiem pierādījumiem** būtu jāpabeidz pēc iespējas drīz — vairāk nekā puse no visām pašreizējām kriminālizmeklēšanām ietver pārrobežu pieprasījumu par piekļuvi elektroniskiem pierādījumiem[24]. Padome pieņēma sarunu nostāju attiecībā uz priekšlikumiem regulai[25], lai uzlabotu pārrobežu piekļuvi elektroniskiem pierādījumiem kriminālizmeklēšanās, un direktīvai[26], ar ko nosaka saskaņotus noteikumus par juridisko pārstāvju iecelšanu, lai apkopotu pierādījumus kriminālprocesā. Ņemot vērā to, cik ļoti svarīga ir efektīva piekļuve elektroniskiem pierādījumiem, lai veiktu pārrobežu

---

18 Tas ietver kiberuzbrukumus, kā arī kiberuzbrukumu mēģinājumu ar iespējami būtisku ietekmi, kas ietver, piemēram, piekļuvi informācijas sistēmām vai datu pārtveršanu, izmantojot digitālu infrastruktūru, piemēram, 5G tīklus (sk. arī III sadaļu par digitālās infrastruktūras drošības uzlabošanu).

19 Sk. ziņojumu par 2016. gada kopīgā regulējuma hibrīddraudu apkarošanai un 2018. gada kopīgā paziņojuma par noturības un spēju palielināšanu cīņā ar hibrīddraudiem īstenošanu (SWD(2019) 200 final (28.5.2019.)). Sk. arī 2016. gada septembra tiesību akta priekšlikumu regulai, ar ko izveido Savienības režīmu divējāda lietojuma preču eksporta, pārvadājumu, starpniecības, tehniskās palīdzības un tranzīta kontrolei (pārstrādāta versija) (COM(2016) 616 final (28.9.2016.)).

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

21 Regula (ES) 2019/1148 (2019. gada 20. jūnijs) par sprāgstvielu prekursoru tirdzniecību un lietošanu

22 Direktīva (ES) 2019/1153 (2019. gada 20. jūnijs), ar ko paredz noteikumus, lai atvieglotu finanšu un citas informācijas izmantošanu noteiktu noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai kriminālvajāšanai par tiem.

23 Regula (ES) 2019/1157 (2019. gada 20. jūnijs) par Savienības pilsoņu personas apliecību un Savienības pilsoņiem un viņu ģimenes locekļiem, kuri izmanto tiesības brīvi pārvietoties, izsniegto uzturēšanās dokumentu drošības uzlabošanu.

24 Elektroniskos pierādījumus ir nepieciešams iegūt aptuveni 85 % kriminālizmeklēšanas gadījumu, un divās trešdaļās no šīm izmeklēšanām pierādījumus ir nepieciešams pieprasīt no tiešsaistes pakalpojumu sniedzējiem, kas atrodas citā jurisdikcijā. Sk. ietekmes novērtējumu, kas pievienots tiesību akta priekšlikumam (SWD(2018) 118 final (17.4.2018.)).

25 COM(2018) 225 final (17.4.2018.). Padome pieņēma sarunu pilnvaras par ierosināto regulu Tieslietu un iekšlietu padomē 2018. gada 7. decembrī.

26 COM(2018) 226 final (17.4.2018.). Padome pieņēma sarunu nostāju par ierosināto direktīvu Tieslietu un iekšlietu padomē 2019. gada 8. martā.

noziedzības, piemēram, terorisma vai kibernoziedzības, izmeklēšanu vai kriminālvajāšanu, Komisija mudina Eiropas Parlamentu straujāk virzīt šo priekšlikumu, lai abi likumdevēji varētu to ātri pieņemt.

Vienlaikus Komisija cenšas uzlabot un nodrošināt nepieciešamos aizsardzības pasākumus **starptautiskajā elektronisko pierādījumu apmaiņā** saistībā ar pašreizējām sarunām par Eiropas Padomes Budapeštas Konvencijas par kibernoziedzību otro papildu protokolu, kā arī ar Amerikas Savienotajām Valstīm saskaņā ar sarunu pilnvarām, kuras Padome piešķīra Tieslietu un iekšlietu padomes sanāksmē 2019. gada 6. un 7. jūnijā[27]. Komisija piedalījās pēdējā sarunu kārtā par Eiropas Padomes Budapeštas Konvencijas par kibernoziedzību otro papildu protokolu, kuras notika 2019. gada 9.–11. jūlijā. Komisija un Amerikas Savienoto Valstu iestādes pašlaik tehniskajā līmenī gatavojas oficiālai sarunu uzsākšanai par ES un ASV nolīgumu attiecībā uz pārrobežu piekļuvi elektroniskiem pierādījumiem.

Lai uzlabotu tiesībaizsardzības iestāžu piekļuvi elektroniskiem pierādījumiem, Komisija aicina Eiropas Parlamentu:

- pieņemt sarunu mandātu par tiesību aktu priekšlikumiem attiecībā uz **elektroniskiem pierādījumiem**, lai ātri uzsāktu trialoga sarunas ar Padomi. *(Kopīgajā paziņojumā paredzēta prioritāte)*

4. Spēcīgākas un viedākas drošības, robežu un migrācijas pārvaldības informācijas sistēmas

Pēc tam, kad tika pieņemti noteikumi par **informācijas sistēmu sadarbspēju**[28], kas novērsīs informācijas nepilnības un neredzamās zonas, palīdzot atklāt personas ar vairākām identitātēm un apkarot identitātes viltošanu, Komisija ātri uzsāka vairākas iniciatīvas, lai atbalstītu dalībvalstis īstenošanas procesā, tostarp vajadzības gadījumā nodrošinot finansējumu, kā arī organizējot seminārus, lai veicinātu pieredzes un paraugprakses apmaiņu. Cieša sadarbība starp ES aģentūrām, visām dalībvalstīm un Šengenas asociētajām valstīm būs īpaši svarīga, lai sasniegtu vērienīgo mērķi – līdz 2020. gadam panākt ES drošības, robežu un migrācijas pārvaldības informācijas sistēmu pilnīgu sadarbspēju.

Šā mērķa sasniegšanai nepieciešams arī ātri un pilnībā īstenot tiesību aktus, par kuriem nesen tika panāktas vienošanās, lai izveidotu jaunas informācijas sistēmas, proti, ES ieceļošanas/izceļošanas sistēmu[29] un Eiropas ceļošanas informācijas un atļauju sistēmu[30], kā arī pastiprināt Šengenas informācijas sistēmu[31], un paplašināt Eiropas Sodāmības reģistru informācijas sistēmu[32], to attiecinot uz trešo valstu valstspiederīgajiem. Jaunā spēcīgāku un viedāku drošības, robežu un migrācijas pārvaldības informācijas sistēmu struktūra būs iedarbīga tikai tad, ja visi komponenti tiks pilnībā īstenoti Savienības līmenī un katrā dalībvalstī saskaņā ar pieņemto grafiku.

Vienlaikus abiem likumdevējiem ir jāveic turpmāki pasākumi, lai pabeigtu darbu pie spēcīgāku un viedāku drošības, robežu un migrācijas pārvaldības informācijas sistēmu izveides. **Eiropas ceļošanas informācijas un atļauju sistēmas** tehniskās īstenošanas ietvaros Komisija 2019. gada 7. janvārī iesniedza divus priekšlikumus, ar ko paredz tehniskus grozījumus saistītajā regulā[33], kuri nepieciešami sistēmas pilnīgai izveidei. Komisija aicina abus likumdevējus paātrināt darbu pie minētajiem tehniskajiem grozījumiem, lai pēc iespējas drīz panāktu vienošanos, tādējādi

[27] https://www.consilium.europa.eu/lv/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[28] Regula (ES) 2019/817 (20.5.2019.) un Regula (ES) 2019/818 (20.5.2019.).

[29] Regula (ES) 2017/2226 (30.11.2017.).

[30] Regula (ES) 2018/1240 (12.9.2018.) un Regula (ES) 2018/1241 (12.9.2018.).

[31] Regula (ES) 2018/1860 (28.11.2018.), Regula (ES) 2018/1861 (28.11.2018.), Regula (ES) 2018/1862 (28.11.2018.).

[32] Regula (ES) 2019/816 (17.4.2019.).

[33] COM(2019) 3 final un COM(2019) 4 final (7.1.2019.).

dodot iespēju ātri un savlaicīgi ieviest Eiropas ceļošanas informācijas un atļauju sistēmu, lai tā varētu sākt darboties 2021. gada sākumā.

Komisija 2018. gada maijā nāca klajā ar priekšlikumu **stiprināt pašreizējo vīzu informācijas sistēmu**[34], kas paredzēja rūpīgāku vīzas pieteikumu iesniedzēju iepriekšējās darbības pārbaudi un informācijas trūkuma novēršanu, nodrošinot labāku informācijas apmaiņu starp dalībvalstīm. Padome 2018. gada 19. decembrī pieņēma sarunu pilnvaras, un 2019. gada 13. martā Eiropas Parlamenta plenārsēdē notika balsojums par ziņojumu saistībā ar priekšlikumu, tādējādi pabeidzot pirmo lasījumu. Komisija aicina pēc iespējas drīz pēc jaunā Eiropas Parlamenta izveides sākt sarunas starp abiem likumdevējiem.

Komisija 2016. gada maijā ierosināja paplašināt ***Eurodac***[35] tvērumu, to izmantojot ne tikai patvēruma meklētāju identifikācijai, bet arī trešo valstu tādu valstspiederīgo identifikācijai, kas uzturas nelikumīgi, un tādu personu identificēšanai, kurs neatbilstīgi ieceļo ES. Saskaņā ar Eiropadomes 2018. gada decembra secinājumiem[36] un Komisijas 2019. gada 6. marta paziņojumu par progresu, īstenojot Eiropas programmu migrācijas jomā[37], Komisija aicina abus likumdevējus nekavējoties pieņemt priekšlikumu. Šis tiesību akta priekšlikums ir jāpieņem, lai *Eurodac* kļūtu par sadarbspējīgu ES informācijas sistēmu nākotnes struktūras sastāvdaļu, tādējādi integrējot būtiskos datus par trešo valstu valstspiederīgajiem, kas uzturas nelikumīgi, un tiem, kuri neatbilstīgi ieceļojuši ES.

Lai nostiprinātu ES drošības, robežu un migrācijas pārvaldības informācijas sistēmas, Komisija aicina Eiropas Parlamentu un Padomi:

- pieņemt tiesību akta priekšlikumu par ***Eurodac*** *(kopīgajā paziņojumā paredzēta prioritāte)*;
- turpināt darbu, lai panāktu drīzu vienošanos par ierosinātajiem tehniskajiem grozījumiem, kas vajadzīgi, lai izveidotu **Eiropas ceļošanas informācijas un atļauju sistēmu**.

III. DIGITĀLO INFRASTRUKTŪRU DROŠĪBAS UZLABOŠANA

Mūsu digitālās infrastruktūras noturība ir būtiski svarīga pārvaldei, uzņēmējdarbībai, personas datu drošībai un demokrātisko iestāžu darbībai. **Piektās paaudzes (5G) tīkli**, kas tiks izvērsti turpmākajos gados, veidos mūsu sabiedrības un ekonomikas digitālo pamatu, savienojot miljardiem iedzīvotāju, objektu un sistēmu, tostarp tādās svarīgās nozarēs kā enerģētika, transports, banku nozare un veselības aprūpe, kā arī savienojot rūpnieciskās kontroles sistēmas, kas apstrādā sensitīvu informāciju un atbalsta drošības sistēmas.

Ir aplēsts, ka 2025. gadā visā pasaulē no 5G tīkliem tiks gūti ieņēmumi 225 miljardu EUR apmērā, tādējādi 5G ir būtisks līdzeklis, kas ļaus Eiropai konkurēt pasaules tirgū, un **5G tīklu drošība ir īpaši svarīga Savienības stratēģiskās autonomijas nodrošināšanā**. Lai nodrošinātu augstu kiberdrošības līmeni, ir vajadzīgi saskaņoti pasākumi gan valstu, gan Eiropas līmenī, jo jebkura neaizsargātība 5G tīklos vienā dalībvalstī ietekmētu Savienību kopumā.

Pēc valstu vai to valdību vadītāju 2019. gada martā paustā atbalsta Eiropadomē[38] Komisija 2019. gada 26. martā nāca klajā ar **Ieteikumu par 5G tīklu kiberdrošību**[39], tajā izklāstot darbības, kas palīdzēs novērtēt 5G tīklu kiberdrošības riskus un stiprināt preventīvus pasākumus. Ieteikumu pamatā ir koordinēti ES riska novērtēšanas un riska pārvaldības pasākumi, efektīvs sadarbības un informācijas apmaiņas regulējums un kopīga ES situācijas apzināšanās, kas aptver svarīgus sakaru tīklus.

---

34 COM(2018) 302 final (16.5.2018.).
35 COM(2016) 272 final (4.5.2016.).
36 https://www.consilium.europa.eu/lv/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
37 COM(2019) 126 final (6.3.2019.).
38 https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/lv/pdf
39 C(2019) 2335 final (26.3.2019.).

Ar ieteikumu ievadītā procesa **pirmajā posmā** visas dalībvalstis līdz 2019. gada 15. jūlijam bija pabeigušas savu **riska novērtējumu** un iesniedza savus secinājumus Komisijai un ES Kiberdrošības aģentūrai vai arī paziņoja, ka tas tiks drīz izdarīts. Pēc valstu riska novērtējumiem sekoja vadlīniju kopums un vienota veidne ziņošanai par konstatējumiem, par kuru dalībvalstis un Komisijas vienojās, lai veicinātu konsekvenci un atvieglotu informācijas apmaiņu par valstu rezultātiem ES līmenī. Visās dalībvalstīs tika izvērtēti šādi parametri:

- galvenie apdraudējumi un apdraudējuma radītāji, kas ietekmē 5G tīklus;
- 5G tīkla sastāvdaļu un funkciju, kā arī citu elementu jutība; kā arī
- dažādi neaizsargātības veidi, tostarp gan tehniski, gan citādi, piemēram, tādi, kas potenciāli izriet no 5G piegādes ķēdes.

Turklāt darbā pie nacionālajiem riska novērtējumiem dalībvalstīs tika iesaistīti vairāki atbildīgie dalībnieki, piemēram, atkarībā no valsts pienākumiem kiberdrošības un telesakaru iestādes, drošības un izlūkošanas dienesti, tādējādi stiprinot to sadarbību un koordinēšanu. Paralēli un ņemot vērā valstu grafikus 5G ieviešanai, vairākas dalībvalstis jau ir veikušas pasākumus, lai šajā jomā pastiprinātu piemērojamās drošības prasības, savukārt vairākas citas ir paudušas savu nodomu tuvākajā nākotnē apsvērt jaunus pasākumus.

Pamatojoties uz nacionālajiem riska novērtējumiem, dalībvalstu kiberdrošības iestādes Tīklu un informācijas sistēmas sadarbības grupā[40] līdz 2019. gada 1. oktobrim sagatavos **ES līmenī esošo risku kopīgu pārskatīšanu**, kas būs ar ieteikumu ierosinātā procesa otrais posms. Uz šā pamata un kā trešo posmu sadarbības grupa līdz 2019. gada 31. decembrim sagatavos **vienotu Savienības riska mazināšanas pasākumu kopumu**, lai novērstu konstatētos riskus. Komisija un ES Kiberdrošības aģentūra turpinās atbalstīt ieteikuma īstenošanu.

Darbu Tīklu un informācijas sistēmu sadarbības grupā atbalsta vairāki citi forumi. Eiropas Elektronisko komunikāciju regulatoru iestāde gatavo apsekojumu par visiem pašreizējiem drošības pasākumiem, kas potenciāli attiecas uz 5G. ES Kiberdrošības aģentūras īpašā ekspertu grupa ir sākusi darbu pie 5G drošības apdraudējuma kopainas izveides. Turklāt pēc Kiberdrošības akta stāšanās spēkā 2019. gada 27. jūnijā Komisija un ES Kiberdrošības aģentūra veiks visus vajadzīgos pasākumus, lai izveidotu ES mēroga sertifikācijas regulējumu. Dalībvalstis 2019. gada jūnijā tikās arī Standartizācijas komitejā, lai apspriestu kiberdrošības un standartizācijas jautājumus, reaģējot uz ieteikumu izpētīt turpmākās kiberdrošības standartizācijas problēmas, tostarp 5G tīklus, kā arī piemērotas politikas iniciatīvas ES līmenī.

Visbeidzot, 5G tīklu drošība Savienībai ir stratēģiski svarīga. Ārvalstu investīcijas stratēģiskās nozarēs, kritisku aktīvu, tehnoloģiju un infrastruktūras iegāde Savienībā un kritiski svarīgu iekārtu piegāde arī var radīt risku Savienības drošībai.

Jaunais **ES regulējums ārvalstu tiešo ieguldījumu izvērtēšanai**[41] stājās spēkā 2019. gada 10. aprīlī. Turpmāko 18 mēnešu laikā Komisija un ES dalībvalstis veiks nepieciešamos pasākumus, lai nodrošinātu, ka ES var pilnībā piemērot Ieguldījumu izvērtēšanas regulu no 2020. gada 11. oktobra.

---

[40] Tīklu informācijas drošības sadarbības grupa ir izveidota saskaņā ar Direktīvu (ES) 2016/1148 (6.7.2016.) par tīklu un informācijas sistēmu drošību. Kā izklāstīts ieteikumā, Tīklu informācijas drošības sadarbības grupā tika izveidota īpaša darba plūsma, ko vada vairākas dalībvalstis. Grupa jau tikās trīs reizes, proti, 2019. gada aprīlī, maijā un jūlijā, lai apmainītos ar informāciju par valstu pieejām un apspriestu, kā atvieglot koordinētu ES riska novērtēšanas sagatavošanu.

[41] Regula (ES) 2019/452 (2019. gada 19. marts), ar ko izveido regulējumu ārvalstu tiešo ieguldījumu Savienībā izvērtēšanai. Ar jauno regulējumu iedibina sadarbības mehānismu, kurā dalībvalstis un Komisija varēs apmainīties ar informāciju un pievērst uzmanību bažām saistībā ar konkrētiem ieguldījumiem. Tas arī ļaus Komisijai izdot atzinumus gadījumos, kad ieguldījumi apdraud vairāk nekā vienas dalībvalsts drošību

IV. CĪŅA PRET NELIKUMĪGI IEGŪTU LĪDZEKĻU LEGALIZĒŠANU

Noziedznieku un teroristu spēja pārskaitīt līdzekļus starp banku kontiem dažu stundu laikā ļauj tiem vieglāk sagatavot terora aktus vai legalizēt noziedzīgi iegūtus līdzekļus dažādās dalībvalstīs. Lai risinātu šo problēmu, Savienība ir izstrādājusi stabilu **tiesisko regulējumu nelikumīgi iegūtu līdzekļu legalizēšanas un teroristu finansēšanas apkarošanai** saskaņā ar starptautiskajiem standartiem, ko pieņēmusi Finanšu darbību darba grupa.

Ņemot vērā vajadzību iet kopsolī ar pārmaiņām tendencēs, tehnoloģiju attīstībā un noziedznieku izdomu sistēmas trūkumu vai nepilnību izmantošanā, Komisija 2019. gada 24. jūlijā pieņēma **četru ziņojumu paketi**, kuros analizēti pašreizējie riski un neaizsargātība saistībā ar nelikumīgi iegūtu līdzekļu legalizāciju, kā arī novērtēts veids, kā attiecīgie dalībnieki piemēro regulējumu gan privātajā, gan publiskajā sektorā[42].

Pakete ietver **novērtējumu par valstu centralizēto banku kontu reģistru un datu izguves sistēmu iespējamo savstarpējo savienojamību** Eiropas Savienībā. Šādas valstu centralizētās sistēmas ļauj identificēt jebkuru fizisku vai juridisku personu, kuras turējumā vai kontrolē ir maksājumu konti, bankas konti un individuāli seifi, — šī informācija bieži vien ir būtiska kompetentajām iestādēm cīņā pret nelikumīgi iegūtu līdzekļu legalizāciju un teroristu finansēšanu. Piektā direktīva par nelikumīgi iegūtu līdzekļu legalizācijas novēršanu[43] paredz dalībvalstīm ieviest šādas valsts centralizētas sistēmas un nodrošināt savām finanšu ziņu vākšanas vienībām tiešu piekļuvi tām. Noteikumi, kas nesen pieņemti, lai atvieglotu finanšu informācijas izmantošanu smagu noziegumu apkarošanai[44], nodrošina noteiktām tiesībaizsardzības iestādēm un līdzekļu atguves dienestiem tiešu piekļuvi to attiecīgajiem valsts centralizētajiem banku kontu reģistriem. Pamatojoties uz to un saskaņā ar Nelikumīgi iegūtu līdzekļu legalizācijas novēršanas direktīvu, ziņojumā novērtēti dažādi IT risinājumi ES līmenī, kas jau darbojas vai tiek izstrādāti un ko var izmantot kā modeli valstu centralizēto sistēmu iespējamai savstarpējai savienojamībai. Tā kā turpmākā centralizēto mehānismu savstarpējā savienojamība ES mērogā varētu paātrināt finanšu informācijas pieejamību un atvieglot kompetento iestāžu pārrobežu sadarbību, Komisija plāno turpināt apspriesties ar attiecīgajām ieinteresētajām personām, valdībām, kā arī finanšu ziņu vākšanas vienībām, tiesībaizsardzības iestādēm un līdzekļu atguves dienestiem kā iespējamās savstarpējās savienojamības sistēmas potenciāliem "galalietotājiem".

Kā daļa no Komisijas pārdomām par finanšu ziņu vākšanas vienību darbu, ziņojums, kurā novērtēta **sadarbība starp finanšu ziņu vākšanas vienībām**, aplūko gan sadarbību Savienībā, gan ar trešām valstīm[45]. Tajā ir apzināti daži trūkumi, kas varētu turpināties, līdz finanšu ziņu vākšanas vienību uzdevumi un pārrobežu sadarbības pienākumi tiks skaidrāk noteikti ES tiesiskajā regulējumā

---

vai sabiedrisko kārtību vai kad ieguldījumi varētu apdraudēt kādu ES mēroga projektu vai programmu. Dalībvalstij, kurā tiek veikti ieguldījumi, ir galīgais vārds par to, kā rīkoties ar šiem ieguldījumiem.

42 *Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities* (Ziņojums par nelikumīgi iegūtu līdzekļu legalizēšanas un teroristu finansēšanas riska novērtējumu, kas skar iekšējo tirgu un attiecas uz pārrobežu darbībām) (COM(2019) 370 final, 24.7.2019.), *Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts* (Ziņojums par dalībvalstu centralizēto automatizēto mehānismu (centrālo reģistru vai centrālo elektronisko datu izguves sistēmu) savstarpējo savienojamību attiecībā uz banku kontiem) (COM(2019) 372 final, 24.7.2019.), *Report on the assessment of recent alleged money laundering cases involving EU credit institutions* (Ziņojums par novērtējumu saistībā ar nesenajiem iespējamiem nelikumīgi iegūtu līdzekļu legalizācijas gadījumiem, kuros iesaistītas ES kredītiestādes) (COM(2019) 373 final, 24.7.2019.), *Report assessing the framework for cooperation between Financial Intelligence Units* (Ziņojums, kurā novērtēts sadarbības starp finanšu ziņu vākšanas vienībām regulējums) (COM(2019) 371 final, 24.7.2019.).

43 Direktīva (ES) 2015/849 (20.5.2015.).

44 Direktīva (ES) 2019/1153 (20.6.2019.).

45 Šāds novērtējums ir prasīts Piektajā direktīvā par nelikumīgi iegūtu līdzekļu legalizācijas novēršanu (Direktīva (ES) 2018/843 (30.5.2018.)).

nelikumīgi iegūtu līdzekļu legalizācijas un teroristu finansēšanas apkarošanai. Novērtējums arī liecina, ka ir vajadzīgs stingrāks mehānisms, lai koordinētu un atbalstītu pārrobežu sadarbību un analīzi.

Līdztekus pašreizējam darbam, kas tiek veikts, lai apkarotu nelikumīgi iegūtu līdzekļu legalizāciju un teroristu finansēšanu, un atbildot arī uz Eiropas Parlamenta aicinājumu[46], Komisija turpinās izvērtēt tādu papildu pasākumu nepieciešamību, tehnisko iespējamību un samērīgumu, kas vajadzīgi, lai izsekotu teroristu finansēšanu ES[47].

V. CITU PRIORITĀRU DROŠĪBAS JOMAS DOKUMENTU ĪSTENOŠANA

1. Likumdošanas pasākumu īstenošana drošības savienībā

Panākot vienošanos par pasākumiem drošības savienībā, procesa nebeidzas — ir vitāli būtiski nodrošināt to ātru un pilnīgu īstenošanu dalībvalstīs, lai būtu iespējams izmantot visas priekšrocības. Šajā nolūkā Komisija aktīvi atbalsta dalībvalstis, tostarp izmantojot finansējumu un veicinot paraugprakses apmaiņu.
Tomēr vajadzības gadījumā Komisija gatava pilnībā izmantot Līgumos paredzētās pilnvaras ES tiesību aktu īstenošanai, tostarp vajadzības gadījumā arī pienākuma neizpildes procedūras.

ES pasažieru datu reģistra direktīvas[48] īstenošanas termiņš bija 2018. gada 25. maijs. Par pilnīgu tās transponēšanu līdz šim Komisijai ir paziņojušas 25 dalībvalstis[49]. Neraugoties uz to, ka 2018. gada 19. jūlijā tika sāktas pienākumu neizpildes procedūras, direktīva joprojām nav pilnībā transponēta divās dalībvalstīs[50]. Līdztekus Komisija turpina atbalstīt visu dalībvalstu pūliņus pabeigt savu pasažieru datu reģistra sistēmu izstrādi, tostarp atvieglinot informācijas un paraugprakses apmaiņu.

Direktīvas par terorisma apkarošanu[51] transponēšanas termiņš beidzās 2018. gada 8. septembrī. Par pilnīgu tās transponēšanu līdz šim Komisijai ir paziņojušas 22 dalībvalstis. Neraugoties uz to, ka 2018. gada 22. novembrī tika sāktas pienākumu neizpildes procedūras, trīs dalībvalstis joprojām nav paziņojušas par tādu valsts tiesību aktu pieņemšanu, ar kuriem pilnībā transponē direktīvu[52].

Direktīvas par ieroču iegādes un turēšanas kontroli[53] transponēšanas termiņš beidzās 2018. gada 14. septembrī. Par pilnīgu tās transponēšanu līdz šim Komisijai ir paziņojušas 8 dalībvalstis. Neraugoties uz to, ka 2018. gada 22. novembrī tika sāktas pienākumu neizpildes procedūras, 20 dalībvalstis joprojām nav paziņojušas par tādu valsts pasākumu pieņemšanu, ar kuriem pilnībā transponē direktīvu[54].

---

46 Eiropas Parlamenta Īpašā komiteja terorisma jautājumos savā 2018. gada decembrī pieņemtajā galīgajā ziņojumā aicināja izveidot Eiropas Savienības Teroristu finansēšanas izsekošanas sistēmu, kas mērķorientēti pievērstos to personu darījumiem, kuras ir saistītas ar terorismu, un to finansēšanai vienotajā euro maksājumu telpā.

47 Sk. Astoņpadsmito progresa ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2019) 145 final (20.3.2019.)).

48 Direktīva (ES) 2016/681 (27.4.2016.).

49 Atsaucēs uz pilnīgas transponēšanas paziņojumu ņem vērā dalībvalstu deklarācijas, un tās neskar Komisijas dienestu veikto transponēšanas pārbaudi.

50 Slovēnija paziņoja par daļēju transponēšanu. Spānija nepaziņoja par transponēšanu (stāvoklis 2019. gada 24. jūlijā).

51 Direktīva (ES) 2017/541 (15.3.2017.).

52 Polija paziņoja par daļēju transponēšanu. Grieķija un Luksemburga par transponēšanu nav ziņojušas (stāvoklis 2019. gada 24. jūlijā).

53 Direktīva (ES) 2017/853 (17.5.2017.).

54 Beļģija, Čehija, Igaunija, Lietuva, Polija, Portugāle, Zviedrija un Apvienotā Karaliste paziņoja par daļēju transponēšanu. Vācija, Īrija, Grieķija, Spānija, Kipra, Luksemburga, Ungārija, Nīderlande, Rumānija, Slovēnija, Slovākija un Somija nav paziņojušas par transponēšanu (stāvoklis 2019. gada 24. jūlijā).

Attiecībā uz **Datu aizsardzības tiesību piemērošanas direktīvas**[55] transponēšanu valsts tiesību aktos — transponēšanas termiņš bija 2018. gada 6. maijs. Par pilnīgu tās transponēšanu līdz šim Komisijai ir paziņojušas 20 dalībvalstis[56]. Neraugoties uz to, ka 2018. gada 19. jūlijā tika sāktas pienākumu neizpildes procedūras, 7 dalībvalstis joprojām nav paziņojušas par tādu valsts pasākumu pieņemšanu, ar kuriem pilnībā transponē direktīvu[57].

Dalībvalstīm līdz 2018. gada 9. maijam bija jātransponē valsts tiesību aktos **Tīklu un informācijas sistēmu drošības direktīva**[58]. Līdz šim 26 dalībvalstis ir paziņojušas Komisijai par pilnīgu transponēšanu, un 2 dalībvalstis direktīvu ir transponējušas daļēji[59]. Turklāt līdz 2018. gada 9. novembrim dalībvalstīm bija pienākums identificēt pamatpakalpojumu sniedzējus saskaņā ar direktīvu. Komisijai līdz 2019. gada 9. maijam bija jāiesniedz Eiropas Parlamentam un Padomei ziņojums, kurā novērtēta tās pieejas konsekvence, ko izmanto pamatpakalpojumu sniedzēju identificēšanā dalībvalstu teritorijā. Tomēr, tā kā vairākām dalībvalstīm vēl bija jāiesniedz pilnīga informācija par identificēšanas procesu, Komisijai bija jāatliek ziņojums.

Komisija novērtē **Ceturtās direktīvas par nelikumīgi iegūtu līdzekļu legalizācijas novēršanu**[60] transponēšanu un kā arī to, vai dalībvalstis īsteno noteikumus. Komisija ir uzsākusi pārkāpuma procedūras pret visām 24 dalībvalstīm, jo tā konstatēja, ka no dalībvalstīm saņemtie paziņojumi liecina par to, ka šī direktīva nav pilnībā transponēta[61].

Komisija aicina dalībvalstis steidzami veikt pasākumus, kas nepieciešami, lai valsts tiesību aktos pilnībā transponētu šādas direktīvas, un paziņot par tiem Komisijai:

- **ES Pasažieru datu reģistra direktīva**, attiecībā uz kuru vienai dalībvalstij vēl jāpaziņo par transponēšanu valsts tiesību aktos un vienai dalībvalstij jāpabeidz transponēšanas paziņošana[62];
- **Direktīva par terorisma apkarošanu**, attiecībā uz kuru divām dalībvalstīm vēl jāpaziņo par transponēšanu valsts tiesību aktos un vienai dalībvalstij jāpabeidz transponēšanas paziņošana[63];
- **Direktīva par ieroču iegādes un turēšanas kontroli**, attiecībā uz kuru 12 dalībvalstīm vēl jāpaziņo par transponēšanu valsts tiesību aktos un astoņām dalībvalstīm jāpabeidz transponēšanas paziņošana[64];
- **Datu aizsardzības tiesību piemērošanas direktīva**, attiecībā uz kuru divām dalībvalstīm vēl jāpaziņo par transponēšanu valsts tiesību aktos un piecām dalībvalstīm ir jāpabeidz transponēšanas paziņošana[65];
- **Direktīva par tīklu informācijas sistēmu drošību**, attiecībā uz kuru divām dalībvalstīm vēl

55 Direktīva (ES) 2016/680 (27.4.2016.).

56 20 dalībvalstis pabeidza transponēšanu (stāvoklis 2019. gada 24. jūlijā).

57 Latvija, Portugāle, Slovēnija un Somija paziņoja par daļēju transponēšanu. Grieķija un Spānija nepaziņoja par transponēšanu. Lai gan Vācija paziņoja par to, ka transponēšana ir pabeigta, Komisija uzskata, ka šī transponēšana nav pilnīga (situācija 2019. gada 24. jūlijā).

58 Direktīva (ES) 2016/1148 (27.4.2016.).

59 Beļģija un Ungārija direktīvu ir daļēji transponējušas (stāvoklis 2019. gada 24. jūlijā).

60 Direktīva (ES) 2015/849 (20.5.2015.).

61 Beļģija, Bulgārija, Čehija, Dānija, Vācija, Igaunija, Īrija, Spānija, Francija, Itālija, Kipra, Latvija, Lietuva, Ungārija, Nīderlande, Austrija, Polija, Portugāle, Rumānija, Slovēnija, Slovākija, Somija, Zviedrija un Apvienotā Karaliste (stāvoklis 2019. gada 24. jūlijā).

62 Slovēnija paziņoja par daļēju transponēšanu. Spānija nepaziņoja par transponēšanu (stāvoklis 2019. gada 24. jūlijā).

63 Polija paziņoja par daļēju transponēšanu. Grieķija un Luksemburga par transponēšanu nav ziņojušas (stāvoklis 2019. gada 24. jūlijā).

64 Beļģija, Čehija, Igaunija, Lietuva, Polija, Portugāle, Zviedrija un Apvienotā Karaliste paziņoja par daļēju transponēšanu. Vācija, Īrija, Grieķija, Spānija, Kipra, Luksemburga, Ungārija, Nīderlande, Rumānija, Slovēnija, Slovākija un Somija nav paziņojušas par transponēšanu (stāvoklis 2019. gada 24. jūlijā).

65 Latvija, Portugāle, Slovēnija un Somija paziņoja par daļēju transponēšanu. Grieķija un Spānija nepaziņoja par transponēšanu. Lai gan Vācija paziņoja par to, ka transponēšana ir pabeigta, Komisija uzskata, ka šī transponēšana nav pilnīga (stāvoklis 2019. gada 24. jūlijā).

jāpabeidz transponēšanas paziņošana[66]; kā arī

- **Ceturtā direktīva par nelikumīgi iegūtu līdzekļu legalizācijas novēršanu**, attiecībā uz kuru 24 dalībvalstīm vēl ir jāpabeidz transponēšanas paziņošana[67].

2. Dezinformācijas novēršana un vēlēšanu aizsardzība pret citiem kiberiespējotiem draudiem

Demokrātisku procesu un iestāžu aizsardzība pret dezinformāciju un ar to saistīto iejaukšanos ir liels izaicinājums sabiedrībai visā pasaulē. Lai to novērstu, ES ir ieviesusi **stabilu sistēmu koordinētai rīcībai pret dezinformāciju** pilnīgā saskaņā ar Eiropas vērtībām un pamattiesībām[68]. Kā izklāstīts 2019. gada 14. jūnija kopīgajā paziņojumā par Rīcības plāna dezinformācijas apkarošanai īstenošanu[69], darbs vairākās papildu jomās ir palīdzējis samazināt dezinformācijas telpu un saglabāt Eiropas Parlamenta vēlēšanu integritāti.

Eiropadome savos 2019. gada 21. jūnija secinājumos[70] atzinīgi novērtēja Komisijas ieceri padziļināti izvērtēt to, kā tiek īstenotas saistības, ko saskaņā ar **prakses kodeksu dezinformācijas jomā**[71] ir uzņēmušās tiešsaistes platformas un citi parakstītāji, un aicināja Komisiju un Savienības Augsto pārstāvi ārlietās un drošības politikas jautājumos pastāvīgi novērtēt *mainīgo draudu raksturu un arvien lielāko ļaunprātīgas iejaukšanās un tiešsaistes manipulēšanas risku saistībā ar mākslīgā intelekta attīstību un datu vākšanas paņēmieniem* un uz to atbilstoši reaģēt.

Komisija un Augstā pārstāve turpinās savu darbu šajā jomā saskaņā ar Eiropadomes secinājumiem. Komisija un Augstā pārstāve 2019. gada martā izveidoja **ātrās brīdināšanas sistēmu** starp ES iestādēm un dalībvalstīm, lai veicinātu dalīšanos ar atziņām, kas saistītas ar dezinformācijas kampaņām un koordinētu reaģēšanu. Dalībvalstu kontaktpunktu pirmā sanāksme pēc Eiropas Parlamenta vēlēšanām notika 2019. gada 3. un 4. jūnijā Tallinā. Lai vēl vairāk pilnveidotu ātrās reaģēšanas sistēmu, Augstā pārstāve un Komisija ciešā sadarbībā ar dalībvalstīm 2019. gada rudenī pārskatīs, kā darbojas ātrās reaģēšanas sistēma. Tās izstrādās arī kopīgu metodiku dezinformācijas kampaņu analīzei un atmaskošanai, kā arī spēcīgākas partnerības ar tādiem starptautiskiem partneriem kā, piemēram, G7 un NATO.

Darbs turpinās arī **Eiropas Parlamenta vēlēšanu sadarbības tīklā**[72], kura pirmā sanāksme notika 2019. gada 7. jūnijā, lai izvērtētu Eiropas Parlamenta vēlēšanas. Minētie apsvērumi un turpmākais

66 Beļģija un Ungārija direktīvu ir daļēji transponējušas (stāvoklis 2019. gada 24. jūlijā).

67 Beļģija, Bulgārija, Čehija, Dānija, Vācija, Igaunija, Īrija, Spānija, Francija, Itālija, Kipra, Latvija, Lietuva, Ungārija, Nīderlande, Austrija, Polija, Portugāle, Rumānija, Slovēnija, Slovākija, Somija, Zviedrija un Apvienotā Karaliste (stāvoklis 2019. gada 24. jūlijā).

68 Sk. Rīcības plānu dezinformācijas apkarošanai (JOIN(2018) 36 final, 5.12.2018.).

69 JOIN(2019) 12 final (14.6.2019.).

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf Eiropadomes aicinājuma pamatā ir Padomes prezidentvalsts Rumānijas, kā arī Komisijas un Savienības Augstās pārstāves ārlietās un drošības politikas jautājumos devums attiecībā uz pieredzi, kas gūta saistībā ar dezinformāciju un brīvu un godīgu vēlēšanu nodrošināšanu, tostarp kopīgais paziņojums par Rīcības plāna dezinformācijas apkarošanai īstenošanu.

71 Prakses kodeksu 2018. gada oktobrī parakstīja tiešsaistes platformas *Facebook*, *Google*, *Twitter* un *Mozilla*, kā arī reklāmdevēju un reklāmas nozare, un tajā ir noteikti pašregulācijas standarti dezinformācijas apkarošanai. Kodeksa nolūks ir sasniegt mērķus, kas izklāstīti 2018. gada aprīļa Komisijas paziņojumā par vēršanos pret dezinformāciju tiešsaistē (COM(2018)236 final, 26.4.2018.), nosakot plašu saistību klāstu, sākot ar politisko reklāmu pārredzamības un beidzot ar viltus kontu slēgšanu un dezinformācijas kanālu demonetizāciju.

72 Eiropas Parlamenta vēlēšanu sadarbības tīklā ir apvienoti to iestāžu valsts vēlēšanu sadarbības tīklu kontaktpunkti, kas ir kompetentas vēlēšanu jautājumos, kā arī to iestāžu, kuras atbild par noteikumu uzraudzību un izpildi saistībā ar tādām darbībām tiešsaistē, kas ir saistītas ar vēlēšanām. Eiropas Parlamenta vēlēšanu sadarbības tīkla uzdevums ir brīdināt par apdraudējumiem, apmainīties ar paraugpraksi starp valstu tīkliem, apspriest kopīgus risinājumus nolūkā identificēt problēmas un veicināt kopīgus projektus un mācības starp valstu tīkliem.

attiecīgo valstu iestāžu, politisko partiju un tiešsaistes platformu ieguldījums palīdzēs sagatavot Komisijas visaptverošu ziņojumu par Eiropas Parlamenta vēlēšanām, kas tiks pieņemts 2019. gada oktobrī. Dalībvalstis izmantoja tīklu ne tikai attiecībā uz Eiropas Parlamenta, bet arī citām vēlēšanām, un tas liecina par tā plašāku lietderību demokrātijas integritātes nodrošināšanai Eiropas Savienībā.

Komisija arī turpinās uzraudzīt un veicināt to saistību īstenošanu, ko platformas ir uzņēmušās **prakses kodeksā dezinformācijas jomā**. Saskaņā ar prakses kodeksu sniegtie *Google*, *Twitter* un *Facebook* ziņojumi liecina, ka visas platformas veica pasākumus pirms Eiropas Parlamenta vēlēšanām, marķējot politiskās reklāmas un padarot tās publiski pieejamas ar reklāmu bibliotēkas meklēšanas funkcijas palīdzību. Tomēr tajā pašā laikā ir iespējami uzlabojumi, kā to konstatējusi Eiropas Audiovizuālo mediju pakalpojumu regulatoru grupa[73]. Proti, joprojām trūkst piekļuves detalizētiem, neapstrādātiem datiem, kas vajadzīgi visaptverošas uzraudzības nolūkā. Visbeidzot, platformām būtu jādod pētniekiem jēgpilna piekļuve datiem atbilstoši personas datu aizsardzības noteikumiem. Šā gada laikā Komisija veiks visaptverošu novērtējumu par to, kā tiek īstenotas visas saskaņā ar prakses kodeksu uzņemtās saistības tā pirmo 12 mēnešu periodā. Pamatojoties uz to, Komisija varētu apsvērt turpmākus pasākumus, tostarp regulatīvus, lai ilgtermiņā uzlabotu ES reakciju uz dezinformāciju.

3. Sagatavotība un aizsardzība

Virzībā uz efektīvu un patiesu drošības savienību svarīgs aspekts ir aizsardzības spēju stiprināšana un izturētspējas veidošana pret drošības apdraudējumiem. Tas ietver atbalstu, ko Komisija sniedz dalībvalstīm un to vietējām iestādēm, lai uzlabotu **sabiedrisko vietu aizsardzību**[74], kā arī atbalstu dalībvalstīm, lai uzlabotu sagatavotību pret **ķīmiskiem, bioloģiskiem, radioloģiskiem un kodoldrošības riskiem**[75], šajā jomā īstenojot divus rīcības plānus, kā arī analizējot attiecīgo reaģēšanas resursu vajadzības, kas jāizveido saskaņā ar *rescEU*[76]. Attiecībā uz jauniem ķīmiskiem apdraudējumiem[77] sadarbībā ar dalībvalstīm un apspriežoties ar starptautiskajiem partneriem, Komisija ir izstrādājusi ķīmisko vielu sarakstu, kas rada vislielākās bažas par ļaunprātīgu to izmantošanu terorisma nolūkos. ES saraksts kalpo par pamatu turpmākam darbam, lai samazinātu šo ķīmisko vielu pieejamību un lai sadarbotos ar ražotājiem atklāšanas spēju uzlabošanas nolūkā.

Ar bezpilota gaisa kuģiem saistītās tehnoloģijas sniedz plašas ekspluatācijas iespējas. Tā kā pēdējos gados strauji paplašinās militāriem, civiliem, komerciāliem un vaļasprieku nolūkiem paredzētu bezpilota gaisa kuģu sistēmu tirgus, droni sniedz ne tikai iespēju, bet arī palielina drošības apdraudējumu kritiskajai infrastruktūrai (tostarp aviācijai), sabiedriskajām telpām un pasākumiem,

---

73 Eiropas Audiovizuālo mediju pakalpojumu regulatoru grupa apvieno valstu neatkarīgu regulatīvo iestāžu vadītājus vai augsta līmeņa pārstāvjus audiovizuālo pakalpojumu jomā, lai konsultētu Komisiju par ES Audiovizuālo mediju pakalpojumu direktīvas īstenošanu (Direktīva 2010/13/ES, (10.3.2010.)). Pēdējā sanāksmē, kas notika 2019. gada 20. un 21. jūnijā Bratislavā, grupa iepazīstināja ar līdz šim paveiktā darba rezultātiem attiecībā uz dezinformāciju, galveno uzmanību pievēršot 2019. gada Eiropas Parlamenta vēlēšanām un ar tām saistītajām politiskās un problēmjautājumos balstītās reklāmas jomām.

74 Sk. sadaļu "Laba prakse publiskām iestādēm un privātiem operatoriem, lai pastiprinātu sabiedrisko vietu drošību", kā tas izklāstīts Astoņpadsmitajā progresa ziņojumā par virzību uz efektīvu un patiesu drošības savienību (COM(2019) 145 final (20.3.2019.)). Tā balstās uz 2017. gada oktobra rīcības plānu sabiedrisko vietu aizsardzības uzlabošanai (COM(2017) 612 final (18.10.2017.)). 2019. gada 5. jūnijā notika operatoru foruma trešā sanāksme ES forumā par sabiedrisko vietu aizsardzību. Tā pulcēja ES dalībvalstu pārstāvjus un privātos sabiedrisko vietu operatorus, ko pārstāvēja 14 Eiropas apvienības, kuras pārstāvēja viesmīlības nozari, izpildītājmākslu, mūziku un izklaidi, tematiskos parkus un atrakcijas, aviāciju, dzelzceļa transportu, tirdzniecības centrus, telekomunikācijas, kā arī privātos drošības dienestus un drošības aprīkojuma ražotājus.

75. Jo īpaši īstenojot 2017. gada oktobra Rīcības plānu, lai uzlabotu sagatavotību pret ķīmiskiem, bioloģiskiem, radioloģiskiem un kodoldrošības riskiem (COM(2017) 610 final (18.10.2017.)).

76 Sk. 12. panta 2. punktu Lēmumā Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu, kas grozīts ar Lēmumu (ES) 2019/420 (13.3.2019.).

77 Sk. Piecpadsmitajā progresa ziņojumā virzībā uz efektīvu un patiesu drošības savienību izklāstītos pastiprinātos pasākumus pret ķīmisko apdraudējumu (COM(2018) 470 final (13.6.2018.)).

sensitīvām vietām un privātpersonām. Eiropā droni ir tikuši izmantoti, lai traucētu aviācijas un tiesībaizsardzības iestāžu operācijām, izpētītu kritisko infrastruktūru un nogādātu kontrabandu cietumos un pāri robežām.

Komisija palīdz dalībvalstīm cīnīties pret pieaugošajiem draudiem, ko droni rada iedzīvotājiem un būtiskām sabiedriskajām funkcijām, nemazinot to lietderīgās izmantošanas iespējas, piemēram, ārkārtas reaģēšanas operācijās. Komisija nesen pieņēma **vienotus ES mēroga noteikumus par dronu drošu ekspluatāciju**[78], lai mazinātu to ļaunprātīgas izmantošanas risku, un šie noteikumi ietver nosacījumus, saskaņā ar kuriem dronu ekspluatanti ir jāreģistrē un jābūt iespējai veikt attālinātu to identificēšanu. Turklāt Komisija atbalsta dalībvalstis, uzraugot dronu radītā apdraudējuma tendences, finansējot attiecīgos pētniecības projektus un spēju veidošanas pasākumus, kā arī veicinot informācijas apmaiņu starp dalībvalstīm un citām ieinteresētajām personām. Lai pastiprinātu šo atbalstu, Komisija 2019. gada 17. oktobrī organizēs augsta līmeņa starptautisku konferenci saistībā ar dronu radīto risku novēršanu.

Reaģējot uz nepieciešamību plaši aplūkot ES politiku attiecībā uz **kritisko infrastruktūru aizsardzību**[79], Komisija 2019. gada 23. jūlijā iepazīstināja ar novērtējumu par Eiropas kritisko infrastruktūru direktīvu[80], kura ir tiesiskais regulējums, lai apzinātu un noteiktu Eiropas kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību. Novērtējumā tika konstatēts, ka apstākļi, kādos Eiropas kritiskās infrastruktūras darbojas, kopš direktīvas stāšanās spēkā ir ievērojami mainījušies, tostarp ņemot vērā norises likumdošanas jomā nozarēs, uz kurām šī direktīva ir īpaši vērsta, piemēram, enerģētikas nozarē[81], un ka šīs direktīvas noteikumi, ņemot vērā mainījušos situāciju, ir tikai daļēji atbilstīgi. Vienlaikus dalībvalstis joprojām atbalsta ES politiku attiecībā uz kritiskās infrastruktūras aizsardzību, kas ievēro subsidiaritāti un nodrošina pievienoto vērtību.

4. Ārējā dimensija

Ņemot vērā to, ka lielākā daļa drošības apdraudējumu, ar ko mūsu Savienība saskaras, ir pārrobežu rakstura apdraudējumi, un tie pastāv pasaules mērogā, sadarbība ar starptautiskām organizācijām un partnervalstīm ārpus ES ir neatņemama daļa no darba virzībā uz efektīvu un patiesu drošības savienību.

Daudzpusējās sadarbības priekšrocību izmantošana ir šo centienu neatņemama sastāvdaļa, un tā ietver ES un ANO sadarbību, kas nesen tika pastiprināta, 2019. gada 24. aprīlī Ņujorkā parakstot **ANO un ES satvaru terorisma apkarošanai** saistībā ar ANO un ES otro augsta līmeņa politisko dialogu par terorisma apkarošanu.[82] Šis satvars veicina sadarbību spēju veidošanas jomā, lai apkarotu terorismu un novērstu un apkarotu vardarbīgu ekstrēmismu Āfrikā, Tuvajos Austrumos un Āzijā. Satvarā ir noteiktas ANO un ES sadarbības jomas un prioritātes līdz 2020. gadam.

Sadarbība drošības jomā ar Rietumbalkāniem ir īpaša reģionāla prioritāte, īstenojot vairākas ar drošību saistītas prioritārās darbības, kas noteiktas 2018. gada Rietumbalkānu stratēģijā[83]. Šajā nolūkā Komisija 2019. gada 4. aprīlī rīkoja pirmo Rietumbalkānu starpaģentūru darba grupas sanāksmi, kurā septiņu ES aģentūru pārstāvji dalījās pieredzē un paplašināja operatīvo sadarbību ar reģiona

78 OV L 152, 11.6.2019. — Komisijas Īstenošanas regula (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu ekspluatācijas noteikumiem un procedūrām.

79 2017. gada ES drošības politikas visaptverošajā novērtējumā (SWD(2017) 278 final (26.7.2017.)) tika norādīts uz vajadzību plaši aplūkot ES kritiskās infrastruktūras aizsardzības politiku.

80 Padomes Direktīvas 2008/114/EK (2008. gada 8. decembris) par to, lai apzinātu un noteiktu Eiropas Kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību, mērķis ir uzlabot kritiskās infrastruktūras aizsardzību Eiropas Savienībā.

81 Jo īpaši Regula (ES) 2017/1938 (2017. gada 25. oktobris) par gāzes piegādes drošības aizsardzības pasākumiem un Regula (ES) 2019/941 (2019. gada 5. jūnijs) par riskgatavību elektroenerģijas sektorā.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final (16.2.2018.).

partneriem, tostarp cīņā pret organizēto noziedzību, terorismu, šaujamieročiem, narkotikām, migrantu kontrabandu un cilvēku tirdzniecību. Kopā ar visām sešām Rietumbalkānu valstīm ir sākti hibrīdriska apsekojumi. Cits konkrēts piemērs sadarbībai ar reģionu ir Eiropas Robežu un krasta apsardzes statusa nolīgums starp ES un Albāniju, kas stājās spēkā 2019. gada 1. maijā, pēc kura drīz sekoja Eiropas Robežu un krasta apsardzes aģentūras vienību izvietošana pie robežas ar Grieķiju. Šis ir pirmais šāds nolīgums ar trešām valstīm un pirmā šāda veida izvietošana. Līdzīgi nolīgumi drīzumā būtu jānoslēdz ar citām reģiona valstīm.

Turklāt 2019. gada jūlijā Albānijā tika izvietots Eiropola sadarbības koordinators, lai turpmāk palīdzētu Albānijas iestādēm to centienos novērst un apkarot organizēto noziedzību. Lai izvērstu cīņu pret šaujamieroču nelikumīgu tirdzniecību, Komisija 2019. gada 27. jūnijā nāca klaja ar novērtējumu attiecībā uz 2015.– 2019. gada rīcības plānu par **šaujamieroču nelikumīgas tirdzniecības** starp Eiropas Savienību un Dienvidaustrumeiropas reģionu **apkarošanu**[84]. Novērtējums liecina par sadarbības pievienoto vērtību, taču tajā ir arī uzsvērts, ka joprojām ir nepieciešami turpmāki pūliņi, piemēram, jāievieš efektīvi valsts koordinācijas centri šaujamieroču jomā vai arī jāsaskaņo informācijas vākšana un ziņošana par šaujamieroču konfiskāciju.

ES tādu pašu prioritāti piešķir **sadarbības** pilnveidošanai **ar Tuvo Austrumu un Ziemeļāfrikas valstīm** drošības jomā. ES ir uzsākusi drošības dialogu ar Tunisiju un Alžīriju. ES un Tunisija 12. jūnijā Tunisā rīkoja trešo dialogu par drošību un terorisma apkarošanu, savukārt 2018. gada 12. novembrī Alžīrā notika otrais ES un Alžīrijas dialogs par drošību un terorisma apkarošanu. Pēc nesen notikušās Asociācijas padomes sanāksmes 27. jūnijā turpinās sarunas par strukturēta drošības dialoga uzsākšanu ar Maroku, un šajā sanāksmē ES un Maroka atzina, ka ir svarīgi padziļināt sadarbību drošības jomā, lai risinātu kopīgas problēmas. Vienlaikus notiek diskusijas par strukturētu dialogu drošības jomā ar Ēģipti, kā to vēl vēlreiz apstiprināja pēdējā ES un Ēģiptes augstāko amatpersonu oficiālajā sanāksmē, kas notika 10. jūlijā Kairā.

Pamatojoties uz Padomes pilnvarojumu, Komisija ir sākusi neoficiālas sarunas ar lielāko daļu **Tuvo Austrumu un Ziemeļāfrikas** valstu nolūkā sākt oficiālas sarunas par starptautisku nolīgumu par personas datu apmaiņu starp Eiropas Savienības Aģentūru tiesībaizsardzības sadarbībai (**Eiropols**) un attiecīgajām **Tuvo Austrumu un Ziemeļāfrikas** valstu kompetentajām iestādēm ar mērķi apkarot smagus noziegumus un terorismu. Šajā sakarībā Komisija arī atbalsta sadarbības vienošanos noslēgšanu tieši starp Eiropolu un partneriestādēm **Tuvajos Austrumos un Ziemeļāfrikas** valstīs, lai izveidotu oficiālu satvaru regulārai sadarbībai stratēģiskajā līmenī.

ES un **Amerikas Savienotās Valstis** ir tuvas stratēģiskās partneres, risinot kopīgus draudus un uzlabojot drošību. Tieslietu un iekšlietu ministru sanāksmē 2019. gada 19. jūnijā ES un Amerikas Savienotās Valstis atkārtoti apstiprināja, ka terorisma apkarošana ir viena no galvenajām to prioritātēm. Attiecībā uz ES un ASV Pasažieru datu reģistra nolīgumu[85] abas puses vēlreiz uzsvēra nolīguma nozīmi un apņēmās 2019. gada septembrī saskaņā ar nolīguma noteikumiem sākt kopīgu izvērtēšanu, lai novērtētu tā īstenošanu. Abas puses arī apņēmās pastiprināt kopīgos centienus terorisma apkarošanā, tostarp paplašinot apmaiņu ar informāciju, kas savākta kauju zonās, lai to izmantotu izmeklēšanas un kriminālvajāšanas nolūkos.

Lai izvērstu šo sadarbību, Komisija kopā ar ES terorisma apkarošanas koordinatoru 2019. gada 10. jūlijā Briselē rīkoja augsta līmeņa darbsemināru par kaujas lauka informāciju. Tajā pulcējās dalībvalstu aizsardzības, iekšlietu un tieslietu ministriju, ASV, Eiropola, *Eurojust* augstākās amatpersonas un starptautisko organizāciju pārstāvji, lai apmainītos ar viedokļiem par kaujas lauka informācijas izmantošanu un kopīgi apsvērtu procesuālās, juridiskās un darbības problēmas, ar kurām pašlaik tie saskaras, cenšoties atklāt teroristus un saukt viņus pie atbildības. Briselē 2019. gada 14. un

[84] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_lv.pdf

[85] OV L 215, 11.8.2012., 5. lpp.

15. maijā ES un ASV rīkoja arī dialogu par spēju veidošanu aizsardzībai pret ķīmisko, radioloģisko un kodolapdraudējumu (*CBRN*), lai koordinētu pūliņus to apdraudējumu mazināšanā, ko rada masu iznīcināšanas ieroči, un par *CBRN* drošības uzlabošanu pasaulē.

Teroristu finansēšanas izsekošanas programmas nolīgums starp ES un Amerikas Savienotajām Valstīm[86] ir spēkā kopš 2010. gada, un tas regulē datu pārsūtīšanu un apstrādi teroristu un viņu tīklu identificēšanas, izsekošanas un vajāšanas nolūkā. Nolīgums ietver garantijas, kas nodrošina ES pilsoņu datu aizsardzību un paredz regulāru "aizsardzības pasākumu, kontroles pasākumu un savstarpējības noteikumu" pārskatīšanu. Kārtējā izvērtējuma ziņojumā[87], kas tika publicēts 2019. gada 22. jūlijā, Komisija norādīja, ka ir pārliecināta, ka nolīgums, tostarp būtiskie tā aizsardzības un kontroles pasākumi, tiek pienācīgi īstenots. Komisija atzinīgi vērtē ASV iestāžu pastāvīgo pārredzamību, apmainoties ar informāciju, tādējādi apliecinot Teroristu finansēšanas izsekošanas programmas vērtību mūsu kopīgajos terorisma apkarošanas centienos. Nolīguma ietvaros sniegtajai informācijai ir bijusi nozīmīga loma, lai sāktu konkrētas izmeklēšanas saistībā ar teroristu uzbrukumiem Eiropas teritorijā, tostarp 2017. gadā Stokholmā, Barselonā un Turku. Dalībvalstis un Eiropols ir sākuši intensīvāk izmantot mehānismu, un Teroristu finansēšanas izsekošanas programmas ietvaros savākto datu rezultātā ir sākts septiņas reizes vairāk izmeklēšanu nekā iepriekšējā pārskata periodā. Nolīguma nākamā kopīgā pārskatīšana ir plānota 2021. gadā.

Attiecībā uz starptautisko sadarbību saistībā ar **pasažieru datu reģistra datu apmaiņu terorisma un smagu noziegumu apkarošanas nolūkā** ES un Kanādas 17. samitā Monreālā 2019. gada 17. un 18. jūlijā ES un Kanāda pauda gandarījumu par to, ka tās ir pabeigušas sarunas par jaunu pasažieru datu reģistra nolīgumu. Kaut arī Kanāda norādīja, ka nolīgums ir juridiski jāpārskata, puses, ņemot vērā šo pārskatīšanu, apņēmās pēc iespējas drīz noslēgt šo nolīgumu, atzīstot šā nolīguma būtisko nozīmi drošības uzlabošanā, vienlaikus nodrošinot privātumu un personas datu aizsardzību. Attiecībā uz spēkā esošo ES un Austrālijas Pasažieru datu reģistra nolīgumu[88] ES grupas apmeklējums Kanberā notiks 2019. gada augustā saistībā ar nolīguma kopīgu pārskatīšanu un kopīgu izvērtēšanu.

Komisija arī kopā ar dalībvalstīm Padomē izstrādā ES nostāju saistībā ar gaidāmo **Starptautiskās civilās aviācijas organizācijas** asamblejas 40. sesiju, kas notiks no 2019. gada 24. septembra līdz 4. oktobrim. Asamblejā tiks noteikta politiskā virzība un sniegti norādījumi Starptautiskās civilās aviācijas organizācijas padomei par tehnisko darbu saistībā ar Starptautiskās civilās aviācijas organizācijas standartiem attiecībā uz pasažieru datu reģistra datu apstrādi. Padome apstiprināja informācijas dokumentu, ko Komisijas sagatavoja, lai izklāstītu Savienības nostāju attiecībā uz pamatprincipiem, uz kuriem vajadzētu balstīt visu turpmāko pasažieru datu reģistru globālos standartus. Informācijas dokuments tiks iesniegts struktūrai attiecībā uz tās locekļiem, kas nav ES dalībvalstis.

VI. SECINĀJUMS

Pateicoties ciešajai Eiropas Parlamenta, Padomes, dalībvalstu un Komisijas sadarbībai, ES pēdējos gados ir guvusi ievērojamus panākumus kopīgajā darbā virzībā uz efektīvu un patiesu drošības savienību, vienojoties par vairākām prioritārām likumdošanas iniciatīvām. Dalībvalstis ar Komisijas atbalstu arī īsteno dažādus neleģislatīvus operatīvos pasākumus, lai uzlabotu drošību visiem iedzīvotājiem. Tajā pašā laikā drošības savienībā joprojām ir vairākas prioritāras iniciatīvas, attiecībā uz kurām abiem likumdevējiem ir jāveic turpmākas darbības, lai novērstu tiešu apdraudējumu. Komisija aicina Eiropas Parlamentu un Padomi veikt nepieciešamos pasākumus, lai panāktu drīzu vienošanos par tiesību aktu priekšlikumiem teroristu propagandas un radikalizācijas tiešsaistē apkarošanai, kiberdrošības uzlabošanai, piekļuves elektroniskiem pierādījumiem atvieglošanai un darba pabeigšanai pie spēcīgāku un viedāku drošības, robežu un migrācijas pārvaldības informācijas

[86] OV L 195, 27.7. 2010., 5. lpp.
[87] COM(2019) 342 final (22.7.2019.).
[88] OV L 186, 14.7.2012., 4. lpp.

sistēmu izveides.

Komisija aicina dalībvalstis ātri un pilnībā īstenot visus tiesību aktus, kas pieņemti drošības savienībā, lai varētu izmantot tās sniegtās iespējas. Turklāt Komisija aicina dalībvalstis turpināt un izvērst svarīgo darbu saistībā ar praktiskiem pasākumiem, lai uzlabotu digitālo infrastruktūru drošību, nepieļautu dezinformāciju un citus kiberiespējotus draudus, pastiprinātu sagatavotību un aizsardzību un nostiprinātu sadarbību ar partneriem ārpus Savienības pret kopīgiem apdraudējumiem. Kopumā minētie pasākumi uzlabo visu iedzīvotāju drošību.