



Briselē, 30.10.2019.
COM(2019) 552 final

**KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, EIROPADOMEI UN
PADOMEI**

Divdesmitais progressa ziņojums par virzību uz efektīvu un patiesu drošības savienību

I. IEVADS

Šis ir divdesmitais ziņojums par turpmāko progresu, kas gūts efektīvas un patiesas drošības savienības izveidē. Tajā ir aplūkotas norises drošības savienības abos pamataspektos: 1) cīņa pret terorismu un organizēto noziedzību un līdzekļiem, kas tos atbalsta, un 2) aizsardzības pasākumu stiprināšana un noturības veidošanai pret šiem draudiem.

Ž. K. Junkera vadītā Komisija jau no paša savas darbības sākuma drošību izvirzīja par vienu no galvenajām prioritātēm. Balstoties uz 2015. gada aprīļa Eiropas Drošības programmu¹ un 2016. gada aprīļa Paziņojumu par virzību uz efektīvu un patiesu drošības savienību², ES pienesums bija rast koordinētu pieeju attiecībā uz teroristu uzbrukumiem un citiem augošiem drošības apdraudējumiem, tādējādi panākot ievērojamu progresu mūsu kolektīvās drošības veicināšanā³. Mēs arvien skaidrāk apzināmies, ka mūsdienu drošības apdraudējumi — gan terorisms, organizētā noziedzība, kiberuzbrukumi, dezinformācija, gan citi jauni kiberapdraudējumi, — skar mūs visus. Tikai strādājot kopā, mēs varam sasniegt tādu kolektīvās drošības līmeni, kādu pamatoti pieprasa un sagaida iedzīvotāji. Šī vienotā izpratne ir pamats progresam virzībā uz efektīvu un patiesu drošības savienību. Ņemot vērā to valsts iestāžu vajadzības, kuru darbs ir saistīts ar drošības garantēšanu iedzīvotājiem, ES līmeņa atbalsts ir vērst uz tādiem likumdošanas un operatīvajiem pasākumiem, kuros kopīga rīcība var uzlabot dalībvalstu drošību. Šis darbs tika veikts ciešā sadarbībā ar Eiropas Parlamentu un Padomi, nodrošinot pilnīgu pārredzamību plašākai sabiedrībai. Šā darba pamatprincips ir pilnīga pamattiesību ievērošana, jo Savienības drošību var garantēt tikai tad, ja iedzīvotāji ir pārliecināti, ka tiek pilnībā ievērotas viņu pamattiesības.

ES ir strādājusi, lai **apkarotu terorismu**, sašaurinot teroristu darbības telpu tādējādi, ka ir ieviesti jauni noteikumi, kas apgrūtina viņiem piekļuvi sprāgstvielām, šaujammieročiem un finansējumam un ierobežo viņu pārvietošanos. ES ir pastiprinājusi **informācijas apmaiņu**, lai nodrošinātu priekšposteņa darbiniekiem, policijas ierēdņiem un robežsargiem efektīvu piekļuvi precīziem un pilnīgiem datiem, pēc iespējas labāk izmantojot esošo informāciju un novēršot informācijas nepilnības un aklos punktus. Ārējo robežu spēcīga aizsardzība ir drošības priekšnoteikums brīvas pārvietošanās telpā, kurā nepastāv iekšējā robežkontrole. Eiropas Parlaments un Padome 2019. gada martā panāca vienošanos par to, ka ir vēl vairāk jānostiprina un pilnībā jānodrošina ar ekipējumu **Eiropas robežu un krasta apsardze**. Paredzams, ka šī jaunā regula stāsies spēkā 2019. gada decembra sākumā. ES ir nodrošinājusi platformu un finansējumu darbiniekiem, kuri strādā vietējās kopienās, lai viņi varētu apmainīties ar paraugpraksi attiecībā uz **radikalizācijas apkarošanu un vardarbīga ekstrēmisma novēršanu**, kā arī ir ierosinājusi jaunus noteikumus nolūkā efektīvi izņemt teroristisku saturu no interneta. ES atbalsts ir palīdzējis **palielināt pilsētu noturību pret uzbrukumiem**, proti, ir izstrādāti rīcības plāni, kā stiprināt sabiedrisko vietu aizsardzību un uzlabot sagatavotību pret ķīmiskiem, bioloģiskiem, radioloģiskiem un kodoldrošības riskiem. ES ir pievērsusies **kiberdrošībai un kiberapdraudējumiem**, ieviešot jaunu ES kiberdrošības stratēģiju un pieņemot attiecīgus tiesību aktus, kā arī vērsties pret **dezinformāciju**, lai labāk aizsargātu vēlēšanas. Turpinās darbs, lai nostiprinātu mūsu **kritiskās digitālās infrastruktūras drošību**, pastiprinot arī sadarbību attiecībā uz **5G tīklu kiberdrošību** visā Eiropā.

Tomēr vēl joprojām ir daudz darāmā. Tiešsaistē straumētais uzbrukums sinagogai un divu pilsoņu nogalināšana Hallē (Vācijā) 2019. gada 9. oktobrī bija šokējošs atgādinājums par draudiem, ko rada labējais vardarbīgais ekstrēmisms un antisemitisms. Šie notikumi bija arī uzskatāms atgādinājums, ka internets tiek ļaunprātīgi izmantots terorisma propagandai un tādēļ ir **vajadzīgi ES mēroga noteikumi teroristiska satura izņemšanai no interneta**. Tieslietu un iekšlietu padomes sanāksmē, kas notika 2019. gada 7. un 8. oktobrī, tika diskutēts par labējo vardarbīgo ekstrēmismu un terorismu, uzsverot

¹ COM(2015) 185 *final* (2015. gada 28. aprīlis).

² COM(2016) 230 *final* (2016. gada 20. aprīlis).

³ Iepriekšējos progresa ziņojumos par virzību uz efektīvu un patiesu drošības savienību sk. vietnē https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

vajadzību turpināt darbu, lai apkarotu arī tāda nelikumīga satura izplatīšanu tiešsaistē un bezaistē, kas popularizē labējo ekstrēmismu. Tajā pašā laikā triju policijas ierēdņu un viena darbinieka nogalināšana Parīzes galvenajā policijas pārvaldē 2019. gada 3. oktobrī pierāda, ka draudi, ko rada džihādistu iedvesmots terorisms, joprojām ir reāli un ir jāturpina nemitīgie centieni atbalstīt dalībvalstis šo apdraudējumu novēršanā. Ieslodzīto *ISIS/Da'esh* kaujinieku izbēgšana saistībā ar nesenajiem notikumiem Ziemeļsīrijā varētu nopietni ietekmēt drošību Eiropā. Ir svarīgi, lai dalībvalstis pilnībā izmantotu esošās informācijas sistēmas ārvalstu kaujinieku teroristu atklāšanai un identificēšanai, kad viņi šķērso ārējās robežas. Notiek arī darbs saistībā ar kaujaslauka informācijas izmantošanu ārvalstu kaujinieku teroristu kriminālvajāšanai.

Šajā ziņojumā ir izklāstīts pēdējā laikā panāktais progress virzībā uz efektīvu un patiesu drošības savienību, jo īpaši pievēršoties jomām, kurās ir vajadzīga turpmāka rīcība. Ziņojumā ir sniegta jaunākā informācija par to, kā tiek īstenoti saskaņotie pasākumi attiecībā uz **5G tīklu kiberdrošību**, jo īpaši saistībā ar 2019. gada 9. oktobrī publicēto **ES Riska novērtējuma ziņojumu**, un attiecībā uz **dezinformācijas apkarošanu**.

Šajā ziņojumā īpaša uzmanība ir pievērsta **ārējai dimensijai** saistībā ar sadarbību drošības savienībā. Šajā jomā jāatzīmē divu divpusējo **vienošanos** parakstīšana ar Albāniju un Ziemeļmaķedonijas Republiku **par terorisma apkarošanu** un progress, kas sadarbībā ar trešo valstu partneriem panākts attiecībā uz **pasāžieru datu reģistra datu apmaiņu**. Turklāt reizē ar šo ziņojumu Komisija pieņēma arī pilnvarojuma pieprasījumu sarunu sākšanai attiecībā uz nolīgumu starp ES un **Jaunzēlandi** par persondatu apmaiņu smagu noziegumu un terorisma apkarošanas jomā.

II. LIKUMDOŠANAS PRIORITĀŠU ĪSTENOŠANA

1. Radikalizācijas novēršana tiešsaistē un kopienās

Radikalizācijas novēršana ir pamatelements, uz kura balstās Savienības rīcība terorisma radīto draudu jomā. Šajā ziņā visnozīmīgākā kaujas platforma teroristu darbībai 21. gadsimtā ir internets. Tas, ka eksistē telpa, kurā radikalizēti indivīdi var sazināties un apmainīties ar saturu, veicina to, ka attīstās gan džihādistu, gan labējo vardarbīgo ekstrēmistu pasaules mēroga tīkli, kas arvien vairāk izplešas. Tāpēc Komisija turpina īstenot savu divējādo pieeju pret radikalizāciju tiešsaistē, proti, ierosinātajiem noteikumiem par nelikumīga teroristiska satura izņemšanu no interneta būtu jāpastiprina brīvprātīgā partnerība ar tiešsaistes platformām.

Lai to izdarītu, svarīga nozīme ir **tiesību akta priekšlikumam par to, kā novērst teroristiska satura izplatīšanu internetā**, kurā paredzēti skaidri noteikumi un drošības pasākumi, saskaņā ar kuriem interneta platformām būtu obligāts pienākums izņemt teroristisku saturu vienas stundas laikā no brīža, kad ir saņemts kompetento iestāžu pamatots pieprasījums, un īstenot proaktīvus pasākumus, kas ir samērīgi ar teroristiskā satura ietekmes līmeni⁴. Norisinās iestāžu sarunas starp Eiropas Parlamentu un Padomi, un pirmā dialoga sanāksme notika 2019. gada 17. oktobrī. Ņemot vērā draudus, ko rada teroristisks saturs internetā, Komisija aicina abus likumdevējus vienoties par ierosināto tiesību aktu līdz 2019. gada beigām.

Ar ierosināto tiesību aktu tiek papildināta brīvprātīgā partnerība ar interneta nozares pārstāvjiem un citām ieinteresētajām personām, kas tiek īstenota **ES Interneta foruma** ietvaros. Minētais forums kopš tā izveides 2015. gadā ir stimulējis interneta uzņēmumus rīkoties proaktīvi, lai identificētu un izņemtu teroristisku saturu no interneta, un, pateicoties tam, ir radusies nozares iniciatīva “koplietojamā *hash* datubāze”⁵ un Globālā interneta foruma terorisma apkarošanai izveidei. Būtisku ieguldījumu, stiprinot sadarbību ar interneta uzņēmumiem un veicinot ES Interneta foruma vispārējo

⁴ COM(2018) 640 *final* (2018. gada 12. septembris).

⁵ Rīks, ko izveidoja uzņēmumu konsorcijs, lai veicinātu sadarbību nolūkā novērst teroristiska satura izplatīšanu platformās.

mērķu sasniegšanu, ir sniegusi ES tiesībsardzības aģentūras (Eiropola) ietvaros izveidotā ES vienība ziņošanai par interneta saturu. Nesenajā ministru sanāksmē par ES Interneta forumu, kas notika 2019. gada 7. oktobrī, ES dalībvalstis un interneta uzņēmumu augstākās vadības pārstāvji apņēmas sadarboties atbilstīgi tā dēvētajam “**ES krīzes protokolam**”. ES krīzes protokolā ir identificēti ciešākas sadarbības robežmērķi un definēti jauni veidi, kā uzlabot reaģēšanu krīzes situācijās. Šie pasākumi ir daļa no starptautiska līmeņa centieniem nolūkā īstenot Kraistcērčas aicinājumu rīkoties⁶, kura mērķis ir nodrošināt koordinētu un ātru reakciju, lai ierobežotu tāda satura lavīnveidīgu izplatīšanos tiešsaistē, kas saistīts ar terorismu vai vardarbīgu ekstrēmismu.

Papildus šiem pasākumiem pret radikalizāciju tiešsaistē Komisija turpina atbalstīt valstu un vietējā līmeņa centienus **novērst un apkarot radikalizāciju tās rašanās vietā**. Ņemot vērā plašo pieredzi un zināšanas, kas apkopotas Radikalizācijas izpratnes tīklā, ES piedāvā mērķtiecīgu atbalstu vietējiem dalībniekiem, tostarp pilsētām⁷, un nodrošina iespējas informācijas apmaiņai starp jomas speciālistiem, pētniekiem un politikas veidotājiem. Piemēram, tīkla ietvaros tika izdotas īpašas pamatnostādnes un tika organizēti darbsemināri, lai atbalstītu kompetentās iestādes darbā ar bērniem, kuri ierodas no konflikta zonām⁸. Lai nodrošinātu Radikalizācijas izpratnes tīklā veikto darbību nepārtrauktību, Komisija ir sākusi procedūru attiecībā uz jauna pamatlīguma noslēgšanu par aptuveno summu 61 miljons EUR uz četrus gadu periodu, sākot no 2020. gada⁹.

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

- līdž gada beigām noslēgt sarunas par tiesību akta priekšlikumu par to, kā novērst **teroristiska satura izplatīšanu internetā**.

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

ES ir intensificējusi informācijas apmaiņu, atvieglojot vēršanos pret identitātes viltošanu¹⁰, pastiprinot robežpārbaudes¹¹, modernizējot Eiropas mēroga tiesībsardzības datubāzes¹², novēršot informācijas

⁶ Reaģējot uz uzbrukumiem Kraistcērčā (Jaunzēlandē) 2019. gada 15. martā, Francijas prezidents Emanuels Makrons un Jaunzēlandes premjerministre Džasinda Ārderna uzaicināja vadītājus un tiešsaistes platformas 2019. gada 15. maijā uz Parīzi, kur iepazīstināja ar Kraistcērčas aicinājumu rīkoties. Komisijas priekšsēdētājs Ž. K. Junkers atbalstīja šo uzaicinājumu un izziņoja, ka tiks sagatavots ES krīzes protokols.

⁷ Attiecībā uz sadarbību ar pilsētām drošības jomā skatīt arī V.2. iedaļu par sagatavotību un aizsardzību, jo īpaši par sabiedrisko vietu aizsardzību.

⁸ https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

⁹ Pamatlīgums ir iedalīts divās daļās: līdzekļi 29 miljonu EUR apmērā ir paredzēti tam, lai atbalstītu Radikalizācijas izpratnes tīkla darbību nākamajos četros gados, bet līdzekļi 32 miljonu EUR apmērā — tam, lai uzlabotu dalībvalstu un valsts, reģionālo un vietējo iestāžu, kā arī prioritāro trešo valstu spējas efektīvi apkarot radikalizāciju, jo īpaši tādējādi, ka tiek piedāvātas tīklošanas iespējas, mērķtiecīgi un vajadzības virzīti pakalpojumi, kā arī pētniecības un analīzes iespējas.

¹⁰ 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.

¹¹ Tādu sistemātisku pārbaudu ieviešana, kuras veic uz ārējām robežām visiem pilsoņiem, izmantojot Šengenas informācijas sistēmu. Visas Šengenas valstis, kā arī Rumānija, Bulgārija, Horvātija un Kipra, piemēro 2017. gada aprīlī ieviestos noteikumus par sistemātiskām pārbaudēm uz ārējām robežām, veicot salīdzināšanu attiecīgajās datubāzēs. Saskaņā ar minētajiem noteikumiem ir iespējamas pagaidu atkāpes uz sauszemes vai jūras robežām, bet tikai attiecībā uz ES pilsoņiem, ņemot vērā nesamērīgo ietekmi uz satiksmes plūsmu. Patlaban par šādām atkāpēm ir paziņojušas sešas dalībvalstis / Šengenas asociētās valstis (Horvātija, Somija, Ungārija, Latvija, Norvēģija un Slovēnija). Attiecībā uz gaisa telpas robežām — termiņš iespējai atkāpties no noteikumiem par sistemātiskām pārbaudēm beidzās 2019. gada aprīlī.

trūkumu¹³ un pastiprinot ES tiesībsardzības aģentūru (Eiropolu)¹⁴. Šajā ziņā īpaša nozīme ir **ES informācijas sistēmu sadarbībai**¹⁵, un tas nozīmē, ka pēc iespējas labāk ir jāizmanto esošās informācijas sistēmas un jānovērš aklie punkti. Reaģējot uz priekšpostenī strādājošo vajadzībām, sadarbība nodrošinās tiesībsardzības amatpersonām, robežsargiem un migrācijas amatpersonām ātrāku un sistemātiskāku piekļuvi informācijai, tādējādi palīdzot uzlabot iekšējo drošību un robežu pārvaldību.

Tomēr sadarbībai un jebkādai ar to saistītai inovācijai būs pozitīva ietekme drošības, robežu un migrācijas pārvaldībā uz vietas tikai tad, ja katra dalībvalsts pilnībā īsteno saistītos tiesību aktus. Tāpēc **sadarbības** īstenošana ir pamatprioritāte drošības savienībā — gan politiskā, gan tehniskā līmenī. Komisija un ES Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*) atbalsta dalībvalstis, nodrošinot speciālās zināšanas un paraugprakses apmaiņu ar valsts koordinatoru tīkla starpniecību un sagatavojot rezultātu pārskatu, kas paver iespēju veikt efektīvus uzraudzības un koordinācijas pasākumus. Cieša sadarbība starp ES aģentūrām, visām dalībvalstīm un Šengenas asociētajām valstīm būs īpaši svarīga virzībā uz vērienīgo mērķi — līdz 2020. gadam panākt ES drošības, robežu un migrācijas pārvaldības informācijas sistēmu pilnīgu sadarbību.

Tajā pašā laikā Eiropas Parlamentam un Padomei šajā saistībā vēl ir **jāpabeidz likumdošanas darbs**. Lai nodrošinātu pilnīgu un savlaicīgu sadarbības izvēršanu, svarīgi ir ātri panākt vienošanos par visiem izskatīšanā esošajiem tiesību aktu priekšlikumiem. Pirmkārt, **Eiropas ceļošanas informācijas un atļauju sistēmas** tehniskās īstenošanas ietvaros ir vajadzīgi tehniski grozījumi saistītajās regulās¹⁶, lai šo sistēmu pilnībā ieviestu. Komisija aicina Eiropas Parlamentu paātrināt tā darbu pie šiem tehniskajiem grozījumiem, lai sāktu iestāžu sarunas, cik drīz vien iespējams. Otrkārt, joprojām notiek iestāžu sarunas par 2018. gada maija priekšlikumu nostiprināt un pilnveidot esošo **vīzu informācijas sistēmu**¹⁷. Pamatojoties uz pirmo dialoga sanākumi, kas notika 2019. gada 22. oktobrī, Komisija aicina abus likumdevējus ātri noslēgt sarunas. Treškārt, vēl joprojām nav panākta vienošanās par Komisijas 2016. maija priekšlikumu paplašināt pirkstu nospiedumu salīdzināšanas sistēmas **Eurodac** darbības jomu¹⁸, lai tajā tiktu glabāti pirkstu nospiedumi un personas dati ne vien par patvēruma pieteikumu iesniedzējiem un personām, kas aizturētas saistībā ar nelikumīgu ārējās robežas šķērsošanu, bet arī par trešo valstu valstspiederīgajiem, kas valstī uzturas nelikumīgi. Ar ierosinātajām izmaiņām tiktu arī pagarināts ES nelikumīgi ieceļojušo personu pirkstu nospiedumu un būtisko datu glabāšanas termiņš. Komisija aicina abus likumdevējus pieņemt šo priekšlikumu.

¹² Pastiprinātā Šengenas informācijas sistēma (Regulas (ES) 2018/1860, (ES) 2018/1861, (ES) 2018/1862 (visas — 2018. gada 28. novembris)) un Eiropas Sodāmības reģistru informācijas sistēma, kas paplašināta, to attiecinot arī uz trešo valstu valstspiederīgajiem (Regula (ES) 2019/816 (2019. gada 17. aprīlis)). Šengenas informācijas sistēmas pastiprināšana ietver vispārēju pienākumu ievadīt šajā sistēmā ar terorismu saistītus brīdinājumus.

¹³ ES ieceļošanas/izceļošanas sistēma (Regula (ES) 2017/2226 (2017. gada 30. novembris)) un Eiropas ceļošanas informācijas un atļauju sistēma (Regulas (ES) 2018/1240 un (ES) 2018/1241 (abas — 2018. gada 12. septembris)).

¹⁴ Pēdējos gados Eiropola loma ir ievērojami palielinājusies gan tvēruma, gan pamatīguma ziņā. Aģentūra ir nostiprināta, 2016. gadā pieņemot Eiropola regulu (Regula (ES) 2016/794 (2016. gada 11. maijs)). Dalībvalstis ir ievērojami palielinājušas tās informācijas apjomu, kurā tās dalās ar Eiropolu un kurā tās dalās ar Eiropola starpniecību. Eiropola Terorisma apkarošanas centra (*ECTC*) izveide ir nostiprinājusi Eiropola analītiskās spējas terorisma gadījumos. Eiropola budžets pēdējos gados ir pastāvīgi palielinājies — no 82 miljoniem EUR 2014. gadā līdz 138 miljoniem EUR 2019. gadā. Norisinās sarunas par 2020. gada budžetu.

¹⁵ Regulas (ES) 2019/817 un (ES) 2019/818 (abas — 2019. gada 20. maijs).

¹⁶ Regulas (ES) 2018/1240 un (ES) 2018/1241 (abas — 2018. gada 12. septembris).

¹⁷ COM(2018) 302 *final* (2018. gada 16. maijs).

¹⁸ COM(2016) 272 *final* (2016. gada 4. maijs).

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

- turpināt darbu, lai panāktu drīzu vienošanos par ierosinātajiem tehniskajiem grozījumiem, kas vajadzīgi, lai izveidotu **Eiropas ceļošanas informācijas un atļauju sistēmu**;
- ātri risināt un noslēgt sarunas par priekšlikumu nostiprināt esošo **vīzu informācijas sistēmu**;
- pieņemt tiesību akta priekšlikumu par **Eurodac** (*Kopīgajā paziņojumā paredzēta prioritāte*).

3. Teroristu darbības telpas sašaurināšana

ES ir apņēmīgi rīkojusies, lai sašaurinātu teroristu darbības telpu, ieviešot jaunus noteikumus, kas apgrūtina teroristiem un citiem noziedzniekiem piekļuvi sprāgstvielām¹⁹, šaujammieročiem un finansējumam²⁰ un ierobežo viņu pārvietošanos²¹.

Lai pastiprinātu tiesu sistēmas reakciju uz terorismu, ES Aģentūra tiesu iestāžu sadarbībai krimināllietās (*Eurojust*) 2019. gada 1. septembrī izveidoja **Eiropas tiesu iestāžu reģistru terorisma apkarošanai**. Reģistrā tiks apkopota tiesu iestāžu informācija, kas ļaus noteikt saiknes tiesvedībā pret personām, kuras tiek turētas aizdomās par terorisma noziegumiem, tādējādi pastiprinot prokuroru savstarpējo koordināciju ar terorisma apkarošanu saistītās izmeklēšanās, kurām var būt pārrobežu ietekme.

Tomēr ir jāturpina centieni, lai atbalstītu un veicinātu izmeklēšanu pārrobežu lietās, jo īpaši saistībā ar tiesībsardzības iestāžu **piekļuvi elektroniskiem pierādījumiem**. Attiecībā uz 2018. gada aprīļa tiesību aktu priekšlikumiem, kuru mērķis ir uzlabot pārrobežu piekļuvi elektroniskiem pierādījumiem kriminālizmeklēšanā²², Eiropas Parlamentam vēl ir jāpieņem sava sarunu nostāja, pirms likumdevēji var sākt sarunas. Komisija aicina Eiropas Parlamentu virzīties uz priekšu darbā ar šo tiesību akta priekšlikumu, lai likumdevēji varētu to ātri pieņemt. Komisija, pamatojoties uz savu priekšlikumu par ES iekšējiem noteikumiem, arī iesaistās **starptautiskās sarunās**, lai uzlabotu pārrobežu piekļuvi elektroniskiem pierādījumiem. Komisija un Amerikas Savienoto Valstu iestādes 2019. gada 25. septembrī organizēja pirmo oficiālo sarunu kārtu par **ES un ASV nolīgumu attiecībā uz pārrobežu piekļuvi elektroniskiem pierādījumiem**. Nākamā kārtā ir iepļānota 2019. gada 6. novembrī. Saistībā ar notiekošajām sarunām par **Eiropas Padomes Budapeštas Konvencijas par kibernetiskajiem noziedzīgiem darbiem papildu protokolu** Komisija Savienības vārdā piedalījās trijās sarunu sesijās — 2019. gada jūlijā, septembrī un oktobrī. Lai gan šajās sarunās ir gūti labi panākumi, vēl joprojām ir jāapspriež vairāki nozīmīgi jautājumi, par kuriem Savienībai ir ievērojama interese, piemēram, datu aizsardzības pasākumi. Sarunas par otro papildu protokolu turpināsies 2019. gada novembrī un visu 2020. gadu. Ir svarīgi strauji risināt abas sarunas, lai veicinātu starptautisko sadarbību saistībā ar elektronisko pierādījumu apmaiņu, vienlaikus nodrošinot saderību ar ES tiesību aktiem un dalībvalstu pienākumiem saskaņā ar tiem, ņemot vērā arī turpmākās izmaiņas ES tiesību aktos.

Atspoguļojot pastāvīgās bažas par nelikumīgi iegūtu līdzekļu legalizāciju, Eiropas Parlaments 2019. gada 19. septembrī pieņēma **rezolūciju par to, kā tiek īstenoti Savienības tiesību akti noziedzīgi iegūtu līdzekļu legalizēšanas novēršanas jomā**²³, tādējādi atbildot uz četru ziņojumu kopumu par nelikumīgi iegūtu līdzekļu legalizēšanas novēršanu, kurus Komisija pieņēma 2019. gada

¹⁹ Regula (ES) 2019/1148 (2019. gada 20. jūnijs) par sprāgstvielu prekursoru tirdzniecību un lietošanu. Regula stājas spēkā 2019. gada 31. jūlijā, un tās piemērošana sāksies 18 mēnešus pēc tās stāšanās spēkā.

²⁰ Direktīva (ES) 2019/1153 (2019. gada 11. jūlijs), ar ko paredz noteikumus, lai atvieglotu finanšu un citas informācijas izmantošanu noteiktu noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai kriminālvajāšanai par tiem.

²¹ Tādu sistematisku pārbažu ieviešana, kuras veic uz ārējām robežām visiem pilsoņiem, izmantojot Šengenas informācijas sistēmu.

²² COM(2018) 225 *final* un COM(2018) 226 *final* (abi — 2018. gada 17. aprīlis).

²³ https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_LVtml

24. jūlijā²⁴. Eiropas Parlaments aicināja dalībvalstis nodrošināt, ka pienācīgi un ātri tiek īstenotas nelikumīgi iegūtu līdzekļu legalizēšanas novēršanas direktīvas. Eiropas Parlaments arī aicināja Komisiju novērtēt, vai nelikumīgi iegūtu līdzekļu legalizēšanas novēršanas regula būtu piemērotāka nekā direktīva un vai finanšu ziņu vākšanas vienībām ir vajadzīgs koordinācijas un atbalsta mehānisms.

Lai uzlabotu tiesībsardzības iestāžu piekļuvi elektroniskajiem pierādījumiem, Komisija aicina Eiropas Parlamentu un Padomi:

- ātri vienoties par tiesību aktu priekšlikumiem attiecībā uz **elektroniskajiem pierādījumiem** (*Kopīgajā paziņojumā paredzēta prioritāte*).

4. Kiberdrošības uzlabošana

Kiberdrošības uzlabošana joprojām ir būtisks darbības aspekts virzībā uz patiesu un efektīvu drošības savienību. Īstenojot ES 2017. gada Kiberdrošības stratēģiju²⁵, Savienība ir pastiprinājusi savu noturību, nodrošinot, ka tai ir grūtāk uzbrukt un tā var ātrāk atkopties, kā arī kiberatturēšanu, palielinot iespējas, ka uzbrucēji tiks aizturēti un sodīti, tostarp īstenojot kopīgu ES diplomātisko atbildes reakciju uz ļaunprātīgām kiberdarbībām. Savienība arī atbalsta dalībvalstis kiberaizsardzībā, īstenojot ES kiberaizsardzības politikas satvaru²⁶.

Līdz ar Kiberdrošības akta²⁷ stāšanos spēkā 2019. gada jūnijā konkrētas aprises sāk iegūt **ES kiberdrošības sertifikācijas sistēma**. Sertifikācijai ir izšķiroša loma, lai palielinātu uzticēšanos produktiem un pakalpojumiem, kuri ir būtiski digitālajam vienotajam tirgum, un lai palielinātu to drošību. Sertifikācijas sistēma nodrošinās ES mēroga sertifikācijas shēmas, kas izpaudīsies kā noteikumu, tehnisko prasību, standartu un procedūru visaptverošs kopums. Tajā ir iesaistītas divas ekspertu grupas, proti, Eiropas Kiberdrošības sertifikācijas grupa, kas pārstāv dalībvalstu iestādes, un Ieinteresēto personu kiberdrošības sertifikācijas grupa, kas pārstāv nozari. Otrā minētā grupa apvieno informācijas un komunikācijas tehnoloģiju produktu un pakalpojumu pieprasījuma un piedāvājuma puses pārstāvjus, tostarp mazos un vidējos uzņēmumus, digitālo pakalpojumu sniedzējus, Eiropas un starptautiskās standartizācijas iestādes, valstu akreditācijas iestādes, datu aizsardzības uzraudzības iestādes un atbilstības novērtēšanas iestādes.

Tajā pašā laikā Eiropas Parlamentam un Padomei vēl ir jāvienojas par likumdošanas iniciatīvu²⁸ attiecībā uz **Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu**. Šā priekšlikuma mērķis ir nostiprināt Savienības kiberdrošības spējas, stimulējot Eiropas tehnoloģisko un rūpniecisko kiberdrošības ekosistēmu, kā arī koordinējot un apvienojot saistītos resursus. Komisija aicina abus likumdevējus atsākt un ātri pabeigt savstarpējās iestāžu sarunas par šo prioritāro iniciatīvu, lai uzlabotu kiberdrošību.

²⁴ Ziņojums par novērtējumu attiecībā uz pārrobežu darbībām piemītošajiem nelikumīgi iegūtu līdzekļu legalizācijas un terorisma finansēšanas riskiem, kuri skar iekšējo tirgu (COM(2019) 370, 2019. gada 24. jūlijs), Ziņojums par dalībvalstu bankas kontu centralizētu automatizētu valsts mēroga mehānismu (centrālo reģistru vai centrālo elektronisko datu izguves sistēmu) savstarpējo savienojamību (COM(2019) 372 *final*, 2019. gada 24. jūlijs), Ziņojums par tādu neseno iespējamās nelikumīgi iegūtu līdzekļu legalizācijas gadījumu novērtēšanu, kuros iesaistītas ES kredītiestādes (COM(2019) 373 *final*, 2019. gada 24. jūlijs), Ziņojums, ar ko novērtē finanšu ziņu vākšanas vienību sadarbības sistēmu (COM(2019) 371 *final*, 2019. gada 24. jūlijs).

²⁵ JOIN(2017) 450 *final* (2017. gada 13. septembris).

²⁶ ES kiberaizsardzības politikas satvars (2018. gada atjauninājums), ko Padome pieņēmusi 2018. gada 19. novembrī (14413/18).

²⁷ Regula (ES) 2019/881 (2019. gada 17. aprīlis).

²⁸ COM(2018) 630 *final* (2018. gada 12. septembris).

Kiberdrošības uzlabošanas darbs ietver atbalstu gan valsts, gan reģionālā līmenī²⁹.

Papildus kiberdraudiem, kas vērsti pret sistēmām un datiem, ES turpina risināt sarežģītās un daudzšķautņainās **hibrīddraudu** radītās problēmas. Padomē tika izveidota horizontāla darba grupa hibrīddraudu apkarošanai, lai uzlabotu ES un tās dalībvalstu noturību pret hibrīddraudiem un atbalstītu rīcību sabiedrības krīžu izturētspējas nostiprināšanai. Komisija un Eiropas Ārējās darbības dienests atbalsta šos centienus saskaņā ar 2016. gada Kopīgo regulējumu hibrīddraudu apkarošanai³⁰ un 2018. gada Kopīgo paziņojumu³¹ par noturības un spēju palielināšanu cīņā pret hibrīddraudiem. Turklāt Kopīgais pētniecības centrs (*JRC*) izstrādā “konceptuālu pamatmodeli” hibrīddraudu raksturošanai, lai palīdzētu dalībvalstīm un to kompetentajām iestādēm identificēt hibrīduzbrukuma veidu, ja pret tām tiktu vērsts šāds uzbrukums. Minētajā modelī tiek aplūkots veids, kā (valsts vai nevalstisks) dalībnieks mērķa ietekmēšanai izmanto vairākus rīku kopumus (sākot no dezinformēšanas un beidzot ar spiegošanu vai fiziskām operācijām) dažādās jomās (ekonomikas, militārajā, sociālajā, politiskajā), lai sasniegtu virkni mērķu.

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**.

III. DIGITĀLO INFRASTRUKTŪRU DROŠĪBAS UZLABOŠANA

Piektās paaudzes (5G) tīkli būs pamats nākotnes ekonomikai un sabiedrībai, kas kļūst arvien digitalizētāka. Runa ir par miljardiem savienotu objektu un sistēmu, tostarp tādās svarīgās nozarēs kā enerģētika, transports, banku pakalpojumi un veselības aprūpe, kā arī rūpnieciskās vadības sistēmas, kas rīkojas ar sensitīvu informāciju, un atbalstošās drošības sistēmas. Tāpēc ir svarīgi nodrošināt 5G tīklu kiberdrošību un noturību.

Īstenojot koordinētu pieeju, dalībvalstis ar Komisijas un Eiropas Kiberdrošības aģentūras atbalstu 2019. gada 9. oktobrī publicēja ziņojumu par **ES koordinēto riska novērtējumu attiecībā uz kiberdrošību 5G tīklos**³². Šis nozīmīgais ziņojums tika sagatavots kā daļa no pasākumiem, kas jāīsteno saistībā ar Komisijas 2019. gada marta ieteikumu nodrošināt augstu 5G tīklu kiberdrošības līmeni visā ES³³. Ziņojuma pamatā ir visu dalībvalstu veikto valsts kiberdrošības riska novērtējumu rezultāti. Tajā ir identificēti galvenie apdraudējumi un to radītāji, jutīgākie aktīvi, galvenie neaizsargātības aspekti (tostarp tehniskās un cita veida neaizsargātības aspekti) un vairāki stratēģiskie riski. Minētais novērtējums nodrošina pamatu to riska mazināšanas pasākumu noteikšanai, kurus var piemērot valsts un Eiropas līmenī.

Ziņojumā ir identificētas vairākas svarīgas **kiberdrošības problēmas**, kas, visticamāk, radīsies vai kļūs pamanāmākas saistībā ar 5G tīkliem. Šīs drošības problēmas ir saistītas galvenokārt ar būtiskākajām *inovācijām* 5G tehnoloģijas jomā, jo īpaši programmatūras nozīmīgumu un ar 5G iespējoto pakalpojumu un lietojumprogrammu plašo klāstu, kā arī ar *piegādātāju* lomu 5G tīklu izveidē un ekspluatācijā un to, cik liela ir atkarība no individuāliem piegādātājiem. Tas nozīmē, ka piegādātāju produkti, pakalpojumi un darbības arvien biežāk kļūst par daļu no “uzbrukuma tvēruma”

²⁹ Piemēram, Komisija atbalsta reģionu inovācijas partnerību kiberdrošības jomā, kurā iesaistīti tādi reģioni kā Britānija, Kastīlija un Leona, Ziemeļreina-Vestfālēne, centrālā Somija un Igaunija, lai attīstītu Eiropas kiberdrošības vērtību ķēdi, jo īpaši pievērsoties komercializācijai un izvēršanai.

³⁰ JOIN(2016) 18 *final* (2016. gada 6. aprīlis).

³¹ JOIN(2018) 16 *final* (2018. gada 13. jūnijs).

³² ES koordinēto riska novērtējumu par kiberdrošību 5G tīklos veica kompetento iestāžu sadarbības grupa, kas izveidota saskaņā ar Direktīvu par tīklu un informācijas sistēmu drošību (Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs)), ar Komisijas un Eiropas Kiberdrošības aģentūras palīdzību: <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.

³³ C(2019) 2355 *final* (2019. gada 26. marts).

attiecībā uz 5G tīkliem. Turklāt īpaši būtiska nozīme būs individuālu piegādātāju riska profilam, tostarp iespējamībai, ka pret piegādātāju tiek vērsta iejaukšanās no trešās valsts.

Atbilstoši procesam, kas noteikts Komisijas 2019. gada marta ieteikumā, dalībvalstīm līdz 2019. gada 31. decembrim būtu jāvienojas par **riska mazināšanas pasākumu kopumu**, lai novērstu identificētos kibernetikas riskus valstu un Savienības līmenī. Komisija un Eiropas Ārējās darbības dienests arī turpinās apmainīties ar informāciju ar līdzīgi domājošiem partneriem par 5G tīklu kibernetiku un noturību. Šajā ziņā Komisija sazinās ar NATO saistībā ar ES koordinēto riska novērtējumu par 5G tīklu kibernetiku.

IV. DEZINFORMĀCIJAS NOVĒRŠANA UN VĒLĒŠANU AIZSARDZĪBA PRET CITIEM KIBERAPDRAUDĒJUMIEM

ES ir izveidojusi **sistēmu koordinētai rīcībai pret dezinformāciju**, pilnībā ievērojot Eiropas vērtības un pamattiesības³⁴. Saskaņā ar Rīcības plānu dezinformācijas apkarošanai³⁵ turpinās darbs, lai slēgtu dezinformācijas telpu, arī nolūkā aizsargāt vēlēšanu integritāti.

Šajā sakarā galvenā nozīme ir sadarbībai ar nozari, izmantojot pašregulējošo **ES prakses kodeksu dezinformācijas jomā** attiecībā uz tiešsaistes platformām un reklāmas nozari, kas ir jāpiemēro no 2018. gada oktobra³⁶. Komisija ir novērtējusi minētā kodeksa efektivitāti pēc tā pirmā darbības gada, par pamatu izmantojot gada pašnovērtējuma ziņojumus, kurus iesniedza tiešsaistes platformas un citi kodeksa parakstītāji un kuri ir publicēti 2019. gada 29. oktobrī kopā ar Komisijas paziņojumu³⁷. Ziņojumi kopumā apliecina, ka parakstītāji patiešām cenšas īstenot savas saistības.

To platformu, kas parakstīja kodeksu, veiktās darbības visos piecos kodeksa saistību pīlāros atšķiras gan tempa, gan tvēruma ziņā. Kopumā lielāks progress ir panākts, ievērojot saistības attiecībā uz 2019. gada Eiropas vēlēšanām, proti, saistības pārtraukt reklāmas un monetizācijas stimulus, kas paredzēti dezinformācijai (1. pīlārs), nodrošināt politiskās reklāmas un problēmjautājumus balstītas reklāmas pārredzamību (2. pīlārs) un nodrošināt pakalpojumu noturību pret neautentiskiem kontiem un rīcību (3. pīlārs). Savukārt mazāks vai nepietiekams progress ir vērojams attiecībā uz saistībām palielināt patērētāju tiesības (4. pīlārs) un saistībām palielināt pētniecības aprindu tiesības, cita starpā nodrošinot platformas pamatotai un privātuma noteikumiem atbilstīgai piekļuvei datu kopām pētniecības nolūkos (5. pīlārs). Atšķiras arī to darbību tvērums, kuras veic katra platforma, lai nodrošinātu savu saistību īstenošanu, kā arī dalībvalstīs individuālas politikas tiek izvērstas atšķirīgi. Komisija turpina sadarboties ar šā kodeksa parakstītājiem un citām ieinteresētajām personām, lai pastiprinātu pret dezinformāciju vērsto rīcību.

Saskaņā ar Rīcības plānu dezinformācijas apkarošanai Komisija un Augstā pārstāve, sadarbojoties ar dalībvalstīm, izveidoja **agrīnās brīdināšanas sistēmu**, lai vērstos pret dezinformācijas kampaņām. Agrīnās brīdināšanas sistēma sniedza iespēju ES iestādēm un dalībvalstīm dalīties ar informāciju un

³⁴ Sk. Rīcības plānu dezinformācijas apkarošanai (JOIN(2018) 36 *final*, 2018. gada 5. decembris).

³⁵ JOIN(2019) 12 *final* (2019. gada 14. jūnijs).

³⁶ Saskaņā ar minēto kodeksu tiešsaistes platformas *Google, Facebook, Twitter* un *Microsoft* ir apņēmušās nepieļaut, ka to pakalpojumus manipulatīvi izmanto dalībnieki ar ļaunprātīgiem nolūkiem, nodrošināt politisko reklāmu pārredzamību un publiskošanu, kā arī veikt citas darbības, lai uzlabotu tiešsaistes ekosistēmas pārredzamību, pārskatbilstību un uzticamību. Arī reklāmas nozares arodasociācijas ir apņēmušās sadarboties ar platformām, lai uzlabotu izvietoto reklāmu rūpīgu pārbaudi un attīstītu zīmolu drošības rīkus, kuru mērķis ir ierobežot dezinformāciju veicinošu reklāmu izvietošanu tīmekļa vietnēs.

³⁷ https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166. Papildus *Google, Facebook, Twitter* un *Microsoft* kodeksu parakstīja arī *Mozilla*, septiņas Eiropas līmeņa vai valsts līmeņa asociācijas, kas pārstāv reklāmas nozari, un *EDiMA* — Eiropas asociācija, kas pārstāv platformas un citus tehnoloģiju uzņēmumus, kuri darbojas tiešsaistes sektorā.

analīzes rezultātiem pirms Eiropas Parlamenta vēlēšanām 2019. gadā un koordinēt atbildes pasākumus. Pēc vēlēšanām šis darbs ir kļuvis vēl intensīvāks, proti, katru dienu tiek rīkota informācijas apmaiņa darba līmenī, kā arī dažādas dalībvalstis organizēja trīs ātrās brīdināšanas sistēmas kontaktpunktu sanāksmes.

Vēl viens praktisks solis dezinformēšanas identificēšanas virzienā bija darbs, ko veica **Stratēģiskās komunikācijas komanda** (“*StratComms*”) un jo īpaši tās Austrumu stratēģiskās komunikācijas darba grupa, kas vadīja projektu “*EUvsDisinfo*”, lai uzraudzītu un analizētu prokremlisko dezinformāciju un veiktu attiecīgus atbildes pasākumus³⁸. Kopš 2019. gada sākuma ar pirmo speciālo budžetu 3 miljonu EUR apmērā tika nodrošināta iespēja intensificēt un paplašināt šo darbu, lai ietvertu uzraudzību un analīzi attiecībā uz prokremlisko dezinformāciju tīmeklī, pārraidēs un sociālajos plašsaziņas līdzekļos 19 valodās, sākot no angļu valodas un beidzot ar serbu un arābu valodu. Uzlabojoties uzraudzības jaudai, atklāto dezinformācijas darbību skaits palielinājās vairāk nekā divas reizes — līdz šim 2019. gadā ir atklāti aptuveni 2000 dezinformācijas gadījumu salīdzinājumā ar 765 gadījumiem tajā pašā laikposmā 2018. gadā. Austrumu stratēģiskās komunikācijas darba grupai bija būtiska loma saistībā ar to, lai tiktu uzraudzīta un atklāta pret Eiropas Parlamenta 2019. gada vēlēšanām vērstā prokremliskā dezinformācija. Šī izpēte tika rīkota vienlaikus ar informatīvu kampaņu par mēģinājumiem iejaukties vēlēšanu procesos visā pasaulē. Izpētē, ko minētā grupa īstenoja ciešā sadarbībā ar Eiropas Parlamentu un Komisiju, tika veiktas vairāk nekā 20 plašsaziņas līdzekļu intervijas, savukārt kampaņā iesaistījās vairāk nekā 300 žurnālistu.

Komisija ir arī rīkojusies, lai **mazinātu dezinformācijas un mītu izplatīšanu par ES iestādēm un politiku**. Komisija ir izveidojusi komunikācijas ekspertu tīklu un tiešsaistes portālu, kurā tiek nodrošināts interaktīvs informācijas materiāls par ES politiku un par izaicinājumiem, ko rada dezinformācija, kā arī par dezinformācijas ietekmi uz sabiedrību. Sadarbojoties ar Eiropas Parlamentu un Eiropas Ārējās darbības dienestu, Komisija ir arī sākusi vairākas kampaņas sociālajos plašsaziņas līdzekļos, kas vērstas uz dezinformācijas apkarošanu³⁹.

V. CITU PRIORITĀRO DROŠĪBAS JOMAS PASĀKUMU ĪSTENOŠANA

1. Likumdošanas pasākumu īstenošana drošības savienībā

Saskaņotie pasākumi drošības savienībā sniegs maksimālu ieguvumu drošībai tikai tad, ja visas dalībvalstis garantēs to ātru un pilnīgu īstenošanu. Tālab Komisija aktīvi atbalsta dalībvalstis ES tiesību aktu īstenošanā, arī nodrošinot finansējumu un veicinot paraugprakses apmaiņu. Komisija pilnībā izmanto savas Līgumos paredzētās pilnvaras ES tiesību aktu īstenošanai, tostarp vajadzības gadījumā arī pienākumu neizpildes procedūras.

ES pasažieru datu reģistra direktīvas⁴⁰ transponēšanas termiņš bija 2018. gada 25. maijs. Līdz šim 25 dalībvalstis ir paziņojušas par pilnīgu transponēšanu⁴¹ — tas ir ievērojams progress kopš 2018. gada jūlija, kad Komisija sāka pienākumu neizpildes procedūras pret 14 dalībvalstīm⁴². Divas dalībvalstis vēl nav paziņojušas par pilnīgu transponēšanu, lai gan pret tām notiek pienākumu neizpildes procedūras, kas sāktas 2018. gada 19. jūlijā⁴³. Vienlaikus Komisija turpina atbalstīt visu dalībvalstu pūliņus pabeigt savu pasažieru datu reģistra sistēmu izstrādi, tostarp veicinot informācijas

³⁸ www.euvdisinfo.eu.

³⁹ <https://europa.eu/euprotects/>.

⁴⁰ Direktīva (ES) 2016/681 (2016. gada 27. aprīlis). Dānija nepiedalījās šīs direktīvas pieņemšanā, un tai šī direktīva nav saistoša un nav jāpiemēro.

⁴¹ Atsaucēs uz pilnīgas transponēšanas paziņojumu tiek ņemtas vērā dalībvalstu deklarācijas, un tās neskar Komisijas dienestu veikto transponēšanas pārbaudi (stāvoklis 2019. gada 17. oktobrī).

⁴² Sk. sešpadsmito progresa ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2018) 690 *final*, 2018. gada 10. oktobris).

⁴³ Slovēnija paziņoja par daļēju transponēšanu. Spānija nav paziņojusi par transponēšanu (stāvoklis 2019. gada 17. oktobrī).

un paraugprakses apmaiņu.

Direktīvas par terorisma apkarošanu⁴⁴ transponēšanas termiņš bija 2018. gada 8. septembris. Līdz šim 22 dalībvalstis ir paziņojušas par pilnīgu transponēšanu — tas ir ievērojams progress kopš 2018. gada novembra, kad Komisija sāka pienākumu neizpildes procedūras pret 16 dalībvalstīm⁴⁵. Trīs dalībvalstis vēl nav paziņojušas par pilnīgu transponēšanu, lai gan pret tām notiek pienākumu neizpildes procedūras⁴⁶. Komisija 2019. gada 25. jūlijā nosūtīja pamatotus atzinumus divām dalībvalstīm par to, ka tās nebija paziņojušas par šīs direktīvas pilnīgu transponēšanu⁴⁷. Atbildot abas dalībvalstis paziņoja, ka likumdošanas darbs tiks pabeigts līdz šā gada beigām.

Direktīvas par ieroču iegādes un turēšanas kontroli⁴⁸ transponēšanas termiņš bija 2018. gada 14. septembris. Par pilnīgu transponēšanu līdz šim ir paziņojušas 13 dalībvalstis. Piecpadsmit dalībvalstis vēl nav paziņojušas par pilnīgu transponēšanu, lai gan pret tām notiek pienākumu neizpildes procedūras, kas sāktas 2018. gada 22. novembrī⁴⁹. Komisija 2019. gada 25. jūlijā nosūtīja pamatotus atzinumus 20 dalībvalstīm par to, ka tās nebija paziņojušas par direktīvas pilnīgu transponēšanu. Atbildot piecas dalībvalstis paziņoja par šīs direktīvas pilnīgu transponēšanu⁵⁰.

Direktīvas par datu aizsardzību tiesībaizsardzības jomā⁵¹ transponēšanas termiņš bija 2018. gada 6. maijs. Līdz šim 25 dalībvalstis ir paziņojušas par pilnīgu transponēšanu — tas ir ievērojams progress kopš 2018. gada jūlija, kad Komisija sāka pienākumu neizpildes procedūras pret 19 dalībvalstīm⁵². Trīs dalībvalstis vēl nav paziņojušas par pilnīgu transponēšanu, lai gan pret tām notiek pienākumu neizpildes procedūras⁵³. Komisija 2019. gada 25. jūlijā nolēma iesūdzēt divas dalībvalstis⁵⁴ Eiropas Savienības Tiesā par direktīvas netransponēšanu un nosūtīja oficiālu vēstuli vienai dalībvalstij⁵⁵ par to, ka tā nebija pilnīgi transponējusi direktīvu⁵⁶.

Komisija izvērtē, kā tiek transponēta **Ceturrtā direktīva par nelikumīgi iegūtu līdzekļu legalizācijas novēršanu**⁵⁷, vienlaikus arī pārbaudot, vai dalībvalstis ir īstenojušas noteikumus. Dalībvalstīm minētā direktīva bija jātransponē valsts tiesību aktos līdz 2018. gada 26. jūnijam. Komisija īsteno pienākumu neizpildes procedūras pret 21 dalībvalsti, jo konstatēja, ka no dalībvalstīm saņemtie paziņojumi

⁴⁴ Direktīva (ES) 2017/541 (2017. gada 15. marts). Direktīva nav piemērojama Apvienotajā Karalistē, Īrijā un Dānijā.

⁴⁵ Sk. septiņpadsmito progresa ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2018) 845 *final*, 2018. gada 11. decembris).

⁴⁶ Grieķija un Luksemburga nav paziņojušas par valsts īstenošanas pasākumiem. Polija ir paziņojusi par valsts pasākumiem, t. i., par daļēju transponēšanu (stāvoklis 2019. gada 17. oktobrī).

⁴⁷ Grieķija un Luksemburga.

⁴⁸ Direktīva (ES) 2017/853 (2019. gada 17. oktobris).

⁴⁹ Apvienotā Karaliste, Beļģija, Čehija, Igaunija, Polija, Slovākija un Zviedrija ir paziņojušas par transponēšanas pasākumiem attiecībā uz daļu no jaunajiem noteikumiem. Grieķija, Kipra, Luksemburga, Rumānija, Slovēnija, Spānija, Ungārija un Vācija nav paziņojušas par transponēšanas pasākumiem (stāvoklis 2019. gada 17. oktobrī).

⁵⁰ Īrija, Lietuva, Nīderlande, Portugāle un Somija (stāvoklis 2019. gada 17. oktobrī).

⁵¹ Direktīva (ES) 2016/680 (2016. gada 27. aprīlis).

⁵² Sk. sešpadsmito progresa ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2018) 690 *final*, 2018. gada 10. oktobris).

⁵³ Slovēnija paziņoja par daļēju transponēšanu. Spānija nav paziņojusi par transponēšanu. Lai gan Vācija paziņoja par pilnīgu transponēšanu, Komisija uzskata, ka šī transponēšana nav pilnīga (stāvoklis 2019. gada 17. oktobrī).

⁵⁴ Grieķija un Spānija.

⁵⁵ Vācija.

⁵⁶ Grieķija paziņoja par pilnīgu transponēšanu, un Komisija to pašlaik izvērtē.

⁵⁷ Direktīva (ES) 2015/849 (2015. gada 20. maijs).

neliecina par šīs direktīvas pilnīgu transponēšanu⁵⁸.

Komisija ir izvērtējusi **ar kibernetizāciju saistīto direktīvu** transponēšanas atbilstību. Komisija 2019. gada jūlijā un oktobrī sāka pienākumu neizpildes procedūras pret 23 dalībvalstīm⁵⁹, jo konstatēja, ka minēto dalībvalstu paziņotie valsts īstenošanas tiesību akti neliecina par to, ka **Direktīva par seksuālas vardarbības pret bērniem apkarošanu**⁶⁰ tiek transponēta pareizi. Tāpat Komisija 2019. gada jūlijā un oktobrī sāka pienākumu neizpildes procedūras pret četrām dalībvalstīm⁶¹, jo konstatēja, ka minēto dalībvalstu paziņotie valsts īstenošanas tiesību akti neliecina par to, ka **Direktīva par uzbrukumiem informācijas sistēmām**⁶² tiek transponēta pareizi.

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

- **ES Pasažieru datu reģistra direktīva**, attiecībā uz kuru vienai dalībvalstij vēl ir jāpaziņo par transponēšanu valsts tiesību aktos un vienai dalībvalstij vēl ir jāpabeidz paziņošana par transponēšanu⁶³;
- **Direktīva par terorisma apkarošanu**, attiecībā uz kuru divām dalībvalstīm vēl ir jāpaziņo par transponēšanu valsts tiesību aktos un vienai dalībvalstij vēl ir jāpabeidz paziņošana par transponēšanu⁶⁴;
- **Direktīva par ieroču iegādes un turēšanas kontroli**, attiecībā uz kuru astoņām dalībvalstīm vēl ir jāpaziņo par transponēšanu valsts tiesību aktos un septiņām dalībvalstīm vēl ir jāpabeidz paziņošana par transponēšanu⁶⁵;
- **Direktīva par datu aizsardzību tiesībaizsardzības jomā**, attiecībā uz kuru vienai dalībvalstij vēl ir jāpaziņo par transponēšanu valsts tiesību aktos un divām dalībvalstīm vēl ir jāpabeidz paziņošana par transponēšanu⁶⁶;
- **Ceturrtā direktīva par nelikumīgi iegūtu līdzekļu legalizācijas novēršanu**, attiecībā uz kuru 21 dalībvalstij vēl ir jāpabeidz paziņošana par transponēšanu⁶⁷;
- **Direktīva par seksuālas vardarbības pret bērniem apkarošanu**, attiecībā uz kuru pret 23 dalībvalstīm ir sāktas pienākumu neizpildes procedūras par nepareizu transponēšanu⁶⁸;

⁵⁸ Apvienotā Karaliste, Austrija, Beļģija, Bulgārija, Čehija, Dānija, Francija, Igaunija, Itālija, Īrija, Kipra, Latvija, Lietuva, Nīderlande, Polija, Rumānija, Slovākija, Somija, Ungārija, Vācija un Zviedrija (stāvoklis 2019. gada 17. oktobrī). Līdz šim ir slēgtas septiņas pienākumu neizpildes procedūras saistībā ar šo direktīvu.

⁵⁹ Austrija, Beļģija, Bulgārija, Čehija, Francija, Grieķija, Horvātija, Igaunija, Itālija, Latvija, Lietuva, Luksemburga, Malta, Polija, Portugāle, Rumānija, Slovākija, Slovēnija, Somija, Spānija, Ungārija, Vācija un Zviedrija.

⁶⁰ Direktīva 2011/93/ES (2011. gada 13. decembris).

⁶¹ Bulgārija, Itālija, Portugāle un Slovēnija.

⁶² Direktīva 2013/40/ES (2013. gada 12. augusts).

⁶³ Slovēnija paziņoja par daļēju transponēšanu. Spānija nav paziņojusi par transponēšanu (stāvoklis 2019. gada 17. oktobrī).

⁶⁴ Grieķija un Luksemburga nav paziņojušas par transponēšanu. Polija paziņoja par daļēju transponēšanu (stāvoklis 2019. gada 17. oktobrī).

⁶⁵ Apvienotā Karaliste, Beļģija, Čehija, Igaunija, Polija, Slovākija un Zviedrija ir paziņojušas par transponēšanas pasākumiem attiecībā uz daļu no jaunajiem noteikumiem. Grieķija, Kipra, Luksemburga, Rumānija, Slovēnija, Spānija, Ungārija un Vācija nav paziņojušas par transponēšanas pasākumiem (stāvoklis 2019. gada 17. oktobrī).

⁶⁶ Slovēnija paziņoja par daļēju transponēšanu. Spānija nav paziņojusi par transponēšanu. Lai gan Vācija paziņoja par to, ka transponēšana ir pabeigta, Komisija uzskata, ka šī transponēšana nav pilnīga (stāvoklis 2019. gada 17. oktobrī).

⁶⁷ Apvienotā Karaliste, Austrija, Beļģija, Bulgārija, Čehija, Dānija, Francija, Igaunija, Itālija, Īrija, Kipra, Latvija, Lietuva, Nīderlande, Polija, Rumānija, Slovākija, Somija, Ungārija, Vācija un Zviedrija (stāvoklis 2019. gada 17. oktobrī).

- **Direktīva par uzbrukumiem informācijas sistēmām**, attiecībā uz kuru pret četrām dalībvalstīm ir sāktas pienākumu neizpildes procedūras par nepareizu transponēšanu⁶⁹.

2. Sagatavotība un aizsardzība

Virzībā uz efektīvu un patiesu drošības savienību būtiska darba daļa attiecas uz izturētspējas pret drošības apdraudējumiem veidošanu. Komisija atbalsta dalībvalstis un vietējās iestādes saistībā ar sabiedrisko vietu aizsardzības uzlabošanu, 2017. gada oktobra rīcības plāna īstenošanu un 2019. gada janvāra Partnerības drošībai sabiedriskajā telpā īstenošanu atbilstīgi ES pilsētprogrammai. Šajā darbā ir iesaistītas pilsētas, kas vērsās pie Komisijas un lūdza atbalstu to problēmu risināšanā, kuras tām radušās, aizsargājot sabiedriskās vietas.

Sabiedrisko vietu drošības nostiprināšanā būtiska nozīme ir paraugprakses apmaiņai starp vietējām iestādēm un privātiem uzņēmējiem. Tā bija galvenā tēma **Eiropas drošības nedēļā**, kas norisinājās Nicā (Francijā) 2019. gada 14.–18. oktobrī un tika organizēta saistībā ar ES finansēto projektu “Sabiedroto pilsētu aizsargāšana no terorisma pilsēteritoriju drošības garantēšanā”. Šajā pasākumā, kurā piedalījās kopumā 500 dalībnieku no Eiropas pilsētām, valsts iestādēm un pētniecības iestādēm, tika uzsvērts tas, cik nozīmīga ir visu iesaistīto ieinteresēto personu (gan no publiskā, gan privātā sektora) cieša sadarbība, kā arī jaunu tehnoloģiju loma, lai nodrošinātu pilsētām labāku aizsardzību. Sabiedrisko vietu aizsardzība bija arī viens no tematiem **Eiropas reģionu un pilsētu nedēļā**, kas norisinājās Briselē 2019. gada 7.–10. oktobrī un kuras laikā tika rīkots darbseminārs par ES pilsētprogrammas partnerību drošībai sabiedriskajās vietās. Tajā galvenā uzmanība tika pievērsta vietējo iestāžu lomai drošības politikas jomā, ES regulējumam un finansējumam, kas ļauj risināt galvenās ar drošību saistītās problēmas pilsētu sabiedriskajās vietās, un tika izskatītas arī tādas svarīgas tēmas kā inovācija, izmantojot viedus risinājumus un tehnoloģijas, tostarp integrētās drošības jēdziens, preventīvā darbība un sociālā iekļaušana. Komisija arī sniedz ieguldījumu, lai veicinātu pilsētu inovāciju šajās jomās, izsludinot jaunāko uzaicinājumu iesniegt priekšlikumus par iniciatīvu “Inovatīvas pilsētvides darbības”, kura rezultāti tika paziņoti 2019. gada augustā. No atlasītajiem projektiem trijās pilsētās (Pirejā (Grieķijā), Tamerē (Somijā) un Turīnā (Itālijā)) tiks izmēģināti jauni risinājumi, kā novērst pilsētu drošības problēmas⁷⁰.

Lai labāk aizsargātu **pielūgsmes vietas** un noskaidrotu, kādas ir dažādu reliģisko grupu vajadzības, Komisija 2019. gada 7. oktobrī rīkoja tikšanos ar ebreju, musulmaņu, kristiešu un budistu kopienu pārstāvjiem. Saistībā ar 2017. gada ES rīcības plāna sabiedrisko vietu aizsardzības atbalstam īstenošanu sanāksmē tika norādīts, ka izpratne par drošību un gatavība drošībai dažādās reliģiskajās kopienās ievērojami atšķiras, uzsverot to, cik nozīmīga ir turpmāka paraugprakses apmaiņa. Sanāksmē tika arī norādīts, ka drošības pamatpasākumu ieviešana un labāka izpratne par drošību nav pretrunā tam, ka tiek uzturēta pielūgsmes vietu atvērtība un pieejamība. Komisija apkopos labas prakses un informētības veicināšanas materiālus savā elektroniskajā ekspertu platformā un informēs par šo jautājumu dalībvalstu drošības iestādes publiskā un privātā sektora forumā par sabiedrisko vietu aizsardzību.

Viena īpaša joma, kurai ir jāturpina pievērst uzmanību, ir pieaugošais kritiskās svarīgas infrastruktūras un sabiedrisko vietu drošības apdraudējums, ko rada **droni**. Papildinot nesenos ES tiesību aktus⁷¹ par dronu drošu ekspluatāciju un neierobežojot dronu lietderīgas izmantošanas iespējas, Komisija atbalsta

⁶⁸ Austrija, Beļģija, Bulgārija, Čehija, Francija, Grieķija, Horvātija, Igaunija, Itālija, Latvija, Lietuva, Luksemburga, Malta, Polija, Portugāle, Rumānija, Slovākija, Slovēnija, Somija, Spānija, Ungārija, Vācija un Zviedrija.

⁶⁹ Bulgārija, Itālija, Portugāle un Slovēnija.

⁷⁰ “Inovatīvas pilsētvides darbības” ir Eiropas Reģionālās attīstības fonda līdzfinansēts instruments. Vairāk informācijas skatīt vietnē <https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals>.

⁷¹ Komisijas Īstenošanas regula (ES) 2019/947 (2019. gada 24. maijs) par bezpilota gaisa kuģu sistēmu ekspluatācijas noteikumiem un procedūrām.

dalībvalstis saistībā ar ļaunprātīgas dronu izmantošanas tendenču izsekošanu, attiecīgas pētniecības finansēšanu un pretpasākumu izmēģināšanas veicināšanu. Būtiska nozīme ir pieredzes un paraugprakses apmaiņai, kā tika apliecināts 2019. gada 17. oktobrī Briselē notikušajā augsta līmeņa starptautiskajā konferencē par vēršanos pret draudiem, ko rada bezpilota gaisa kuģu sistēmas. Šajā Komisijas organizētajā pasākumā piedalījās 250 dalībnieki no dalībvalstīm, starptautiskām organizācijām, trešām partnervalstīm, nozares, akadēmiskajām aprindām un pilsoniskās sabiedrības, lai apspriestu dronu radītās drošības problēmas un veidus, kā tās risināt. Šī tikšanās apliecināja, ka ir vajadzīga regulāra riska novērtēšana saistībā ar droniem un cieša sadarbība starp aviācijas un tiesībsardzības iestādēm, turpinot izstrādāt Eiropas tiesību aktus par dronu drošu ekspluatāciju. Ir arī jāturpina pretpasākumu izmēģināšana pret droniem, īstenojot koordinētu Eiropas pieeju. Turklāt tika panākta vienprātība par to, ka svarīga ir cieša sadarbība starp iestādēm un nozari, lai garantētu, ka droni ir droši, nekaitīgi, uzticami ekspluatācijā un grūti izmantojami ļaunprātīgos nolūkos.

3. *Ārējā dimensija*

Tā kā lielākā daļa drošības risku, ar kuriem saskaras Savienība, sniedzas pāri ES robežām un rada globālus apdraudējumus, efektīvas un patiesas drošības savienības veidošanā būtiska nozīme ir sadarbībai ar partnervalstīm, organizācijām un attiecīgajām ieinteresētajām personām.

Šādā sadarbībā galvenā nozīme ir informācijas apmaiņai. Kopā ar šo ziņojumu Komisija pieņēma ieteikumu Padomei sniegt pilnvarojumu sarunu sākšanu par **nolīgumu starp ES un Jaunzēlandi par persondatu apmaiņu smagu noziegumu un terorisma apkarošanas jomā**, kas tiktu veikta starp Eiropolu un Jaunzēlandes kompetentajām iestādēm. Šāds nolīgums vēl vairāk nostiprinās Eiropola spējas sadarboties ar Jaunzēlandi nolūkā novērst un apkarot noziegumus, kuru apkarošana ietilpst Eiropola mērķu tvērumā. Lai gan 2019. gada aprīļa darba vienošanās starp Eiropolu un Jaunzēlandes Policiju nosaka satvaru strukturētai stratēģiskā līmeņa sadarbībai, tā neparedz juridisku pamatu persondatu apmaiņai. Persondatu apmaiņa, pilnīgi ievērojot ES tiesību aktus un pamattiesības, ir būtiska, lai varētu īstenot efektīvu policijas operatīvo sadarbību. Līdz šim Komisija ir apzinājusi astoņas prioritārās valstis Tuvo Austrumu / Ziemeļāfrikas reģionā, pamatojoties uz terorisma draudiem, ar migrāciju saistītām problēmām un Eiropola operatīvajām vajadzībām sākt sarunas⁷². Ņemot vērā tiesībsardzības iestāžu operatīvās vajadzības visā ES un ciešākas sadarbības sniegtos potenciālos ieguvumus šajā jomā, par ko liecina arī turpmākā uzraudzība pēc uzbrukuma Kraistčērčā 2019. gada martā, Komisija uzskata, ka arī Jaunzēlande ir jāpievieno kā prioritāra valsts, ar kuru drīzumā uzsākt sarunas.

Vēl viens stūrakmens Savienības sadarbībā ar trešām partnervalstīm drošības jomā ir **pasažieru datu reģistra datu** nosūtīšana. Komisija 2019. gada 27. septembrī pieņēma ieteikumu Padomei atļaut sarunu sākšanu attiecībā uz **ES un Japānas** nolīgumu par pasažieru datu reģistra datu nosūtīšanu, lai novērstu un apkarotu terorismu un smagus pārobežu noziegumus, pilnīgi ievērojot datu aizsardzības pasākumus un pamattiesības⁷³. Ieteikums tiek izskatīts Padomes darba grupas līmenī, un Komisija aicina Padomi nekavējoties pieņemt pilnvarojumu sarunām ar Japānu. Ja vienošanās tiks noslēgta laikus, līdz 2020. gada olimpiskajām spēlēm, tā dos reālu ieguvumu drošībai.

Pasaules līmenī Komisija atbalsta **Starptautiskās Civilās aviācijas aģentūras** darbu, kas tiek veikts, lai noteiktu standartu pasažieru datu reģistra datu apstrādei. Tā ir atbilde uz Apvienoto Nāciju Organizācijas Drošības padomes Rezolūciju 2396, kurā visas Apvienoto Nāciju organizācijas dalībvalstis ir aicinātas vākt, apstrādāt un analizēt pasažieru datu reģistra datus. Komisija 2019. gada 13. septembrī nāca klajā ar priekšlikumu⁷⁴ par Padomes lēmumu par nostāju, kas ES vārdā jāieņem

⁷² Sk. vienpadsmito progresā ziņojumu virzībā uz efektīvu un patiesu drošības savienību (COM(2017) 608 *final*, 2017. gada 18. oktobris). Prioritārās valstis ir Alžīrija, Ēģipte, Izraēla, Jordānija, Libāna, Maroka, Tunisija un Turcija.

⁷³ COM(2019) 420 *final* (2019. gada 27. septembris).

⁷⁴ COM(2019) 416 *final* (2019. gada 13. septembris).

Starptautiskajā Civilās aviācijas organizācijā attiecībā uz standartiem un ieteicamo praksi pasažieru datu reģistra datu jomā. Šis priekšlikums tiek izskatīts Padomes darba grupas līmenī, un Komisija aicina nekavējoties pieņemt Padomes lēmumu. Savienības un tās dalībvalstu nostāja ir izklāstīta arī informatīvajā dokumentā “Standarti un principi attiecībā uz pasažieru datu reģistra datu vākšanu, izmantošanu, apstrādi un aizsardzību”, kas tika iesniegts Starptautiskās Civilās aviācijas organizācijas Asamblejas 40. sesijai.

Attiecībā uz darbu, kas tiek veikts, lai noslēgtu jaunu nolīgumu ar **Kanādu** par pasažieru datu reģistru, Komisija ir izvirzījusi mērķi ātri pabeigt šo nolīgumu. Tajā pašā laikā šovasar tika sākta nolīguma ar **Austrāliju** par pasažieru datu reģistru apvienotā kopīgā pārskatīšana un izvērtēšana, kā arī nolīguma ar **Amerikas Savienotajām Valstīm** par pasažieru datu reģistru kopīgā izvērtēšana, sākot ar vizītēm uz Kanberu un Vašingtonu attiecīgi 2019. gada augustā un septembrī. Komisija slēgtā sesijā 2019. gada 14. oktobrī informēja Eiropas Parlamenta Pilsuņu brīvību, tieslietu un iekšlietu komiteju par aktuālo situāciju attiecībā uz to, kā norit darbs ar Japānu, Austrāliju un Kanādu saistībā ar pasažieru datu reģistra datiem.

Ir gūti panākumi arī sadarbībā drošības jomā ar **Rietumbalkānu** partnervalstīm, īstenojot 2018. gada oktobra kopīgo rīcības plānu terorisma apkarošanai Rietumbalkānu reģionā. Komisija 9. oktobrī parakstīja divas nesaistošas divpusējas vienošanās ar Albāniju un Ziemeļmaķedonijas Republiku par terorisma apkarošanu⁷⁵. Šajās vienošanās tiek noteikts, kādas pielāgotas prioritārās darbības ir jāveic attiecīgās partnervalsts iestādēm, aptverot piecus kopīgā rīcības plāna⁷⁶ mērķus un norādot, kādu atbalstu Komisija plāno sniegt. Paredzams, ka līdzīgas vienošanās ar pārējām Rietumbalkānu partnervalstīm tiks parakstītas turpmākajās nedēļās. Turklāt 2019. gada 7. oktobrī Komisija parakstīja nolīgumu ar Melnkalni par Melnkalnes un Eiropas Robežu un krasta apsardzes aģentūras (*EBCGA*) sadarbību robežu pārvaldības jomā. Minētais nolīgums sniedz aģentūrai iespēju palīdzēt Melnkalnei robežu pārvaldībā, lai vērstos pret neatbilstīgu migrāciju un pārrobežu noziedzību, tādējādi uzlabojot drošību uz ES ārējām robežām.

Lai uzlabotu sadarbību ar partnervalstīm cīņā pret kopējiem drošības apdraudējumiem, Komisija aicina Padomi:

- dot pilnvarojumu sākt sarunas par nolīgumu starp ES un **Jaunzēlandi** par persondatu apmaiņu smagu noziegumu un terorisma apkarošanas jomā;
- dot pilnvarojumu sākt sarunas par nolīgumu starp ES un **Japānu** pasažieru datu reģistra datu pārsūtīšanas jomā;
- pieņemt ierosināto **Padomes lēmumu par nostāju, kas ES vārdā jāieņem Starptautiskajā Civilās aviācijas organizācijā attiecībā uz standartiem un ieteicamo praksi pasažieru datu reģistra datu jomā.**

VI. SECINĀJUMI

Šajā ziņojumā ir aprakstīti dažādie pasākumi, kurus ES ir veikusi, lai vērstos pret kopējiem apdraudējumiem Eiropā un uzlabotu mūsu kolektīvo drošību. Gūtais progress virzībā uz efektīvu un patiesu drošības savienību, ko veicinājusi vienota izpratne par to, ka mūsdienu drošības problēmas vislabāk var atrisināt, strādājot kopā un sadarbojoties ar trešām valstīm, ir rezultāts, ko nesis tas, ka cieši sadarbojās plašs dalībnieku loks, tika veidota uzticēšanās, koplietoti resursi un kopīgi karots pret apdraudējumiem. Šie dalībnieki ietver visus pārvaldes līmeņus no pilsētām un citiem vietējiem dalībniekiem, reģioniem un valsts iestādēm līdz ES līmenim ar Eiropas Parlamentu un Padomi; tika

⁷⁵ https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en.

⁷⁶ Kopīgajā rīcības plānā ir paredzētas darbības, kas vērstas uz šādiem pieciem mērķiem: stingrs pretterorisma regulējums, vardarbīga ekstrēmisma efektīva novēršana un apkarošana; efektīva informācijas apmaiņa un operatīvā sadarbība; uzlabota spēja apkarot nelikumīgi iegūtu līdzekļu legalizēšanu un terorisma finansēšanu; iedzīvotāju un infrastruktūras aizsardzības pastiprināšana.

iesaistītas publiskās iestādes, ES aģentūras, privātie dalībnieki un pilsoniskā sabiedrība. Tika izmantotas speciālās zināšanas, rīki un resursi, kas pieejami dažādās politikas jomās, piemēram, transporta politikas, digitālā vienotā tirgus vai kohēzijas politikas jomā. Darbs, kas tiek veikts drošības savienības jomā, integrē pamattiesību aizsardzību un aizsargā un popularizē mūsu vērtības.

Darbam virzībā uz efektīvu un patiesu drošības savienību ir jāturpinās. Ir ātri jāpanāk vienošanās par svarīgām izskatīšanā esošām iniciatīvām, proti: 1) tiesību akta priekšlikumu par teroristiska satura izņemšanu no interneta, 2) tiesību akta priekšlikumu par uzlabotu tiesībaizsardzības iestāžu piekļuvi elektroniskiem pierādījumiem, 3) tiesību akta priekšlikumu par Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīkla izveidi un 4) izskatīšanā esošajiem tiesību aktu priekšlikumiem par spēcīgākām un viedākām drošības, robežu un migrācijas pārvaldības informācijas sistēmām. Saskaņotie pasākumi un instrumenti ir jāpārvērš praktiskā rīcībā uz vietas, visām dalībvalstīm laikus un pilnībā īstenojot ES tiesību aktus, lai varētu realizēt visus to sniegtos ieguvumus drošības ziņā. Ir īpaši svarīgi, lai visas dalībvalstis īstenotu nesen saskaņotos tiesību aktus par ES drošības, robežu un migrācijas pārvaldības informācijas sistēmu sadarbību nolūkā sasniegt vērienīgo mērķi, proti, līdz 2020. gadam nodrošināt pilnīgu sadarbību. Visbeidzot, Eiropai jāturpina modri sekot līdzi jaunajiem un mainīgajiem apdraudējumiem un ir jāturpina sadarbība, lai uzlabotu visu iedzīvotāju drošību.