EUROOPA
KOMISJON

Brüssel, 24.7.2020
COM(2020) 605 final

KOMISJONI TEATIS EUROOPA PARLAMENDILE, EUROOPA ÜLEMKOGULE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE

ELi julgeolekuliidu strateegia kohta

I. Sissejuhatus

Komisjoni poliitilistes suunistes on selgelt öeldud, et me peame tegema kõik endast oleneva oma kodanike kaitsmiseks. Julgeolek ei ole üksnes igaühe turvalisuse alus – see on vajalik ka põhiõiguste kaitsmiseks ning loob vundamendi, millele toetub meie majanduse, ühiskonna ja demokraatia usaldusväärsus ja dünaamilisus. Tänased eurooplased on silmitsi kiirelt muutuva julgeolekuolukorraga, mida mõjutavad teisenevad ohud, samuti muud tegurid, sh kliimamuutused, demograafilised trendid ja poliitiline ebastabiilsus väljaspool meie piire. Üleilmastumine, vaba liikumine ja digiüleminek suurendavad jätkuvalt heaolu, lihtsustavad meie elu ning kannustavad innovatsiooni ja majanduskasvu. Kuid nende eelistega kaasneb paratamatult ka riske ja kulusid. Kõige sellega võidakse manipuleerida terrorismi, organiseeritud kuritegevuse, uimastikaubanduse ja inimkaubanduse eesmärgil, millega seatakse vahetult ohtu meie kodanikud ja euroopalik eluviis. Küberründed ja küberkuritegevus on jätkuvalt tõusuteel. Ka julgeolekuohud muutuvad üha keerukamaks: neid süvendavad piiriülese töötamise võimalused ja vastastikused seosed; neis kasutatakse ära füüsilise ja digitaalse maailma piiride hägustumist; neis kasutatakse ära haavatavaid rühmi ning sotsiaalseid ja majanduslikke erinevusi. Ründed võivad alata ootamatult ja neid võib olla raske või suisa võimatu jälitada; nii riiklikud kui ka valitsusvälised osalejad võivad panustada mitmesugustele hübriidohtudele[1]; ning väljaspool ELi toimuv võib otsustavalt mõjutada ka ELi sisejulgeolekut.

COVID-19 kriis on muutnud ka meie arusaama ohutuse ja julgeolekuga seotud ohtudest ning seonduvat poliitikat. See on välja toonud vajaduse tagada turvalisus nii füüsilises kui ka digikeskkonnas. See on näidanud seda, kui oluline on kriitilise tähtsusega toodete, teenuste, taristute ja tehnoloogia jaoks meie tarneahelate avatud strateegiline autonoomia. See on teravdanud vajadust kaasata kõik sektorid ja üksikisikud ühistesse jõupingutustesse, et tagada algusest peale ELi parem valmisolek ja vastupidavusvõime ning paremad vahendid vajaduse korral reageerimiseks.

Liikmesriigid ei suuda kodanikke kaitsta üksi tegutsedes. On olulisem kui kunagi varem, et me arendaksime koostöös oma tugevaid külgi, ning ELil on võimalus teha ära enam kui kunagi varem. EL võib anda eeskuju, parandades üldist kriisiohje süsteemi ja aidates nii ELi piires kui ka mujal kaasa ülemaailmsele stabiilsusele. Kuigi esmane vastutus julgeoleku eest lasub liikmesriikidel, on viimastel aastatel hakatud üha enam mõistma, et ühe liikmesriigi julgeolek on kõigi julgeolek. ELi võimuses on reageerida valdkonnaüleselt ja integreeritult, aidates liikmesriikide julgeolekujõude vajalike vahendite ja teabega.[2]

EL saab samuti tagada, et julgeolekupoliitika tugineb jätkuvalt meie ühistele Euroopa väärtustele – õigusriigi, võrdsuse[3] ja põhiõiguste austamisele ning läbipaistvuse, vastutuse ja demokraatliku kontrolli tagamisele, et poliitika tugineks – nii nagu peab – usaldusel. Samuti saame üles ehitada tulemusliku ja tegeliku julgeolekuliidu, kus kodanike õigused ja vabadused on hästi kaitstud. Julgeolek ja põhiõiguste austamine ei ole eesmärkidena vastuolus, vaid need kuuluvad kokku ja on üksteist täiendavad. Meie väärtused ja

[1] Kuigi hübriidohtu on erinevalt määratletud, on kontseptsiooni eesmärk tabada see sunni- ja õõnestustaktika, konventsionaalsete ja mittekonventsionaalsete meetodite (st diplomaatiliste, sõjaliste, majanduslike ja tehnoloogiliste meetodite) kooslus, mida riigid või muud jõud saavad koordineeritud viisil kasutada konkreetsete eesmärkide saavutamiseks, seejuures ametlikku sõjategevust alustamata. Vt JOIN(2016) 18 (final).

[2] Näiteks selliste ELi kosmoseprogrammi teenuste kaudu nagu Copernicus, mis pakuvad Maa seire andmeid ja rakendusi piiride valvamiseks, meresõidu turvalisuseks, õiguskaitseks, piraatlusevastaseks võitluseks, uimastite salakaubaveo tõkestamiseks ja hädaolukordade ohjamiseks.

[3] Võrdõiguslikkuse liit: soolise võrdõiguslikkuse strateegia 2020–2025 (COM(2020) 152).

põhiõigused peavad moodustama julgeolekupoliitika aluse, tagades vajalikkuse, proportsionaalsuse ja seaduslikkuse põhimõtte järgmise ning sobivad vastutuse ja õiguskaitse tagatised, võimaldades samas tulemuslikku reageerimist üksikisikute, eriti kõige haavatavamate isikute kaitseks.

Olulised õiguslikud, praktilised ja tugivahendid on juba olemas, kuid neid tuleb nii tugevdada kui ka paremini rakendada. Suuri edusamme on tehtud liikmesriikidega teabe- ja luurealase koostöö parandamisel ning terroristide ja kurjategijate tegutsemisruumi kitsendamisel. Kuid endiselt esineb killustatust.

Tuleb vaeva näha ka väljaspool ELi piire. Liidu ja selle kodanike kaitsmine ei tähenda enam üksnes julgeoleku tagamist ELi piires, vaid ka tegelemist julgeoleku välismõõtmega. ELi välisjulgeolekukäsitus ühise välis- ja julgeolekupoliitika (ÜVJP) ning ühise julgeoleku- ja kaitsepoliitika (ÜJKP) raames on ka edaspidi oluline osa ELi jõupingutustes ELis julgeoleku suurendamiseks. Koostöö kolmandate riikidega ja ülemaailmsel tasandil on ühiste probleemide lahendamisel keskse tähtsusega, et reageerida tulemuslikult ja terviklikult, lisaks on stabiilsus ja julgeolek ELi naabruses kriitilise tähtsusega ka ELi enda julgeoleku jaoks.

Euroopa Parlamendi[4], nõukogu[5] ja komisjoni[6] varasemale tööle tuginev uus strateegia näitab, et tegeliku ja tulemusliku julgeolekuliidu jaoks on vaja ühendada põhivahendid ja poliitikameetmed, millega tagada päriselus julgeolek selliselt, et teadvustatakse julgeoleku mõju ühiskonna kõikidele osadele ja igasugusele avalikule poliitikale. EL peab tagama turvalise keskkonna kõigile, olenemata inimeste rassilisest või etnilisest päritolust, usutunnistusest, veendumustest, soost, vanusest või seksuaalsest sättumusest.

Käesolev strateegia hõlmab ajavahemikku 2020–2025 ning selles keskendutakse tulevikukindla julgeolekukeskkonna tagamise võime ja suutlikkuse suurendamisele. Selles esitatakse kogu ühiskonda hõlmav julgeolekukäsitus, mis võimaldab tulemuslikult ja koordineeritult reageerida kiiresti muutuvatele ohtudele. Selles määratakse kindlaks strateegilised prioriteedid ja vastavad meetmed, et maandada digi- ja füüsilisi riske integreeritud viisil kogu julgeolekuliidu ökosüsteemi ulatuses, keskendudes valdkondadele, kus EL saab pakkuda lisaväärtust. Selle eesmärk on pakkuda turvadividende, et kaitsta kõiki ELis.

II. Euroopa pidevalt muutuvad julgeolekuohud

Kodanike turvalisus, jõukus ja heaolu sõltub julgeolekust. Seda julgeolekut ähvardavad ohud on olenevalt elu ja elatusvahendite haavatavuse määrast erinevad. Mida suurem on haavatavus, seda suurem on ka selle ärakasutamise oht. Nii haavatavused kui ka ohud on pidevas muutumises ja EL peab nendega kohanema.

Sõltume igapäevases elus mitmesugustest teenustest – energeetika, transpordi, rahanduse ja tervishoiu vallas. Nende teenuse jaoks on vaja nii füüsilist kui ka digitaristut ning seeläbi

[4] Näiteks Euroopa Parlamendi TERR-komisjoni (terrorismi käsitleva erikomisjoni) töö, mille aruanne esitati 2018. aasta novembris.

[5] Alates nõukogu 2015. aasta juuni järeldustest sisejulgeoleku uuendatud strateegia kohta kuni nõukogu viimaste järeldusteni 2019. aasta detsembris.

[6] „Euroopa julgeoleku tegevuskava elluviimine, et võidelda terrorismi vastu ning liikuda tulemusliku ja tegeliku julgeolekuliidu poole“ (COM(2016) 230 final, 20.4.2016). Vt hiljutist hinnangut õigusaktide rakendamise kohta sisejulgeoleku valdkonnas: „Siseasjade valdkonnas sisejulgeolekualaste õigusaktide rakendamine aastatel 2017–2020“ (SWD(2020) 135).

suureneb haavatavus ja häirete võimalikkus. COVID-19 pandeemia ajal on uus tehnoloogia aidanud edasi tegutseda paljudel ettevõtetel ja võimaldanud avalike teenuste jätkumist, ühendades meid kaugtöö kaudu või tagades tarneahelate logistika. Kuid see on ka avanud ukse pahatahtlike rünnete arvu erakordsele suurenemisele, sest kuritegelikel eesmärkidel püütakse ära kasutada pandeemiaga tekkinud häiret ja üleminekut kodusele digitööle.[7] Kaupade nappus on avanud organiseeritud kuritegevusele uusi uksi. Kõige suurema surve ajal oluliste tervishoiuteenuste häirimisel oleksid võinud olla surmavad tagajärjed.

Digitehnoloogia toob meie ellu lisaväärtust järjest enamates valdkondades ning seetõttu on tehnoloogia **küberturvalisus** omandanud strateegilise tähtsuse.[8] Küberründed võivad anda hoobi kodudele, pankadele, finantsteenustele ja ettevõtjatele (eriti väikestele ja keskmise suurusega ettevõtjatele). Võimalikku kahju mitmekordistab füüsiliste ja digitaalsete süsteemide vastastikune sõltuvus: igasugune füüsiline kahjustus mõjutab tahes-tahtmata ka digisüsteeme ning teisest küljest võivad küberründed infosüsteemidele ja digitaristutele rivist välja lüüa olulisi teenuseid[9]. Asjade interneti levik ja tehisintellekti laialdasem kasutamine toob kaasa nii uusi hüvesid kui ka uusi riske.

Meie maailm toetub digitaristutele, -tehnoloogiale ja veebipõhistele süsteemidele, mis võimaldavad meil tegeleda äriga, tarbida tooteid ja nautida teenuseid. Kõik need sõltuvad teabevahetusest ja suhtlusest. Internetist sõltumise kaasnäht on **küberkuritegevuse** laine võimalus.[10] „Küberkuritegevus teenusena“ ja küberkuritegevuse varimajandus annab internetis lihtsa juurdepääsu küberkuritegudega seotud toodetele ja teenustele. Kurjategijad võtavad oma eesmärkide saavutamiseks uue tehnoloogia kiiresti üle. Näiteks on võltsitud ravimid imbunud ravimite seaduslikku tarneahelasse[11]. Lasteporno hüppeline kasv internetis[12] ilmestab kuritegevuse muutuvate vormide sotsiaalseid tagajärgi. Hiljutine uuring näitas, et ELis teeb enamikule (55 %) inimestele muret kurjategijate ja petturite võimalik ligipääs nende andmetele.[13]

Neid ohte süvendab ka **üleilmne keskkond**. Kolmandate riikide jõuline tööstuspoliitika ühes intellektuaalomandi jätkuva kübervargusega sunnib muutma Euroopa huvide kaitsmise ja edendamise strateegilist paradigmat. Seda võimendab kahese kasutusega rakenduste arvu kasv, mille tulemusel annab tugev tsiviiltehnoloogia sektor suure eelise kaitse- ja julgeolekuvõimele. Tööstusspionaažil on märkimisväärne mõju ELi majandusele, töökohtadele ja majanduskasvule: ärisaladuste kübervargus läheb ELile hinnanguliselt

---

7 Europol: „Pärast pandeemiat. Kuidas COVID-19 kujundab ELis ümber raske ja organiseeritud kuritegevuse?“ (Aprill 2020).

8 Komisjoni soovitus „5G-võrkude küberturvalisus“ (C(2019) 2335); teatis „5G turvaline kasutuselevõtt ELis: ELi meetmepaketi rakendamine“ (COM(2020) 50).

9 2020. aasta märtsis tabas Tšehhis asuvat Brno Ülikooli haiglat küberrünne, mis sundis haiglat patsiente ümber suunama ja operatsioone edasi lükkama (Europol: „Pandeemiast kasu saamine. Kuidas kurjategijad COVID-19 kriisi ära kasutavad?“. Tehisintellekti võidakse kuritarvitada digitaalseteks rünneteks, poliitilisteks ja füüsilisteks rünnakuteks ning jälgimistegevuseks. Asjade interneti kogutavaid andmeid saab kasutada eraisikute jälgimiseks (nutikellad, virtuaalsed assistendid jne).

10 Mõne prognoosi kohaselt küündivad andmelekete kulud, mis veel 2015. aastal olid 3 triljonit USA dollarit aastas, 2024. aastaks juba 5 triljoni USA dollarini aastas (Juniper Research, The Future of Cybercrime & Security).

11 Ühes 2016. aasta uuringus (Legiscript) prognoositi, et ülemaailmselt tegutseb ainult 4 % internetiapteekidest seaduslikult, kusjuures veebis tegutsevatest ebaseaduslikest internetiapteegitest on 30 000–35 000 jaoks peamine sihtmärk ELi tarbijad.

12 ELi strateegia, mis käsitleb tõhusamat võitlust laste seksuaalse väärkohtlemise vastu (COM(2020) 607).

13 Euroopa Liidu Põhiõiguste Amet (2020) „Sinu õigused väärivad kaitset: turvalisusega seotud probleemid ja kogemused. Põhiõiguste uuring“, Luxembourg, Euroopa Liidu Väljaannete Talitus.

maksma 60 miljardit eurot[14]. Seetõttu on vaja põhjalikult analüüsida seda, kuidas sõltuvused ja suurem avatus küberohtudele mõjutavad ELi suutlikkust kaitsta nii üksikisikuid kui ka ettevõtjaid.

COVID-19 kriis on näidanud ka seda, et sotsiaalsed lõhed ja ebakindlus teevad julgeoleku haavatavaks. See suurendab võimalust, et riiklikud ja valitsusvälised osalejad panevad toime keerukamaid ründeid ja **hübriidrünnakuid**, kusjuures haavatavuste ärakasutamiseks kombineeritakse küberründeid, elutähtsa taristu kahjustamist[15], desinformatsioonikampaaniaid ning poliitilise narratiivi radikaliseerimist.[16]

Samal ajal muutuvad jätkuvalt ka ammused ohud. **Terrorirünnakud** olid ELis 2019. aastal langustrendis. Daeshi ja Al Qaeda või neist inspireeritud džihaadirünnakute oht ELi kodanikele on siiski endiselt suur.[17] Sellega paralleelselt suureneb ka vägivaldse paremäärmusluse oht.[18] Tõsiseks mureks annavad põhjust ka rassismist ajendatud rünnakud: surmavad antisemiitlikud terrorirünnakud Halles tuletasid meelde vajadust reageerimist kooskõlas nõukogu 2018. aasta avaldusega[19] tõhustada. ELis on iga viies inimene väga mures, et järgmise 12 kuu jooksul võib toimuda terrorirünnak.[20] Suurem osa hiljutistest terrorirünnakutest olid avalikes kohtades üksikisikute vastu suunatud „madaltehnoloogilised“ rünnakud, kuid Christchurchi rünnakute reaalajas voogedastamine näitas terroristliku veebipropaganda tähtsamaks muutumist[21]. Radikaliseerunud isikud kujutavad endast endiselt suurt ohtu ja seda ohtu võivad suurendada tagasipöörduvad terroristidest välisvõitlejad ja vanglast vabastatud äärmuslased.[22]

Kriis on näidanud ka seda, kuidas teada-tuntud ohud võivad uutes oludes muutuda. **Organiseeritud kuritegelikud** rühmitused on ära kasutanud kaupade nappust, mis võimaldas neil luua uusi ebaseaduslikke turge. Ebaseaduslike uimastitega kaubitsemine on jätkuvalt ELi suurim kuritegelik turg, mille jaeturu hinnanguline väärtus ELis on vähemalt 30 miljardit eurot aastas[23]. Inimkaubandust ei ole õnnestunud likvideerida: hinnangute kohaselt on igasuguse ärakasutamisega lõigatav iga-aastane kogukasum peaaegu 30 miljardit eurot.[24] Rahvusvaheline kauplemine võltsitud ravimitega ulatus 38,9 miljardi euroni[25]. Samal ajal võimaldab vähene konfiskeerimine kurjategijatel jätkuvalt oma kuritegelikku

---

14 Tööstusspionaaži ja ärisaladuste kübervarguse ulatus ja mõju, 2018.

15 Elutähtsad taristud on hädavajalikud eluliselt tähtsate ühiskondlike toimingute, tervishoiu, turvalisuse, julgeoleku, majandusliku või sotsiaalse heaolu jaoks ning nende kahjustada saamisel või hävimisel on oluline mõju (nõukogu direktiiv 2008/114/EÜ).

16 ELi kodanikest on 97 % puutunud kokku libauudistega, 38 % iga päev. Vt JOIN (2020) 8 final.

17 13 ELi liikmesriiki teatasid kokku 119 toimepandud, ebaõnnestunud ja nurjatud terrorirünnakust, milles hukkus kümme ja sai vigastada 27 inimest (Europoli aruanne terrorismi olukorra ja suundumuse kohta, 2020).

18 2019. aastal toimus kuus paremäärmuslikku terrorirünnakut (üks pandi toime, üks ebaõnnestus, neli nurjati (kolmes liikmesriigis)) võrreldes ainult ühega 2018. aastal, kuigi siis oli veel surmajuhtumeid, mida ei liigitatud terrorismiks (Europol, 2020).

19 Vt ka nõukogu avaldus, mis käsitleb antisemitismi vastu võitlemist ja turvalisust puudutava ühise lähenemisviisi väljatöötamist, et paremini kaitsta juudi kogukondi ja institutsioone Euroopas.

20 Euroopa Liidu Põhiõiguste Amet „Sinu õigused väärivad kaitset: turvalisusega seotud probleemid ja kogemused“, 2020.

21 Alates 2015. aasta juulist kuni 2019. aasta lõpuni leidis Europol terroristliku sisu 361 platvormil (Europol, 2020).

22 Europol: „Ülevaade Atlandi-ülestest parimatest tavadest nii vanglates radikaliseerumise kui ka pärast vabanemist taas terroristliku tegevuse vastu võitlemisel“, 2019.

23 Euroopa Narkootikumide ja Narkomaania Seirekeskus ja Europol – ELi uimastituru aruanne 2019.

24 Europoli aruanne inimkaubanduse ärimudeli kohta (2015).

25 Euroopa Liidu Intellektuaalomandi Ameti ja OECD aruanne võltsravimitega kauplemise kohta

haaret laiendada ja imbuda seaduslikku majandustegevusse[26]. Kurjategijate ja terroristide jaoks on muutunud tulirelvadele juurdepääs lihtsamaks nii internetiturul kui ka uute tehnoloogiate, näiteks 3D-printimise kaudu.[27] Tehisintellekti, uue tehnoloogia ja robootika kasutamine suurendab veelgi ohtu, et kurjategijad kasutavad innovatsiooni ära kuritahtlikel eesmärkidel[28].

Need ohud on kategooriaülesed ja tabavad ühiskonna eri osi erineval viisil. Need kõik kujutavad endast suurt ohtu üksikisikutele ja ettevõtjatele ning vajavad terviklikku ja sidusat reageerimist ELi tasandil. Kui turvanõrkused võivad peituda isegi väikestes omavahel ühendatud kodumasinates, nagu internetiühendusega külmik või kohvimasin, ei saa me oma turvalisuses veendumiseks enam panustada üksnes traditsioonilistele riiklikele osalejatele. Ettevõtjad peavad võtma turule lastavate toodete ja teenuste küberturvalisuse eest suurema vastutuse; üksikisikutel peab omalt poolt olema vähemalt elementaarne arusaam küberturvalisusest, et nad suudaksid end kaitsta.

III. Kogu ühiskonda hõlmav ELi koordineeritud reageerimine

EL on juba näidanud, kuidas ta saab pakkuda tõelist lisaväärtust. Alates 2015. aastast on julgeolekuliit aidanud julgeolekupoliitikat ELi tasandil paremini seostada. Siiski on vaja rohkem ära teha, et kaasata kogu ühiskond, sealhulgas kõik valitsustasandid, kõigi sektorite ettevõtjad ja üksikisikud kõikides liikmesriikides. Suurenev teadlikkus sõltuvuse riskidest[29] ja vajadus tugeva Euroopa tööstusstrateegia järele[30] osutavad sellele, et ELil peab olema tööstuse, tehnoloogia tootmise ja tarneahela vastupidavusvõime kriitiline mass. Selleks et tugev olla, tuleb ka täielikult austada põhiõigusi ja ELi väärtusi: nendeta ei ole õiguspärane, tulemuslik ja kestlik julgeolekupoliitika võimalik. Käesolevas julgeolekuliidu strateegias sätestatakse konkreetsed töösuunad, mida edasi arendada. See põhineb alljärgnevatel ühistel eesmärkidel.

- ***Suurendada kriiside varajase avastamise, ennetamise ja neile kiirelt reageerimise võimet ja suutlikkust:*** Euroopa vastupidavusvõime peab olema parem, et tulevasi šokke ennetada, end nende eest kaitsta ja nendega toime tulla. Peame suurendama võimet ja suutlikkust julgeolekukriise varakult avastada ja neile kiirelt reageerida, rakendades integreeritud ja koordineeritud lähenemist nii ülemaailmselt kui ka sektoripõhiste algatuste kaudu (näiteks finants-, energeetika-, kohtusüsteemi-, õiguskaitse-, tervishoiu-, merendus- ja transpordisektoris) ning kasutades ära olemasolevaid vahendeid ja algatusi[31]. Julgeoleku jaoks võivad olla olulised ka komisjoni koostatavad ettepanekud ELis laiaulatusliku kriisiohjesüsteemi loomiseks.

---

[26] Aruanne „Vara sissenõudmine ja konfiskeerimine: meetmed kuritegevuse mittetasuvaks muutmisel“ (COM(2020) 217).

[27] 2017. aastal kasutati tulirelvi 41 % terrorirünnakutes (Europol, 2018).

[28] 2020. aasta juulis tutvustasid Prantsusmaa ja Madalmaade õiguskaitse- ja kohtuasutused koos Europoli ja Eurojustiga ühist uurimist, mille eesmärk oli lammutada EncroChat, krüpteeritud telefonivõrk, mida kasutavad vägivaldsetes rünnakutes, korruptsioonis, mõrvakatsetes ja suuremahulises uimastitranspordis osalevad kuritegelikud võrgustikud.

[29] Välissõltuvuse riskid hõlmavad suuremat avatust võimalikele ohtudele, alates (nt energeetikas, transpordis, panganduses, tervishoius) elutähtsaid taristuid toetavate IT-taristute nõrkuste ärakasutamisest või tööstuslike juhtimissüsteemide üle kontrolli haaramisest kuni andmete varguse või spionaaži suutlikkuse suurendamiseni.

[30] Komisjoni teatis „Euroopa uus tööstusstrateegia“ (COM(2020) 102).

[31] Näiteks integreeritud kord poliitiliseks reageerimiseks kriisidele (IPCR), hädaolukordadele reageerimise koordineerimiskeskus, komisjoni soovitus koordineeritud reageerimise kohta ulatuslike küberturvalisuse

- ***Keskenduda tulemustele***: tulemuslikkusel põhinev strateegia peab põhinema hoolikal ohu- ja riskihindamisel, et asuda tegutsema seal, kus meie jõupingutustest on kõige rohkem kasu. Strateegias on vaja määratleda õiged eeskirjad ja õiged vahendid ning neid kohaldada. Selles peab olema ELi julgeolekupoliitika aluseks võetud usaldusväärne strateegiline luureteave. Kui vaja läheb ELi õigusakte, tuleb nende täielikku rakendamist jälgida, et vältida killustumist ja ärakasutamist võimaldavaid lünki. Käesoleva strateegia tulemuslik rakendamine sõltub ka vajaliku rahastamise tagamisest järgmisel programmitöö perioodil 2021–2027, sealhulgas asjaomastele ELi ametitele.
- ***Tuua kõik avaliku ja erasektori osalejad kokku ühiseks jõupingutuseks:*** ei avaliku ega erasektori olulised osalejad ei ole soovinud julgeolekualast teavet jagada, olgu siis kartusest riikliku julgeoleku või konkurentsivõime ohtuseadmise ees.[32] Kuid kõige enam suudame me ära teha siis, kui me oma jõud ühendame. Esiteks tähendab see tihedamat koostööd liikmesriikide vahel, kaasates õiguskaitse-, kohtu- ja avaliku sektori asutused, ning ELi institutsioonide ja asutustega, et jõuda ühiste lahenduste jaoks vajaliku arusaama ja teabevahetuseni. Väga oluline on ka koostöö erasektoriga, seda enam, et tööstusele kuulub oluline osa digi- ja muust taristust, mis on tulemuslikult kuritegevuse ja terrorismi vastu võitlemiseks keskse tähtsusega. Ka üksikisikud saavad anda oma panuse, näiteks arendades küberkuritegevuse või desinformatsiooni vastu võitlemiseks vajalikke oskusi ja teadlikkust. Lisaks peavad need ühised jõupingutused ulatuma meie piiridest kaugemale, et luua tihedamad sidemed samameelsete partneritega.

IV. Kõigi jaoks turvaline EL: julgeolekuliidu strateegilised prioriteedid

ELil on ainulaadsed võimalused nendele uutele ülemaailmsetele ohtudele ja probleemidele reageerimiseks. Eespool esitatud ohuanalüüs osutab neljale omavahel seotud strateegilisele prioriteedile, mida tuleb täielikult põhiõigusi austades ELi tasandil edendada: i) tulevikukindel julgeolekukeskkond, ii) muutuvate ohtudega tegelemine, iii) eurooplaste kaitsmine terrorismi ja organiseeritud kuritegevuse eest, iv) tugev Euroopa julgeoleku ökosüsteem.

1. Tulevikukindel julgeolekukeskkond

Elutähtsa taristu kaitse ja vastupidavusvõime

Oma igapäevaelus sõltuvad inimesed olulisest taristust – reisimisel, töötamisel, avalikes põhiteenustes (näiteks haiglad, transport, energiavarustus) ja oma demokraatlike õiguste kasutamisel. Kui nende taristute kaitse ja vastupidavusvõime ei ole piisav, võivad ründed põhjustada suuri häireid – füüsiliselt või digitaalselt – nii üksikute liikmesriikide kui ka potentsiaalselt kogu ELi jaoks.

ELi olemasolev elutähtsate taristute kaitse ja vastupidavusvõime raamistik[33] ei ole muutuvate riskidega sammu pidanud. Suurenev vastastikune sõltuvus tähendab, et ühe sektori häired võivad vahetult mõjutada teiste sektorite tegevust: rünnak elektritootmisele

---

intsidentide ja kriiside korral (C(2017) 6100), ELi hübriidohutõrje operatiivprotokoll (ELi käsiraamat) (SWD(2016) 227).

[32] Vt ühisteatis „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“ (JOIN(2017) 450).

[33] Direktiiv 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016); nõukogu direktiiv 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta.

võib rivist välja lüüa telekommunikatsiooni, haiglad, pangad või lennujaamad ning rünne digitaristule võib põhjustada häireid elektri- või finantsvõrkudes. Kuna meie majandus ja ühiskond on järjest veebipõhisemad, teravnevad sellised riskid veelgi. Sellist suuremat omavahelist seotust ja vastastikust sõltuvust tuleb õigusraamistikus silmas pidada ning näha elutähtsate taristute jaoks ette usaldusväärsed meetmed kaitse ja vastupidavusvõime tagamiseks nii küber- kui ka füüsilises mõõtmes. Olulised teenused, sealhulgas kosmosetaristul põhinevad teenused, peavad olema praeguste ja eeldatavate ohtude eest piisavalt kaitstud, kuid ka vastupidavusvõimelised. See tähendab, et süsteem suudab kahjulikuks sündmuseks valmis olla ja sellele reageerida, edasi töötada, taastuda ja selliste sündmustega edukamalt kohaneda.

Samal ajal on liikmesriigid kasutanud oma kaalutlusruumi, rakendades olemasolevaid õigusakte erineval viisil. Sellest tulenev killustatus võib õõnestada siseturgu ja muuta piiriülese koordineerimise keerulisemaks – seda kõige ilmsemalt piirialadel. Ettevõtjad, kes osutavad olulisi teenuseid eri liikmesriikides, peavad järgima erinevat aruandluskorda. Komisjon uurib, kas **nii füüsiliste kui ka digitaristute uued raamistikud** võiksid suurendada järjepidevust ja lähenemise ühtsust, et tagada oluliste teenuste usaldusväärne osutamine. Sellele raamistikule peavad lisanduma **sektoripõhised algatused**, et tegeleda konkreetsete riskidega, mis ohustavad elutähtsaid taristuid näiteks transpordi-, kosmose-, energeetika-, finants- ja tervishoiusektoris[34]. Võttes arvesse finantssektori suurt sõltuvust IT-teenustest ja selle suurt haavatavust küberrünnete suhtes, võetakse esimesena ette finantssektori digitaalse operatiivvastupidavusvõime algatus. Energiasüsteemi erilise tundlikkuse ja mõju tõttu toetatakse sihtotstarbelise algatusega elutähtsa energiataristu suuremat vastupidavusvõimet füüsiliste, küber- ja hübriidohtude suhtes, tagades samas energiaettevõtjate piiriülesed võrdsed võimalused.

Elutähtsaid taristuid või elutähtsat tehnoloogiat mõjutada võivate välismaiste otseinvesteeringute julgeolekumõjusid hindavad ka ELi liikmesriigid ja komisjon välismaiste otseinvesteeringute uue Euroopa raamistiku alusel[35].

EL saab samuti luua uusi vahendeid, et toetada elutähtsate taristute vastupidavusvõimet. Ülemaailmset internetti on seni iseloomustanud suur vastupidavusvõime, eelkõige seoses suutlikkusega toetada internetiliikluse mahtude suurenemist. Siiski peame olema valmis võimalikeks tulevasteks kriisideks, mis ohustavad interneti turvalisust, stabiilsust ja vastupidavusvõimet. Interneti toimimine eeldab jõulist sekkumist küberintsidentide ja internetis toimuva pahatahtliku tegevuse korral ning väljaspool Euroopat asuvatest taristutest ja teenustest sõltuvuse piiramist. Selleks on vaja mitmesuguseid õigusakte ja seda, et lisaks vaadataks läbi senised eeskirjad, millega tagatakse ELis võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase; suuremaid investeeringuid teadusuuringutesse ja innovatsiooni ning üle

[34] Arvestades asjaolu, et tervishoiusektor on olnud eriti COVID-19 kriisi ajal surve all, kaalub komisjon ka algatusi, millega tugevdada ELi terviseturve raamistikku ja vastutavaid ELi ameteid, et reageerida tõsistele piiriülestele terviseohtudele.

[35] Euroopa Parlamendi ja nõukogu 19. märtsi 2019. aasta määrus (EL) 2019/452 (millega luuakse liitu tehtavate välismaiste otseinvesteeringute taustauuringute raamistik) muutub täielikult kohaldatavaks 11. oktoobril 2020 ja sellega saab EL enda käsutuse uue koostöömehhanismi, mille kaudu tegeleda väljastpoolt ELi tehtavate otseinvesteeringutega, mis tõenäoliselt mõjutavad julgeolekut või avalikku korda. Määruse kohaselt hindavad liikmesriigid ja komisjon selliste välismaiste otseinvesteeringutega seotud võimalikke riske, ja kui see on asjakohane rohkem kui ühe liikmesriigi jaoks, teevad ettepaneku nende riskide maandamiseks sobivate meetmete kohta.

vaadata, kas oleks vaja juurutada või tugevdada keskse tähtsusega internetitaristut ja -ressursse, eelkõige domeeninimede süsteemi[36].

ELi ja riikide peamiste digivarade kaitseks on hädavajalik võimaldada elutähtsatele taristutele turvalist sidepidamise kanalit. Komisjon teeb liikmesriikidega koostööd, et luua maa- ja kosmosepõhine sertifitseeritud turvaline otspunktidevaheline kvanttaristu, mis kombineeritakse turvalise riikliku satelliitsidesüsteemiga, nagu on sätestatud kosmoseprogrammi määruses[37].

Küberturvalisus

Küberrünnete arv on endiselt tõusuteel[38]. Need ründed on varasemast keerukamad, pärinevad paljudest erinevatest ELi-sisestest ja -välistest allikatest ning on suunatud kõige haavatavamatele valdkondadele. Sageli on kaasatud riiklikud ja riigi toetusega osalejad, kes on sihikule võtnud taolised olulisemad digitaristud nagu suured pilvandmetöötluse pakkujad[39]. Küberriskid on muutunud oluliseks ohuks ka finantssüsteemile. Rahvusvahelise Valuutafondi hinnangul on küberrünnetega tekitatud iga-aastane kahju 9 % pankade ülemaailmsest netosissetulekust ehk ligikaudu 100 miljardit dollarit[40]. Kasutajate jaoks on ühendatud seadmetele üleminekul palju plusse. Ent olukorras, kus andmekeskustes töötlemise ja säilitamise asemel töödeldakse andmeid järjest enam kasutajale lähemal „servadel“[41], ei saa küberturvalisus enam seisneda eelkõige kesksete kohtade kaitsmises.[42]

2017. aastal esitas EL küberturvalisuse alase lähenemisviisi, mille keskmes oli vastupidavusvõime suurendamine, kiire reageerimine ja tulemuslik heidutus.[43] EL peab nüüd tagama oma küberturvalisuse võime vastavuse muutuvatele vajadustele, et tagada nii vastupidavusvõime kui ka reageerimine. See nõuab tõesti kogu ühiskonda hõlmavat lähenemisviisi, milles ELi institutsioonid, asutused ja organid, liikmesriigid, tööstus, akadeemilised ringkonnad ja üksikisikud omistavad küberturvalisusele vajaliku prioriteedi[44]. Ka selle horisontaalse lähenemisviisi täienduseks tuleb rakendada sektoripõhiseid küberturvalisuse lähenemisviise sellistes valdkondades nagu energeetika, finantsteenused, transport või tervishoid. ELi töö järgmine etapp tuleks kokku võtta läbivaadatud Euroopa Liidu küberjulgeoleku strateegias.

Luureteenistuste, ELi luure- ja situatsioonikeskuse ja muude julgeolekuga tegelevate organisatsioonide vaheliseks koostööks uute ja tõhusamate viiside kindlakstegemine peaks

---

[36] Domeeninimede süsteem (DNS) on arvutite, teenuste või internetti või privaatvõrku ühendatud muude ressursside nimede hierarhiline ja detsentraliseeritud süsteem. See tõlgib domeeninimed IP-aadressideks, mida on vaja arvutiteenuste ja -seadmete asukoha kindlakstegemiseks ja tuvastamiseks.

[37] Ettepanek: määrus, millega luuakse liidu kosmoseprogramm ja Euroopa Liidu Kosmoseprogrammi Amet (COM(2018) 447).

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Hajusate teenusetõkestusrünnete oht ei ole endiselt kuhugi kadunud: suured teenuseosutajad pidid toime tulema hajusate teenusetõkestusrünnetega, näiteks 2020. aasta veebruaris Amazoni veebiteenuste vastu toime pandud ründega.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] Servtöötlus on hajutatud avatud IT-arhitektuur, milles kasutatakse detsentraliseeritud töötlusvõimsust, mis teeb võimalikuks mobiilse andmetöötluse ja asjade interneti tehnoloogia. Servtöötluses ei edastata andmeid andmekeskusele, vaid andmeid töötleb seade ise või kohalik arvuti või server.

[42] Teatis „Euroopa andmestrateegia“ (COM(2020) 66 final).

[43] Vt ühisteatis „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, (JOIN (2017) 450).

[44] Teadusuuringute Ühiskeskuse aruandest „Küberturvalisus – meie digitaalne soomus“ leiab mitmemõõtmelisi analüüse küberturvalisuse sektori kasvust viimase 40 aasta jooksul.

olema osa jõupingutustest küberturvalisuse parandamiseks ning terrorismi, äärmusluse, radikalismi ja hübriidohtude vastu võitlemiseks.

Arvestades kõikjal ELis **5G-taristu** kasutuselevõtuga jätkamist ning paljude kriitilise tähtsusega teenuste võimalikku sõltuvust 5G-võrgust, kujuneksid süsteemse ja laiaulatusliku halvamise tagajärjed eriti raskeks. Komisjoni 2019. aasta soovituses 5G-võrkude küberturvalisuse kohta[45] kehtestatud protsessi tulemusena on liikmesriigid astunud 5G-meetmepaketi kohaste põhimeetmete jaoks konkreetseid samme[46].

Üks olulisemaid pikaajalisi vajadusi on arendada **sisseprojekteeritud küberturvalisuse** kultuuri, mis tähendab, et turvalisus on algusest peale toodetesse ja teenustesse integreeritud. Olulise panuse annab küberturvalisuse määruse kohane uus küberturvalisuse sertifitseerimise raamistik[47]. Raamistiku koostamist on juba alustatud ning kaks sertifitseerimiskava on juba jõudnud ettevalmistusetappi ja järgmiste kavade prioriteedid määratakse kindlaks käesoleva aasta lõpus. Selles valdkonnas on väga oluline Euroopa Liidu Küberturvalisuse Ameti (ENISA), andmekaitseasutuste ja Euroopa Andmekaitsenõukogu[48] vaheline koostöö.

Komisjon on juba kindlaks teinud, et struktureeritud ja koordineeritud operatiivkoostööks on vaja **ühist küberüksust**. See võiks sisaldada kriiside ajal ELi tasandil kasutatavat vastastikuse abi mehhanismi. Tegevuskava kohta antud soovituse[49] rakendamisele tuginedes võiks ühine küberüksus suurendada usaldust Euroopa küberturvalisuse ökosüsteemi eri osalejate vahel ja pakkuda liikmesriikidele olulist teenust. Komisjon alustab arutelusid asjaomaste sidusrühmadega (alustades liikmesriikidest) ning kehtestab 2020. aasta lõpuks selge protsessi, vahe-eesmärgid ja ajakava.

Samuti on oluline, et kõigil ELi institutsioonidel, organitel ja asutustel oleksid ühised infoturbe ja küberturvalisuse eeskirjad. Eesmärk peaks olema luua kohustuslikud ja kõrged ühised standardid turvaliseks teabevahetuseks ning digitaristute ja -süsteemide turvalisuseks kõigis ELi institutsioonides, organites ja asutustes. See uus raamistik peaks toetama ELi institutsioonide, organite ja asutuste tugevat ja tõhusat küberturvalisuse alast operatiivkoostööd, milles täidab keskset rolli ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm (CERT-EU).

Ülemaailmset iseloomu arvesse võttes on küberrünnete edasiseks ennetamiseks, takistamiseks ja neile reageerimiseks äärmiselt oluline tugevate **rahvusvaheliste partnerluste** loomine ja säilitamine. Pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistikus („küberdiplomaatia meetmete kogum“)[50] on sätestatud ühise välis- ja julgeolekupoliitika meetmed, sealhulgas piiravad meetmed (sanktsioonid), mida saab kasutada ELi poliitilisi, julgeoleku- ja majandushuve kahjustavale tegevusele reageerimiseks. Samuti peaks EL süvendama oma tööd arengu- ja koostööfondide raames, et toetada partnerriike nende digiökosüsteemide tugevdamisel, riiklike õigusreformide vastuvõtmisel ja rahvusvaheliste standardite järgimisel. See

[45] Komisjoni soovitus „5G-võrkude küberturvalisus“ (COM(2019) 2335 final). Soovituses nähakse ette selle läbivaatamine 2020. aasta viimases kvartalis.

[46] Vt võrgu- ja infoturbe koostöörühma aruanne meetmepaketi rakendamise kohta, 24. juuli 2020.

[47] Määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist (küberturvalisuse määrus).

[48] Teatis „Andmekaitse kodanike võimestajana ja ELi valmistumine digiüleminekuks – isikuandmete kaitse üldmääruse kohaldamise kaks esimest aastat“ (COM(2020) 264).

[49] Komisjoni soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral.

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/et/pdf

suurendab kogu kogukonna vastupidavusvõimet ja suutlikkust küberohte tõrjuda ja neile tulemuslikult reageerida. See hõlmab konkreetset tööd ELi standardite ja asjaomaste õigusaktide edendamiseks, et suurendada naabruses asuvate partnerriikide küberturvalisust[51].

Avaliku ruumi kaitse

Hiljutistes terrorirünnakutes on sihikule võetud avalik ruum, muu hulgas kultusekohad ja transpordisõlmed, ning kasutatud ära nende paikade avatust ja juurdepääsetavust. Poliitilistest või ideoloogilistest motiividest lähtuva terrorismi kasvu tõttu on kirjeldatud oht eriti terav. See tähendab, et tugevdada tuleb selliste kohtade füüsilist kaitset ning samuti on vaja piisavaid tuvastussüsteeme, mis ei õõnestaks kodanike vabadusi[52]. Komisjon tõhustab avaliku ruumi kaitseks tehtavat avaliku ja erasektori koostööd rahastamise, kogemuste ja heade tavade vahetamise, konkreetsete juhiste[53] ja soovituste abil[54]. Lähenemisviisi osaks on ka teadlikkuse suurendamine, tuvastamisseadmete toimivusnõuded ja testimine ning taustakontrolli tõhustamine, et tulla toime siseohtudega. Oluline on mõelda sellele, et mõju võib olla ebaproportsionaalselt suur vähemuste ja haavatavate isikute puhul, sealhulgas isikute puhul, kes jäävad mõjuvälja oma usulise kuuluvuse või soo tõttu, ning seepärast tuleks neile pöörata erilist tähelepanu. Avaliku ruumi turvalisuse parandamisel on oluline koht piirkondlikel ja kohalikel ametiasutustel. Komisjon aitab ühtlasi edendada linnade avaliku ruumi turvalisuse vallas toimuvat innovatsiooni[55]. Liikmesriikide, komisjoni ja linnade kindlat tahet avaliku ruumi turvalisust ähvardavate ohtudega paremini toime tulla peegeldab ka novembris 2018 alguse saanud avaliku ruumi turvalisuse alane linnade uue tegevuskava[56] partnerlus.

Droonide turg kasvab jätkuvalt ning nende kasutamiseks on palju väärtuslikke ja seaduslikke võimalusi. Samas võivad kurjategijad ja terroristid droone ka väärkasutada, seades ohtu just avaliku ruumi. Sihtmärkideks võivad olla üksikisikud, rahvakogunemised, elutähtis taristu, õiguskaitseasutused, piirid või avalik ruum. Teadmised selle kohta, kuidas droone konfliktiolukorras kasutada, võivad jõuda tagasi Euroopasse kas otse (naasvate terroristist välisvõitlejate vahendusel) või internetis. Euroopa Lennundusohutusameti välja töötatud eeskirjad on esimene oluline samm sellistes valdkondades nagu droonide käitajate registreerimine ja droonide kohustuslik kaugtuvastus. Arvestades, et droonid muutuvad üha laiemalt kättesaadavaks, taskukohasemaks ja võimekamaks, on vaja täiendavaid meetmeid. See võiks hõlmata teabe jagamist, juhiseid ja häid tavasid, mida saaksid kasutada kõik, kaasa arvatud õiguskaitseorganid, ning lisaks tuleks teha rohkem katseid droonivastaste

[51] Vt ELi välise kübersuutlikkuse suurendamise suunised, mis võeti vastu nõukogu 26. juuni 2018. aasta järeldustes.

[52] Erilise tähelepanu alla tuleb võtta biomeetrilise kaugtuvastuse süsteemid. Komisjoni esialgsed seisukohad on esitatud komisjoni 19. veebruari 2020. aasta valges raamatus tehisintellekti kohta, COM(2020) 65.

[53] Näiteks juhised avaliku ruumi kaitsmiseks nõuetekohaste turvabarjäärilahenduste valimise kohta (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Juhiseid heade tavade kohta on antud dokumendis SWD (2019) 140, mille ühes osas on käsitletud avaliku ja erasektori koostööd. Politseikoostöö, kuritegevuse tõkestamise ja selle vastu võitlemise ning kriisiohje rahastamisvahendist toimuva rahastamise puhul pööratakse avaliku ja erasektori koostööle erilist tähelepanu.

[55] Kolm linna (Pireus Kreekas, Tampere Soomes ja Torino Itaalias) hakkavad linnadega seotud uuenduslike meetmete raames katsetama uusi lahendusi; tegevust kaasrahastatakse Euroopa Regionaalarengu Fondist (ERF).

[56] ELi linnade tegevuskava kujutab endast uut mitmetasandilist töömeetodit, mis edendab liikmesriikide, linnade, Euroopa Komisjoni ja muude sidusrühmade koostööd, et tõugata tagant Euroopa linnade kasvu, suurendada elukeskkonna kvaliteeti ja lisada innovatsiooni ning aidata sotsiaalseid probleeme kindlaks teha ja nendega toime tulla.

kaitsemeetmetega[57]. Täiendavalt tuleks analüüsida ja käsitleda ka seda, kuidas mõjutab droonide kasutamine avalikus ruumis privaatsust ja andmekaitset.

Peamised meetmed
• Elutähtsa taristu kaitset ja vastupidavust käsitlevad õigusnormid • Küberturvalisuse direktiivi läbivaatamine • Finantssektori operatiivse vastupidavuse algatus • Elutähtsa energiataristu kaitse ja küberturvalisus ning piiriüleste elektrivoogude küberturvalisuse võrgueeskiri • Euroopa küberturvalisuse strateegia • Järgmised sammud ühise küberüksuse loomise suunas • ELi institutsioonide, organite ja asutuste infoturbe ja küberturvalisuse ühiseeskirjad • Tihedam koostöö avaliku ruumi kaitsel, muu hulgas kultusekohtades. • Heade tavade jagamine droonide väärkasutamisega toimetuleku kohta

2. Arenevate ohtudega tegelemine

Küberkuritegevus

Tehnoloogia pakub ühiskonnale uusi võimalusi ning loob uusi vahendeid ka kohtusüsteemile ja õiguskaitsele, kuid samal ajal avab see uusi võimalusi ka kurjategijatele. Üha rohkem esineb pahavara, häkkimist isikuandmete ja ettevõtteandmete varastamiseks ning rahalist või mainekahju põhjustavat digitaalse tegevuse katkestamist. Esmast kaitset pakub tugeva küberturvalisuse loodud vastupidav keskkond. Õiguskaitseasutused peavad saama tegeleda digitaalse uurimisega ning olemas peavad olema selged reeglid selle kohta, kuidas kuritegusid uurida ja nende eest vastutusele võtta ning kuidas pakkuda ohvritele vajalikku kaitset. Sellealane tegevus peaks tuginema Europoli küberkuritegevusega tegeleva ühise töökonna tegevusele ja suuremahulistele küberrünnetele reageerimise koordineerimiseks loodud hädaolukordades õiguskaitsealase reageerimise protokollile. Olulised on ka tõhusad mehhanismid, mis võimaldavad avaliku ja erasektori partnerlust.

Samal ajal peaks küberkuritegevuse vastasest võitlusest saama kogu ELis strateegiline kommunikatsiooniprioriteet, et hoiatada eurooplasi ohtudest ja anda teada, milliseid ennetusmeetmeid võiks võtta. Kõik see peaks olema proaktiivse lähenemisviisi osa. Veel üks oluline samm on praeguse õigusraamistiku[58] täielik rakendamine: komisjon on valmis kasutama vajaduse korral rikkumismenetlusi ning tegeleb kõnealuse raamistiku läbivaatamisega, et tagada selle otstarbekohasus. Ühtlasi uurib komisjon koos Europoli ja ELi küberturvalisuse ametiga (ENISA), milline oleks küberkuritegudest varajase hoiatamise ELi süsteemi teostatavus, et tagada küberkuritegude ilmnemise korral teabe liikumine ja sujuv reageerimine.

Küberkuritegevus on ülemaailmne probleem, millega toimetulekuks on vaja tõhusat rahvusvahelist koostööd. EL toetab Euroopa Nõukogu küberkuritegevuse konventsiooni (Budapesti konventsioon), mis on mõjus ja hästi sissetöötatud raamistik, mis võimaldab kõigil riikidel kindlaks teha, millised süsteemid ja sidekanalid tuleb omavahelise tulemusliku koostöö jaoks luua.

[57] Hiljuti loodi mitmeaastane katseprogramm, et toetada liikmesriike ühise metoodika ja katseplatvormi väljatöötamisel selles valdkonnas.

[58] Direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid.

Peaaegu pooled ELi kodanikud tunnevad muret andmete väärkasutamise pärast[59] ja **identiteedivargused** on suur probleem[60]. Identiteedi kuritarvitamine rahalise kasu saamiseks on vaid üks aspekt, millele võib lisanduda märkimisväärne isiklik ja psühholoogiline mõju, sest identiteedivarga tehtud ebaseaduslikud postitused võivad internetti jääda aastateks. Komisjon uurib, milliste praktiliste meetmetega võiks ohvreid igasuguse identiteedivarguse eest kaitsta, võttes arvesse tulevast Euroopa digitaalse identiteedi algatust[61].

Küberkuritegevusest jagu saamiseks tuleb mõelda tulevikule. Nii nagu ühiskonnas kasutatakse uusi tehnoloogilisi lahendusi majanduse ja ühiskonna tugevdamiseks, võivad kurjategijad püüda samu vahendeid kasutada halbadel eesmärkidel. Näiteks võivad kurjategijad kasutada tehisintellekti, et avastada või tuvastada paroole, lihtsustada pahavara loomist või kasutada ära kujutisi ja heli, mille toel teostada identiteedivargusi või pettusi.

Tänapäevane õiguskaitse

Õiguskaitsjad ja õigusvaldkonna töötajad peavad uue tehnoloogiaga kohanema. Tehnika areng ja tekkivad ohud tähendavad, et õiguskaitseasutustel peab olema juurdepääs uutele vahenditele ning nad peavad omandama uusi oskusi ja arendama alternatiivseid uurimismeetodeid. Täiendamaks õiguslikke meetmeid, mille eesmärk on parandada kriminaaluurimistes piiriülest juurdepääsu elektroonilistele tõenditele, võib EL aidata õiguskaitseasutustel arendada suutlikkust, mida on vaja, et teha kindlaks kuritegude uurimiseks vajalikud andmed, neid turvata ja lugeda ning neid andmeid kohtus tõendusmaterjalina kasutada. Komisjon uurib, mis meetmetega saaks **suurendada õiguskaitseasutuste suutlikkust digitaalsete uurimiste valdkonnas,** ning selgitab välja, kuidas kasutada õiguskaitse jaoks uute vahendite loomiseks võimalikult hästi teadus- ja arendustegevust ning kuidas pakkuda õiguskaitsele ja kohtutele koolitustega vajalikke oskusi. Ühtlasi hõlmab see rangete teaduslike hindamiste ja katsemetoodika pakkumist komisjoni Teadusuuringute Ühiskeskuse kaudu.

Ühiste lähenemisviisidega võib samuti tagada, et **intellektitehnika, kosmosealane suutlikkus, suurandmed** ja **kõrgjõudlusega andmetöötlus** integreeritakse turbepoliitikasse viisil, mis annab tulemusi nii kuritegevuse vastases võitluses kui ka põhiõiguste tagamisel. Intellektitehnika võib olla kuritegevuse vastases võitluses võimas töövahend, mis loob tohutult suure uurimissuutlikkuse ning võimaldab analüüsida suuri infohulki ja tuvastada neis mustreid ja hälbeid[62]. Samas võivad intellektitehnikal põhinevad tööriistad olla ka spetsiifilisemad ja aidata näiteks kindlaks teha terroristlikku veebisisu, avastada ohtlike toodete müügis kahtlasi tehinguid või pakkuda kodanikele hädaolukorras abi. Kirjeldatud potentsiaali realiseerimiseks tuleb teadusuuringud, innovatsioon ja intellektitehnika kasutajad viia kokku õige juhtimise ja tehnilise taristuga, kaasates sellesse aktiivselt ka erasektori ja akadeemilised ringkonnad. Sealjuures tuleb tagada põhiõiguste järgimise rangeimad standardid ning kodanike tulemuslik kaitse. Esmajoones tähendab see, et kui

[59] 46 % (Eurobaromeetri uuring eurooplaste suhtumise kohta küberturvalisusesse, jaanuar 2020).

[60] Suur osa (95 %) inimestest, kes vastas 2018. aasta Eurobaromeetri uuringule eurooplaste suhtumise kohta internetiturvalisusse, pidas identiteedivargust raskeks kuriteoks ja 70 % ütles, et see on väga raske kuritegu. 2020. aasta jaanuaris avaldatud Eurobaromeetri uuring kinnitas, et küberkuritegevus, võrgupettused ja identiteedivargused on muret tekitavad: pangapettuste ja identiteedivarguste pärast muretses kaks kolmandikku vastanutest (vastavalt 67 % ja 66 %).

[61] 19. veebruari 2020. aasta teatis Euroopa digituleviku kujundamise kohta, COM (2020) 67.

[62] Näiteks finantskuritegude puhul.

tehakse üksikisikuid mõjutavaid otsuseid, peavad inimesed need läbi vaatama ning need peavad vastama asjaomastele kohaldatavatele ELi õigusnormidele[63].

Elektroonilist teavet ja elektroonilisi tõendeid on vaja umbes 85 % raskete kuritegude uurimisel ning 65 % kõigist päringutest lähevad teises õigusruumis paiknevatele isikutele.[64]. See, et tavapärased materiaalsed jäljed on asendunud võrgus olevatega, suurendab veelgi lõhet õiguskaitse ja kurjategijate suutlikkuse vahel. On äärmiselt oluline, et kehtestatakse selged õigusnormid, mis reguleerivad kriminaalasjades piiriülest juurdepääsu elektroonilistele tõenditele. Seepärast ongi elektroonilisi tõendeid käsitlevate ettepanekute kiire vastuvõtmine Euroopa Parlamendis ja nõukogus nii oluline, et anda selles valdkonnas töötajate käsutusse tõhus töövahend. Oluline on ka mitme- ja kahepoolsete rahvusvaheliste läbirääkimistega tagatav piiriülene juurdepääs elektroonilistele tõenditele, et kehtestada rahvusvahelisel tasandil võrreldavad normid[65].

Juurdepääs digitaalsetele tõenditele sõltub ka teabe kättesaadavusest. Kui andmed kustutatakse liiga kiiresti, võivad olulised tõendid kaduda ning seega kaob ka kahtlusaluste ja kuritegelike võrgustike (aga ka ohvrite) tuvastamise ja nende asukoha kindlaks tegemise võimalus. Teisalt tekitavad andmete säilitamise süsteemid küsimusi seoses privaatsuse kaitsega. Komisjon hindab andmete säilitamise edasisi võimalusi lähtuvalt sellest, milliseks kujuneb Euroopa Kohtus pooleli olevate kohtuasjade tulemus.

Kriminaaluurimiste, küberturvalisuse ja tarbijakaitse jaoks on oluline juurdepääs interneti domeeninimede registreerimise teabele (nn Whois teave)[66]. Paraku muutub juurdepääs sellele teabele üha keerulisemaks ning uute Whois-põhimõtete vastuvõtmine on Interneti Aadressikorporatsioonis (ICANN) praegu alles pooleli. Komisjon jätkab koostööd ICANNi ja arvukaid sidusrühmi koondava kogukonnaga tagamaks, et õiguspäraselt andmetele juurdepääsu taotlejatel, sh õiguskaitsel on võimalik saada tõhus juurdepääs WHOISi andmetele kooskõlas ELi ja rahvusvaheliste andmekaitsenormidega. See eeldab võimalike lahenduste hindamist, muu hulgas näiteks selle, kas sellisele teabele juurdepääsu eeskirjade selgemaks muutmiseks oleks vaja õigusakte.

Õiguskaitse- ja õigusasutused peavad olema valmis saama vajalikke andmeid ja tõendeid ka siis, kui ELis on **mobiilside jaoks võetud täielikult kasutusele 5G arhitektuur**, ning sealjuures tuleb austada side konfidentsiaalsust. Komisjon toetab rahvusvaheliste standardite loomisel tõhustatud ja koordineeritud lähenemisviisi, mille raames määratakse kindlaks parimad tavad, protsessid ja tehniline koostalitlusvõime tehnika sellistes olulistes valdkondades nagu intellektitehnika, asjade internet ja plokiaheltehnoloogiad.

Tänapäeval on kuritegude ja terrorismi kõigi vormide uurimisest oluline osa seotud **krüpteeritud teabega**. Krüpteerimine on digimaailmas äärmiselt oluline, sest see võimaldab turvata digisüsteeme ja tehinguid ning kaitsta mitmesuguseid põhiõigusi, kaasa arvatud väljendusvabadust, privaatsust ja andmekaitset. Ent kuritegelikul otstarbel kasutatuna võib see samas varjata kurjategijate identiteeti ja peita nende sideseansside sisu. Komisjon uurib

---

[63] See tähendab vastavust kehtivatele õigusaktidele, kaasa arvatud isikuandmete kaitse üldmäärusele (määrus (EL) 2016/679), aga ka direktiivile, mis käsitleb isikuandmete kaitset õiguskaitse valdkonnas (direktiiv (EL) 2016/680) ja millega reguleeritakse isikuandmete töötlemist süütegude avastamise, tõkestamise, uurimise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil.

[64] Komisjoni talituste töödokument (2018) 118 final

[65] Eelkõige Euroopa Nõukogu küberkuritegevuse konventsiooni (Budapesti konventsiooni) teine lisaprotokoll küberkuritegevuse kohta ning ELi ja Ameerika Ühendriikide vaheline leping, mis käsitleb piiriülest juurdepääsu elektroonilistele tõenditele.

[66] Neid andmeid hoitakse andmebaasides, mille haldamisega tegeleb 2500 registrit ja registri käitajat kõikjal maailmas.

ja toetab tasakaalukaid tehnilisi, operatiivseid ja õiguslikke lahendusi võimalikele probleemidele ning propageerib lähenemisviisi, mis ühest küljest säilitaks krüpteerimise tõhususe privaatsuse ja side turvalisuse kaitsmisel ning teisalt võimaldaks kuritegevusele ja terrorismile tulemuslikult vastu astuda.

Võitlus ebaseadusliku veebisisuga

Võrgukeskkonna ja reaalse maailma turvalisuse vastavusse viimine eeldab pidevat **võitlust ebaseadusliku veebisisuga**. Peamised kodanikke ähvardavad ohud, näiteks terrorism, äärmuslus ja laste seksuaalne kuritarvitamine on üha enam seotud digitaalse keskkonnaga. See tähendab, et põhiõiguste järgimise tagamiseks on vaja konkreetseid meetmeid ja raamistikku. Esimese sammuna on oluline viia sujuvalt lõpule läbirääkimised terroristlikku veebisisu käsitleva õigusakti ettepaneku[67] üle ning tagada selle rakendamine. Õiguskaitseasutuste ja erasektori vabatahtliku koostöö tugevdamine **ELi internetifoorumis** on samuti oluline, et võidelda interneti kuritarvitamisega terroristide, vägivaldsete äärmuslaste ja kurjategijate poolt. Europoli internetisisust teavitamise üksus teeb jätkuvalt olulist tööd terrorirühmituste tegevuse jälgimisel internetis ja platvormide meetmete seire vallas,[68] aga ka **ELi kriisiprotokolli arendamisel**[69]. Lisaks sellele jätkab komisjon suhtlemist rahvusvaheliste partneritega ning osaleb sealhulgas **ülemaailmse terrorismivastase võitluse internetifoorumi tegevuses**, et püüda leida neile probleemidele lahendus ülemaailmsel tasandil. Jätkub töö selle nimel, et toetada alternatiivsete narratiivide ja vastupropaganda väljatöötamist kodanikuühiskonna tugevdamise programmi kaudu[70].

Internetis leviva ebaseadusliku vaenukõne ärahoidmiseks ja sellega võitlemiseks avaldas komisjon 2016. aastal internetis leviva vihakõne vastase võitluse tegevusjuhendi, millega koos võtsid digiplatvormid vabatahtliku kohustuse kõrvaldada vaenukõnet sisaldavad materjalid. Värskeim hindamine näitab, et ettevõtted analüüsivad 90 % neile teatatud sisust 24 tunni jooksul ja eemaldavad 71 % ebaseaduslikuks vaenukõneks peetud sisust. Samas peavad platvormid parandama läbipaistvust ja kasutajatele antavat tagasisidet ning tagama neile teatatud sisu hindamisel järjepidevuse[71].

ELi internetifoorum soodustab olemasolevat ja arendusjärgus tehnoloogiat käsitlevat infovahetust, et lahendada probleeme, mis seonduvad laste seksuaalse kuritarvitamisega internetis. Võitlus laste seksuaalse kuritarvitamisega internetis on kesksel kohal uues strateegias, mis käsitleb jõulisemat **võitlust laste seksuaalse kuritarvitamise vastu**[72] ning mille eesmärk on kasutada selliste kuritegudega võitlemiseks maksimaalselt ära ELi tasandil kättesaadavaid vahendeid. Ettevõtted peavad saama jätkata oma tööd, et avastada internetist lastepornot ja see sealt kõrvaldada. Selliste materjalide tekitatava kahjuga tegelemine eeldab probleemi lahendamiseks selgeid ja alalisi kohustusi sisaldavat raamistikku. Samuti teatatakse strateegias, et komisjon hakkab ette valmistama sektorispetsiifilist õigusakti, et tegeleda internetis laste seksuaalse kuritarvitamise teemaga tõhusamalt, austades sealjuures igati põhiõigusi.

Üldisemas plaanis selgitatakse ja uuendatakse tulevases digiteenuste õigusaktis digiteenustega seotud vastutust ja turvaeeskirju ning kõrvaldatakse takistavad asjaolud, mis pidurdavad tegelemist ebaseadusliku sisu, kaupade või teenustega.

---

67 Ettepanek terroristliku veebisisu levitamise tõkestamise kohta, COM(2018) 640, 12.september 2018.
68 Europol, november 2019.
69 A Europe that protects - EU Crisis Protocol: responding to terrorist content online. (oktoober 2019).
70 Seotud radikaliseerumisalase teadlikkuse programmi raames tehtava tööga, vt punkt IV.3 allpool.
71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf
72 ELi strateegia, mis käsitleb tõhusamat võitlust laste seksuaalse väärkohtlemise vastu (COM(2020) 607).

Lisaks sellele jätkab komisjon suhtlemist rahvusvaheliste partneritega ja **ülemaailmse terrorismivastase võitluse internetifoorumiga**, tehes seda muu hulgas sõltumatu nõuandekomitee kaudu, et arutada, kuidas lahendada kirjeldatud probleemid üleilmsel tasandil, säilitades sealjuures ELi väärtused ja põhiõigused. Tegeleda tuleks ka uute teemadega, nagu algoritmid või võrgumängud[73].

Hübriidohud

Nüüdsel ajal on hübriidohud erakordselt ulatuslikud ja mitmekesised. COVID-19 kriis andis sellest taas kord märku, kui mitu riiki ja mitteriiklikku instantsi püüdsid pandeemiat oma huvides ära kasutada, seda eeskätt infokeskkonna manipuleerimise ja kesksete taristute proovile panemisega. See toob kaasa sotsiaalse ühtekuuluvuse vähenemise ohu ja õõnestab usaldust ELi institutsioonide ja liikmesriikide valitsuste vastu.

Seda, kuidas EL läheneb hübriidohtudele, on kirjeldatud 2016. aasta ühises raamistikus[74] ja 2018. aasta ühisteatises hübriidohtudega võitlemise suutlikkuse suurendamise kohta[75]. ELi tasandi tegevuse aluseks on mitmekesised vahendid, mida saab kasutada nii sise- kui ka välisküsimuste puhul ning mis põhinevad kogu ühiskonda hõlmaval lähenemisviisil ja tihedal koostööl strateegiliste partnerite, eeskätt NATO ja G7-ga. Aruanne selle kohta, kuidas ELi lähenemisviisi hübriidohtudele on rakendatud, avaldatakse koos käesoleva strateegiaga[76]. Käesoleva strateegiaga samal ajal tutvustatud kaardistuse[77] põhjal loovad komisjoni talitused ja Euroopa välisteenistus **piiratud võrguplatvormi**, mis hakkab pakkuma liikmesriikidele tutvumiseks infot ELi tasandil hübriidohtudega võitlemiseks kasutatavate vahendite ja vastumeetmete kohta.

Vastutus hübriidohtudele vastu astumise eest lasub peamiselt liikmesriikidel, sest see valdkond on lahutamatult seotud riikliku julgeoleku ja kaitsepoliitikaga, kuid mõned haavatavused esinevad kõigi liikmesriikide puhul ja mõned ohud on piiriülesed, näiteks juhul, kui sihikule võetakse piiriülesed võrgud või taristu. Komisjon ja kõrge esindaja koostavad ELi lähenemisviisi hübriidohtudele, milles kombineeritakse sujuvalt välised ja sisemised aspektid ning viiakse kokku riike ja kogu ELi puudutavad argumendid. Selline lähenemisviis peab hõlmama kogu meetmeteskaalat alates varajasest avastamisest, analüüsist, teadlikkusest ja vastupidavuse suurendamisest kuni kriisidele reageerimise ja sellele järgneva kriisiohjeni.

Lisaks jõulisemale rakendamisele tuleb hübriidohtude pideva arenguga sammu pidamiseks pöörata erilist tähelepanu **hübriidohtudega seotud aspektide integreerimisele üldisesse poliitika kujundamisse**, et kiirest arengust mitte maha jääda ja tagada, et ükski potentsiaalselt oluline algatus ei jääks tähelepanuta. Hübriidohtude võimalust tuleb arvesse võtta ka uute algatuste mõju hindamisel. Seda ka juhul, kui algatus puudutab seni hübriidohtudega võitlemisest kaugele jäänud valdkondi, näiteks haridust, tehnoloogiat või teadusuuringuid. Sellise lähenemisviisi jaoks oleks kasu hübriidohtude mõiste määratlemiseks tehtud tööst, sest see annab põhjaliku ülevaate erinevatest vahenditest, mida

[73] Terroristid kasutavad teabevahetuseks üha rohkem mänguplatvormide sõnumisüsteeme ning noored terroristid kordavad videomängudes vägivaldseid rünnakuid.

[74] Hübriidohtudega võitlemise ühine raamistik – Euroopa Liidu vastumeetmed, JOIN (2016) 18.

[75] Vastupanuvõime tugevdamine ja suutlikkuse suurendamine võitluseks hübriidohtudega, JOIN (2018) 16.

[76] SWD(2020) 153, aruanne 2016. aasta teatise „Hübriidohtudega võitlemise ühine raamistik“ ja 2018. aasta ühisteatise „Vastupanuvõime tugevdamine ja suutlikkuse suurendamine võitluseks hübriidohtudega“ rakendamise kohta.

[77] SWD(2020) 152, vastupanuvõime parandamise ja hübriidohtude vastu võitlemisega seotud meetmete kaardistamine.

vastased võivad kasutada[78]. Eesmärk peaks olema tagada, et otsustusprotsess tugineb korrapärastele ja põhjalikele, luureandmetel põhinevatele aruannetele hübriidohtude arengu kohta. Selline tegevus sõltub suuresti liikmesriikide luureteabest ja ELi luure- ja situatsioonikeskuse kaudu liikmesriikide pädevate asutustega tehtava luurealase koostöö tõhustamisest.

Olukorrateadlikkuse arendamiseks uurivad komisjoni talitused ja Euroopa välisteenistus, kuidas saaks eri allikatest (sh liikmesriikidest, aga ka ELi ametitest, nt ENISAst, Europolist ja Frontexist) pärit infovooge optimeerida. ELis koondub hübriidohtude hindamise alane tegevus peamiselt ELi hübriidohtude ühisüksusse. **Vastupidavuse suurendamine** on hübriidohtude ärahoidmisel ja nende eest kaitsmisel äärmiselt tähtis. Seepärast on väga oluline selle valdkonna edusammudel pidevalt silma peal hoida ja neid objektiivselt mõõta. Esimese sammuna tuleb nii liikmesriikide kui ka ELi institutsioonide ja asutuste puhul kindlaks teha hübriidohtudele vastupidavuse sektoripõhine baastase. Lisaks eespool kirjeldatud meetmetele tuleks suurendada valmisolekut hübriidkriisidele reageerimiseks; selleks tuleks läbi vaadata 2016. aastal välja töötatud ELi käsiraamatus[79] kindlaks määratud protokoll, et võtta arvesse ELi kriisile reageerimise süsteemi praegu käimasolevat laialdasemat läbivaatamist ja tugevdamist[80]. Eesmärk on saavutada ELi tegevuse maksimaalne mõju valdkondlike reaktsioonide koondamise ja partneritega (eeskätt NATOga) tehtava sujuva koostöö tagamisega.

Peamised meetmed
• Küberkuritegevust käsitlevate õigusaktide rakendamise ja otstarbekohasuse tagamine • Strateegia, mis käsitleb tõhusamat võitlust laste seksuaalse väärkohtlemise vastu • Ettepanekud lasteporno avastamise ja kõrvaldamise kohta • ELi lähenemisviis hübriidohutõrjele • ELi hübriidohutõrje operatiivprotokolli (ELi käsiraamat) läbivaatamine • Hinnang sellele, kuidas suurendada õiguskaitseasutuste suutlikkust tegeleda digitaalse uurimisega

3. Eurooplaste kaitsmine terrorismi ja organiseeritud kuritegevuse eest

Terrorism ja radikaliseerumine

ELis on suur terrorismioht. Kuigi rünnakute üldarv on vähenenud, võib nende mõju olla sellele vaatamata laastav. Samuti võib radikaliseerumine ühiskonda laiemalt lõhestada ja sotsiaalset ühtekuuluvust häirida. Terrorismi ja radikaliseerimise vastu võitlemise eest vastutavad eeskätt liikmesriigid, ent ohu piiriülesus/sektoriülesus kasvab üha ning see tähendab, et ELi koostöös ja koordineerimises tuleb võtta lisameetmeid. ELi terrorismivastase võitluse alaste õigusnormide, kaasa arvatud piiravate meetmete[81]

[78] „The Landscape of Hybrid Threats: A conceptual Model“, JRC117280, valminud Teadusuuringute Ühiskeskuse ja Euroopa Hübriidohutõrje Oivakeskuse ühistööna.

[79] ELi hübriidohutõrje operatiivprotokoll (ELi käsiraamat), (SWD(2016) 227).

[80] Pärast 26. märtsil 2020 toimunud videokonverentsi võtsid Euroopa Ülemkogu liikmed vastu avalduse, mis käsitleb ELi meetmeid COVID-19 puhangule reageerimisel ning milles kutsuti komisjoni üles esitama ettepanekud ELi ambitsioonikama ja laiaulatuslikuma kriisiohjesüsteemi kohta.

[81] Nõukogu kehtestas terrorismi piiravad meetmed ISISe (Daesh) ja Al-Qaida suhtes ning eripiirangud teatavate isikute ja üksuste vastu, et võidelda terrorismi vastu. Kõigist piiravatest meetmetest ülevaate saamiseks vt ELi sanktsioonide kaarti (https://www.sanctionsmap.eu/#/main).

tulemuslik rakendamine on esmatähtis. Üheks eesmärgiks on endiselt Euroopa Prokuratuuri ülesannete laiendamine piiriülestele terrorikuritegudele.

Terrorismivastane võitlus eeldab tegelemist terrorismi algpõhjustega. Ühiskonna lõhestumine, tegelik või tajutav diskrimineerimine ning muud psühholoogilised ja sotsioloogilised tegurid võivad muuta inimesed vastuvõtlikumaks radikaalse diskursuse suhtes. Sellistes oludes tuleb **radikaliseerumise** vastu võitlemiseks suurendada sotsiaalset ühtekuuluvust nii kohalikul ja riiklikul kui ka Euroopa tasandil. Viimase kümne aasta jooksul on välja töötatud mitu mõjusat algatust ja poliitikameedet, eeskätt on seda tehtud radikaliseerumisalase teadlikkuse võrgustiku ja algatuse „ELi linnad radikaliseerumise vastu“ raames[82]. Nüüd on aeg mõelda meetmete peale, millega ühtlustada ELi poliitikat, algatusi ja vahendeid, et radikaliseerumise probleemile vastu astuda. Selliste meetmetega saab toetada suutlikkuse ja oskuste arendamist, parandada koostööd, tugevdada tõendusbaasi ja aidata hinnata saavutatud edu, kaasates kõik sidusrühmad, kaasa arvatud eesliinil tegutsejad, poliitikakujundajad ja teadlased[83]. Pehmed poliitikavaldkonnad, nagu haridus, kultuur, noored ja sport võiksid aidata radikaliseerumist ennetada ning pakkuda riskirühmade noortele võimalusi ja ühtekuuluvustunnet ELi sees[84]. Prioriteetide hulka kuulub töö varajase avastamise ja riskijuhtimisega, vastupanuvõime suurendamine ja suhete katkestamine, aga ka rehabiliteerimine ja ühiskonda taasintegreerimine.

Terroristid on püüdnud omandada **keemilisi, bioloogilisi, kiirgus- ja tuumamaterjale** (KBRT)[85] ja neid relvadena kasutada ning ühtlasi arendada teadmisi ja suutlikkust, et neid materjale kasutada[86]. Terroristlikus propagandas on KBRT-rünnakute potentsiaal sagedane teema. Võimalik kahju oleks väga suur ja seega tuleb olla eriti ettevaatlik. Komisjon analüüsib lõhkeainete lähteainetele juurdepääsu reguleerimises kasutatavale lähenemisviisile tuginedes võimalusi piirata juurdepääsu teatavatele ohtlikele kemikaalidele, mida võidaks kasutada rünnakute korraldamiseks. Seega on oluline ka ELi kodanikukaitsealase suutlikkuse (rescEU) arendamine KBRT vallas. Samuti on tähtis koostöö kolmandate riikidega, et tõhustada KBRT ohutuse ja julgeoleku valdkonnas ühist kultuuri, kasutades sealjuures ELi üleilmsete KBRT tippkeskuste kõiki võimalusi. Selline koostöö hõlmab riiklikke puuduste ja riskide hindamisi, riiklike ja piirkondlike KBRT tegevuskavade toetamist, heade tavade vahetamist ja KBRT alase suutlikkuse suurendamise meetmeid.

EL on välja töötanud maailma kõige progressiivsemad õigusaktid, et piirata juurdepääsu **lõhkeainete lähteainetele**[87] ja avastada kahtlasi tehinguid, mille eesmärk on valmistada isetehtud lõhkeseadmeid. Samas on isetehtud lõhkeainete oht endiselt suur ning neid on ELis kasutatud mitmes rünnakus[88]. Esimeseks sammuks peab olema õigusnormide rakendamine, ent ühtlasi tuleb tagada, et võrgukeskkonnas ei saa kontrollimeetmetest mööda hiilida.

---

[82] Katsealgatusel „ELi linnad radikaliseerumise vastu“ on kaks eesmärki: soodustada ELi linnade vahel eksperditeadmiste vahetamist ja koguda tagasisidet selle kohta, kuidas ELi tasandil kohalikke kogukondi kõige paremini toetada.

[83] Näiteks rahastamine Euroopa julgeolekufondist ja kodakondsuse programmist.

[84] ELi meetmed, näiteks Erasmus+ virtuaalsed vahetusprogrammid, eTwinning.

[85] Viimasel kahel aastal on nii Euroopas (Prantsusmaal, Saksamaal, Itaalias) kui ka mujal (Tuneesias, Indoneesias) aset leidnud mitu juhtumit, milles kasutati bioloogilisi mõjureid (enamasti taimseid toksiine).

[86] Nõukogu kehtestas keemiarelvade leviku ja kasutamise vastased piiravad meetmed.

[87] Kemikaalid, mida võib vääriti kasutada isevalmistatud lõhkeainete komponentidena. Nende ainete suhtes kohaldatakse määrust (EL) 2019/1148 lõhkeainete lähteainete turustamise ja kasutamise kohta.

[88] Sellised laastavad rünnakud toimusid näiteks Oslos (2011), Pariisis (2015), Brüsselis (2016) ja Manchesteris (2017). Lyonis (2019) sai isevalmistatud lõhkeainega korraldatud rünnakus viga 13 inimest.

Terrorismivastase võitluse poliitika oluline osa on ka terrorikuritegude toimepanijate, sealhulgas praegu Süürias ja Iraagis tegutsevate **terroristist välisvõitlejate** tõhus kohtu alla andmine. Kuigi nende teemadega tegelevad eeskätt liikmesriigid, võib ELi poolne koordineerimine ja toetus aidata liikmesriikidel ühistest probleemidest üle saada. Olulised on meetmed, mida juba võetakse piirijulgeolekut käsitlevate õigusaktide täielikuks rakendamiseks[89] ja kõigi asjaomaste ELi andmebaaside igakülgseks kasutamiseks, et jagada teavet teadaolevate kahtlusaluste kohta. Lisaks potentsiaalselt ohtlike isikute kindlakstegemisele on vaja ka taasintegreerimise ja rehabiliteerimise poliitikat. Kutsealadevaheline koostöö, mis hõlmab ka vanglatöötajaid ja kriminaalhooldajaid, tugevdab kohtute arusaamist vägivaldse ekstremismini viivast radikaliseerumisest ja õigussektori lähenemist karistuste määramisele ja kinnipidamise alternatiividele.

Terroristist välisvõitlejate problemaatika on sise- ja **välisjulgeoleku** vahelistele seostele väga iseloomulik. Koostöö, mida tehakse terrorismivastases võitluses ning radikaliseerimise ja vägivaldse äärmusluse ennetamiseks ja sellega võitlemiseks, on ELi sisejulgeoleku seisukohast keskse tähtsusega[90]. Terrorismivastase võitluse alaste partnerluste ning naabruskonna ja kaugemate riikidega tehtava koostöö arendamiseks tuleb astuda täiendavaid samme, tuginedes ELi terrorismivastase võitluse ja/või julgeoleku valdkonna ekspertide võrgustiku kogemustele. Sellise sihipärase koostöö hea näide on Lääne-Balkani terrorismivastase võitluse ühine tegevuskava. Eeskätt tuleks tegutseda selle nimel, et toetada partnerriikide suutlikkust terroristist välisvõitlejaid tuvastada ja nende asukoht kindlaks teha. Lisaks propageerib EL ka edaspidi mitmepoolset koostööd ning tegutsemist koos selle valdkonna maailma mastaabis juhtivate organisatsioonidega, nagu Ühinenud Rahvaste Organisatsioon, NATO, Euroopa Nõukogu ja OSCE. Ühtlasi teeb ta koostööd ülemaailmse terrorismivastase võitluse foorumi ja ülemaailmse Daeshi-vastase koalitsiooni ning asjaomaste kodanikuühiskonna esindajatega. Terrorismi ja piraatluse ärahoidmiseks kolmandate riikidega tehtavas koostöös on oluline koht ka liidu välispoliitika vahenditel, sh arengupoliitikal ja koostööl. **Terrorismi rahastamise** kõigi allikate kõrvaldamiseks on oluline teha koostööd ka rahvusvahelises plaanis, näiteks rahapesuvastase töökonna kaudu.

Organiseeritud kuritegevus

Organiseeritud kuritegevus põhjustab suuri kulusid nii kogu majandusele kui ka üksikisikutele. Hinnanguliselt põhjustavad organiseeritud kuritegevus ja korruptsioon majandusele aastas 218–282 miljardit eurot kahju[91]. Euroopas oli 2017. aastal uurimise all üle 5000 organiseeritud kuritegeliku rühmituse – seda on 50 % rohkem kui 2013. aastal[92]. Organiseeritud kuritegevus on üha enam piiriülene ja lähtub muu hulgas ELi lähinaabrusest. See tähendab, et on vaja intensiivsemat operatiivkoostööd ja teabevahetust naabruskonna partneritega.

Esile kerkivad uued probleemid ning kuritegevus kolib internetti: COVID-19 pandeemia ajal kasvas järsult haavatavate elanikkonnarühmade vastu suunatud võrgupettuste arv ning vargustes ja sissemurdmistes võeti sihikule tervise- ja hügieenitooted[93]. EL peab

[89] Sealhulgas Euroopa Piiri- ja Rannikuvalve Ameti (Frontex) uued ülesanded.

[90] Nõukogu 16. juuni 2020. aasta järeldustes rõhutati, et ELi kodanikke on vaja kaitsta terrorismi ja vägivaldse äärmusluse kõigi vormide eest olenemata selle päritolust ning tugevdada tuleb ELi terrorismivastast välistegevust ja meetmeid teatavates esmatähtsates geograafilistes ja temaatilistes valdkondades.

[91] Võrreldes sisemajanduse koguproduktiga (SKP); Europoli aruanne „Does crime still pay? – Criminal asset recovery in the EU“, 2016.

[92] Europol, raske ja organiseeritud kuritegevuse põhjustatud ohtude hinnangud (SOCTA), 2013 ja 2017.

[93] Europol, 2020.

organiseeritud kuritegevuse jõulisemalt käsile võtma ka rahvusvahelisel tasandil ning kasutama nende ärimudeli lõhkumiseks rohkem vahendeid. Võitlus organiseeritud kuritegevusega eeldab tihedat koostööd kohalike ja piirkondlike haldusasutuste ja kodanikuühiskonnaga, kes on olulised partnerid nii kuritegevuse ennetamisel kui ka ohvrite abistamisel ja toetamisel, kusjuures vajadused on eriti suured piirialade haldusasutuste seas. Kirjeldatud tegevuste kohta on kavas koostada **organiseeritud kuritegevuse vastu võitlemise tegevuskava**.

Rohkem kui kolmandik ELis tegutsevatest kuritegelikest organisatsioonidest on seotud uimastite tootmise, uimastitega kauplemise või uimastite levitamisega. 2019. aastal tõi uimastisõltuvus kaasa rohkem kui 8000 üledoosist põhjustatud surma. Valdavalt on **ebaseaduslik uimastikaubandus** piiriülene ja suur osa kasumist imbub legaalsesse majandusse[94]. ELi uus uimastitevastane programm[95] tugevdab ELi ja liikmesriikide jõupingutusi, et vähendada nõudlust uimastite järele ja nende pakkumist, ning aitab kindlaks määrata ühismeetmed, mille abil lahendada ühine probleem ning kindlustada ELi ja välispartnerite uimasteid käsitlevat dialoogi ja koostööd. Pärast Euroopa Narkootikumide ja Narkomaania Seirekeskuse hindamist analüüsib komisjon, kas nende mandaati on vaja uute probleemide valguses ajakohastada.

Organiseeritud kuritegelikud rühmitused ja terroristid on põhitegijad ka **ebaseaduslike tulirelvadega** kauplemises. Aastatel 2009–2018 toimus Euroopas 23 massitulistamist, mille käigus tapeti üle 340 inimese[96]. Tulirelvi tuuakse ELi selle lähinaabruse kaudu[97]. See osutab vajadusele tugevdada koordineerimist ja koostööd nii ELis kui ka rahvusvaheliste partneritega, eelkõige Interpoliga, et ühtlustada teabe kogumist ja aruandlust tulirelvade konfiskeerimise kohta. Samuti on oluline parandada relvade jälgitavust, sealhulgas internetis, ning tagada teabevahetus litsentse väljastavate ja õiguskaitseasutuste vahel. Komisjon esitab uue **ELi tulirelvade salakaubaveo vastase tegevuskava**[98] ning hindab ka seda, kas tulirelvade ekspordilubasid, importi ja transiiti käsitlevad eeskirjad on endiselt eesmärgikohased[99].

Kuritegelikud organisatsioonid käsitlevad rändajaid ja rahvusvahelist kaitset vajavaid inimesi kaubana. 90 % ELi saabuvatest ebaseaduslikest rändajatest toovad sisse kuritegelikud võrgustikud.[100] Rändajate ebaseaduslik üle piiri toimetamine on sageli seotud ka muude organiseeritud kuritegevuse vormidega, eelkõige inimkaubandusega[101]. Lisaks inimkaubandusega kaasnevatele tohututele inimkuludele on Europoli hinnangul kõigist inimkaubandusega seotud ärakasutamise vormidest saadav kasum kogu maailmas 29,4 miljardit eurot aastas. Tegu on rahvusvahelise kuritegevusega, mis põhineb ebaseaduslikul nõudlusel nii ELis kui ka sellest väljaspool, ning mõjutab kõiki ELi liikmesriike. Nende kuritegude tuvastamise, nende eest süüdistuse esitamise ja süüdimõistmise puudulikkus nõuab uut lähenemisviisi meetmete tõhustamisele. Uus **terviklik lähenemisviis**

---

94 EMCDDA ja Europol, „EU Drug Markets Report 2019“. (2019 november)

95 ELi uimastitevastane programm ja tegevuskava aastateks 2021–2025, COM(2020) 606.

96 Flemish Peace Institute, Armed to kill. (oktoober 2019).

97 EL on rahastanud väike- ja kergrelvade leviku ja salakaubaveo vastast võitlust piirkonnas alates 2002. aastast; ta on rahastanud eelkõige Kagu-Euroopa tulirelvaekspertide võrgustikku (SEEFEN). Alates 2019. aastast on Lääne-Balkani partnerid olnud täielikult kaasatud kuritegevusega seotud ohte käsitleva valdkondadevahelise Euroopa platvormi (EMPACT) tulirelvade prioriteeti.

98 COM (2020) 608.

99 Määrus (EL) nr 258/2012, millega rakendatakse tulirelvade ebaseaduslikku valmistamist ja nendega ebaseaduslikku kauplemist tõkestava ÜRO protokolli artiklit 10.

100 Allikas: Europol.

101 Europol, EMSC, 4. aastaaruanne.

inimkaubandusele koondab kokku tegevussuunad. Lisaks esitab komisjon **uue ELi tegevuskava rändajate ebaseadusliku üle piiri toimetamise tõkestamiseks** aastateks 2021–2025. Mõlemad tegevussuunad keskenduvad kuritegelike võrgustike vastu võitlemisele, koostöö tugevdamisele ja õiguskaitsealase töö toetamisele.

Organiseeritud kuritegelikud rühmitused – nagu ka terroristid – otsivad võimalusi ka muudes valdkondades, eelkõige väikese avastamisriskiga suurt tulu toovates valdkondades, nagu **keskkonnakuriteod**. Ebaseaduslik jahipidamine ja elusloodusega kauplemine, ebaseaduslik kaevandamine, metsaraie ning ebaseaduslik jäätmete kõrvaldamine ja vedu on muutunud maailmas suuruselt neljandaks kuritegelikuks äriks[102]. Samuti on kuritegelikult ära kasutatud heitkogustega kauplemise ja energiasertifikaatide süsteeme ning väärkasutatud keskkonna vastupidavusvõime suurendamisele ja säästvale arengule eraldatud vahendeid. Lisaks ELi, liikmesriikide ja rahvusvahelise üldsuse keskkonnakuritegude vastase võitluse tõhustamismeetmete edendamisele[103] hindab komisjon, kas keskkonnakuritegude direktiiv[104] täidab endiselt oma eesmärki. **Kultuuriväärtuste salakaubandus** on muutunud samuti üheks kõige tulusamaks kuritegevuse liigiks, terroristide ja organiseeritud kuritegevuse rahastamisallikaks, ja see üha laieneb. Tuleks uurida võimalusi, kuidas parandada kultuuriväärtuste jälgitavust siseturul (veebis ja ka mujal) ja koostööd kolmandate riikidega, kus kultuuriväärtusi rüüstatakse.

Majandus- ja finantskuriteod on väga keerukad, kuid mõjutavad igal aastal miljoneid ELi kodanikke ja tuhandeid ettevõtjaid. Pettusevastane võitlus on väga oluline ja nõuab ELi tasandi meetmeid. Europol koos Eurojusti, Euroopa Prokuratuuri ja Euroopa Pettustevastase Ametiga toetavad liikmesriike ja ELi majandus- ja finantsturgude kaitsmisel ning ELi maksumaksjate raha säilitamise tagamisel. Euroopa Prokuratuur hakkab täielikult toimima 2020. aasta lõpus ning hakkab uurima ELi eelarvet kahjustavaid kuritegusid, nagu pettus, korruptsioon ja rahapesu, ning esitama nende eest süüdistusi ja viima teostajaid kohtu ette. Samuti aitab see võidelda piiriüleste käibemaksupettustega, mis lähevad maksumaksjatele maksma vähemalt 50 miljardit eurot aastas.

Komisjon toetab ka eksperditeadmiste ja õigusraamistiku arendamist seoses esilekerkivate riskidega, nagu krüptovarad ja uued maksesüsteemid. Eelkõige võtab komisjon arvesse algatust, milles käsitletakse reageerimist selliste krüptovarade nagu *bitcoin*, tekkimisele ja uue tehnoloogia mõjule finantsvarade emiteerimisele, nendega börsil kauplemisele, nende jagamisele ja neile juurdepääsule.

Euroopa Liidus peaks olema ebaseadusliku raha suhtes nulltolerants. Kolmekümne aasta jooksul on EL välja töötanud tugeva õigusraamistiku **rahapesu** ja terrorismi rahastamise tõkestamiseks ja nende vastu võitlemiseks, võttes täielikult arvesse vajadust kaitsta isikuandmeid. Siiski ollakse üha enam üksmeelel, et praeguse raamistiku rakendamist tuleb oluliselt täiustada. Kõrvaldada tuleb suured erinevused nimetatud raamistiku kohaldamises ja tõsised puudused eeskirjade jõustamisel. Nagu on üksikasjalikult kirjeldatud 2020. aasta mai tegevuskavas,[105] on käimas töö, et hinnata võimalusi ELi rahapesu ja terrorismi rahastamise vastase võitluse raamistiku tõhustamiseks. Uuritavate valdkondade hulka kuulub riiklike pangakontode keskregistrite ühendamine, mis võiks oluliselt kiirendada rahapesu andmebüroode ja pädevate ametiasutuste juurdepääsu finantsteabele.

[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime, juuni 2016.
[103] Vt „Euroopa roheline kokkulepe“ (COM (2019) 640 final).
[104] Direktiiv 2008/99/EL keskkonna kaitsmise kohta kriminaalõiguse kaudu.
[105] Rahapesu ja terrorismi rahastamise tõkestamise tegevuskava (COM (2020) 2800).

Organiseeritud kuritegelike rühmituste kasum ELis on hinnanguliselt 110 miljardit eurot aastas. Praegused vastumeetmed hõlmavad konfiskeerimist ja kuritegeliku vara tagasivõitmist käsitlevaid ühtlustatud õigusakte,[106] et tõhustada kuritegeliku vara arestimist ja konfiskeerimist ELis ning hõlbustada vastastikust usaldust ja mõjusat piiriülest koostööd liikmesriikide vahel. Siiski konfiskeeritakse ainult umbes 1 % sellest tulust,[107] mis võimaldab organiseeritud kuritegelikel rühmitustel investeerida oma kuritegeliku tegevuse laiendamisse ja imbuda seaduslikku majandusse; eelkõige on rahapesu sihtmärgiks väikesed ja keskmise suurusega ettevõtted, kellel on raskusi laenude saamisega. Komisjon analüüsib õigusaktide rakendamist[108] ja võimalikku vajadust täiendavate ühiste eeskirjade järele, sealhulgas konfiskeerimist ilma süüdimõistva kohtuotsuseta. Kriminaaltulu jälitamise talitustele,[109] kes on kuritegeliku vara tagasivõitmise protsessi peamised osalised, võiks samuti anda paremad vahendid varade kiiremaks tuvastamiseks ja jälitamiseks kogu ELis, et suurendada konfiskeerimise määrasid.

Organiseeritud kuritegevuse ja **korruptsiooni** vahel on tugev seos. Hinnanguliselt läheb ainuüksi korruptsioon ELi majandusele maksma 120 miljardit eurot aastas[110]. Korruptsiooni ennetamise ja korruptsioonivastase võitluse jälgimine jätkub korrapäraselt õigusriigi mehhanismi ja Euroopa poolaasta raames. Euroopa poolaasta raames on hinnatud korruptsioonivastase võitluse probleemseid valdkondi, nagu riigihanked, avalik haldus, ettevõtluskeskkond või tervishoid. Komisjoni uues iga-aastases aruandes õigusriigi olukorra kohta käsitletakse korruptsioonivastast võitlust ning võimaldatakse ennetavat dialoogi riiklike ametiasutuste ja huvitatud sidusrühmadega ELi ja riiklikul tasandil. Kodanikuühiskonna organisatsioonidel võib samuti olla võtmeroll avaliku sektori asutuste tegevuse stimuleerimisel organiseeritud kuritegevuse ja korruptsiooni ennetamisel ja nende vastu võitlemisel ning need rühmad võiks kokku viia ühiseks foorumiks. Nende piiriülese olemuse tõttu on teine oluline mõõde koostöö ELi naaberpiirkondadega ja abi andmine organiseeritud kuritegevuse ja korruptsiooni valdkonnas.

Peamised meetmed
• ELi terrorismivastane tegevuskava, sealhulgas uuendatud radikaliseerumisvastased meetmed ELis • Uus koostöö oluliste kolmandate riikide ja rahvusvaheliste organisatsioonidega terrorismivastase võitluse valdkonnas • Organiseeritud kuritegevuse, sealhulgas inimkaubanduse vastu võitlemise tegevuskava • ELi narkootikumidealane tegevuskava aastateks 2021–2025 • Narkootikumide ja Narkomaania Euroopa Järelevalvekeskuse hindamine • Ebaseadusliku tulirelvakaubanduse vastane ELi tegevuskava 2020–2025 • Vara arestimist ja konfiskeerimist ning kriminaaltulu jälitamise talitusi käsitlevate õigusaktide läbivaatamine • Keskkonnakuritegude direktiivi hindamine

[106] ELi õiguse kohaselt peavad kriminaaltulu jälitamise talitused olema asutatud kõikides liikmesriikides.

[107] Aruanne „Vara sissenõudmine ja konfiskeerimine: meetmed kuritegevuse mittetasuvaks muutmisel“ (COM(2020) 217).

[108] Direktiiv 2014/42/EL kuriteovahendite ja kriminaaltulu arestimise ja konfiskeerimise kohta.

[109] Nõukogu otsus 2007/845/JSK, mis käsitleb kriminaaltulu jälitamise talituste vahelist koostööd kuritegelikul teel saadud tulu või kuritegevusega seotud muu vara jälitamise ja tuvastamise valdkonnas.

[110] Korruptsiooni majanduslike kogukulude hindamine on keeruline, ehkki sellised organid nagu Rahvusvaheline Kaubanduskoda, Transparency International, ÜRO Global Compact ja Maailma Majandusfoorum on teinud jõupingutusi, mille tulemused viitavad sellele, et korruptsioon moodustab 5 % maailma SKPst.

- ELi tegevuskava rändajate ebaseadusliku üle piiri toimetamise tõkestamiseks (2021-2025)

4. Tugev Euroopa julgeoleku ökosüsteem

Tõeline ja tõhus julgeolekuliit peab olema ühiskonna kõigi osade ühine ettevõtmine. Valitsused, õiguskaitseasutused, erasektor, haridus ja kodanikud ise peavad olema kaasatud, varustatud ja nõuetekohaselt ühendatud, et suurendada kõigi, eelkõige kõige haavatavamate, ohvrite ja tunnistajate valmisolekut ja vastupanuvõimet.

Kõik poliitikavaldkonnad vajavad julgeolekumõõdet ja EL saab anda oma panuse kõigil tasanditel. Koduvägivald on üks tõsisemaid turvariske. ELis on 22 % naistest kogenud lähisuhtevägivalda[111]. ELi ühinemine naistevastase vägivalla ja perevägivalla ennetamise ja tõkestamise Istanbuli konventsiooniga jääb peamiseks prioriteediks. Kui läbirääkimised ei edene, võtab komisjon muid meetmeid, et saavutada konventsiooniga samad eesmärgid, sealhulgas teeb ettepaneku lisada naistevastane vägivald ELi aluslepingus määratletud kuritegude nimekirja.

Koostöö ja teabevahetus

Üks olulisemaid panuseid, mida EL saab kodanike kaitsmisel anda, on aidata julgeoleku eest vastutavatel isikutel teha head koostööd. Koostöö ja teabevahetus on kõige võimsamad vahendid kuritegevuse ja terrorismi vastu võitlemiseks ning õiguskaitse tagamiseks. Tõhususe tagamiseks peab see olema sihipärane ja õigeaegne. Usaldusväärsuse tagamiseks tuleb seda kasutada koos ühiste kaitsemeetmete ja kontrollidega.

Liikmesriikide vahelise **operatiivse õiguskaitsealase koostöö** edasiarendamiseks on loodud mitmeid ELi vahendeid ja valdkondlikke strateegiaid[112]. Üks peamisi ELi vahendeid, millega toetatakse õiguskaitsealast koostööd liikmesriikide vahel, on Schengeni infosüsteem, mida kasutatakse tagaotsitavate ja kadunud isikute ning esemete kohta reaalajas andmete vahetamiseks. Tulemusi on tunda kurjategijate vahistamises, uimastite konfiskeerimises ja võimalike ohvrite päästmises[113]. Koostöö taset saaks aga veelgi parandada, ühtlustades ja ajakohastades olemasolevaid vahendeid. Suurem osa õiguskaitsealase operatiivkoostöö aluseks olevast ELi õigusraamistikust töötati välja 30 aastat tagasi. Paljude aegunud või alakasutatud liikmesriikidevaheliste kahepoolsete lepingute keerukas võrgustik võib põhjustada killustumist. Väiksemates või sisemaariikides peavad piiriüleselt töötavad õiguskaitseametnikud võtma operatiivmeetmeid, järgides mõnel juhul kuni seitset erinevat eeskirjadekogumit. Tulemuseks on see, et mõned operatsioonid, näiteks kahtlusaluste jälitamine üle sisepiiride, lihtsalt ei toimu. ELi praegune raamistik ei hõlma ka operatiivkoostööd uute tehnoloogiate, näiteks droonide valdkonnas.

Operatiivtöö tõhusust saab toetada konkreetse õiguskaitsealase koostööga, mis võib aidata anda olulist toetust ka muudele poliitikaeesmärkidele, näiteks anda julgeolekualast teavet välismaiste otseinvesteeringute uueks hindamiseks. Komisjon uurib, kuidas võiks seda toetada politseikoostöö seadustik. Liikmesriikide õiguskaitseasutused on üha enam kasutanud ELi tasandi toetust ja oskusteavet, samal ajal kui ELi luure- ja situatsioonikeskusel on olnud oluline roll liikmesriikide luure- ja julgeolekuteenistuste

[111] „Võrdõiguslikkuse liit: soolise võrdõiguslikkuse strateegia 2020–2025“ (COM (2020) 152).

[112] Näiteks ELi merendusjulgeoleku strateegia tegevuskava, mis tõi kaasa olulised saavutused rannikuvalveülesannete alases koostöös asjaomaste ELi ametite vahel.

[113] ELi võitlus organiseeritud kuritegevuse vastu 2019. aastal (nõukogu, 2020).

vahelise strateegilise luureteabe vahetamise edendamisel, mis annab ELi institutsioonidele ülevaate luure olukorrast[114]. **Europolil** võib olla samuti oluline roll kolmandate riikidega tehtava koostöö laiendamisel, et võidelda kuritegevuse ja terrorismi vastu kooskõlas muude ELi välispoliitika valdkondade ja vahenditega. Europol seisab praegu aga silmitsi mitmete tõsiste piirangutega, eelkõige seoses isikuandmete otsese vahetamisega eraõiguslike osapooltega, mis takistab tal tõhusalt toetamast liikmesriike võitluses terrorismi- ja kuritegevuse vastu. Praegu hinnatakse Europoli volitusi, et näha, kuidas neid tuleks täiendada, et amet saaks oma ülesandeid täielikult täita. Seoses sellega peaksid ka ELi tasandi asjaomased asutused (nt OLAF, Europol, Eurojust ja Euroopa Prokuratuur) tegema tihedamat koostööd ja parandama teabevahetust.

Veel üks oluline seos on **Eurojusti** edasiarendamine, et maksimeerida õiguskaitse- ja õigusalase koostöö koostoimet. EL saaks kasu ka suuremast strateegilisest sidususest: organiseeritud ja rasket rahvusvahelist kuritegevust käsitlev ELi poliitikatsükkel **EMPACT**[115] pakub ametiasutustele kriminaaljälitusel põhinevat metoodikat, et ühiselt võidelda kõige olulisemate ELi mõjutavate kuritegelike ohtudega. See on andnud viimase kümne aasta jooksul olulisi tulemusi[116]. Praktikute kogemustele tuginedes tuleks olemasolevat mehhanismi uueks poliitikatsükliks 2022–2025 ühtlustada ja lihtsustada, et paremini tegeleda kõige pakilisemate ja arenevate kuritegelike ohtudega.

Õigeaegne ja asjakohane **teave** on igapäevatöös kuritegude lahendamisel keskse tähtsusega. Vaatamata uute ELi tasandi julgeoleku ja piirihalduse andmebaaside väljatöötamisele asub suur osa teabest endiselt riiklikes andmebaasides või seda vahetatakse väljaspool neid vahendeid. Tulemuseks on märkimisväärne lisatöö, viivitused ja suurem oht, et oluline teave jääb leidmata. Paremad, kiiremad ja lihtsamad protsessid, mis hõlmavad kõiki julgeolekuringkondi, annaksid paremaid tulemusi. Õiged vahendid on olulised selleks, et teabevahetus täidaks oma potentsiaali kuritegevuse tõhusal jälitamisel koos vajalike kaitsemeetmetega, et andmete jagamisel peetaks kinni andmekaitsealastest õigusaktidest ja põhiõigustest. Võttes arvesse tehnoloogia, kohtuekspertiisi ja andmekaitse arengut ning muutunud operatiivvajadusi, võiks EL kaaluda, kas on vaja ajakohastada selliseid vahendeid nagu **2008. aasta Prümi otsused** (millega pandi alus DNA-, sõrmejälgede ja sõidukite registreerimisandmete automatiseeritud vahetamisele), et võimaldada liikmesriikide kriminaal- või muudes andmebaasides kriminaaluurimise eesmärgil juba kättesaadavate täiendavate andmekategooriate automatiseeritud vahetamist. Lisaks uurib komisjon võimalust vahetada karistusregistri andmeid, et aidata tuvastada, kas isik on kantud teiste liikmesriikide karistusregistrisse, ning hõlbustada juurdepääsu nendele andmetele, kui need on tuvastatud, koos kõigi vajalike kaitsemeetmetega.

Rändajaid käsitlev teave on aidanud parandada piirikontrolli, vähendada ebaseaduslikku rännet ja tuvastada julgeolekuohtu kujutavaid isikuid. Reisijaid käsitlev eelteave on iga reisija biograafilised andmed, mille lennuettevõtjad koguvad lennule registreerimise ajal ja saadavad eelnevalt sihtkoha piirivalveasutustele. Õigusraamistiku[117] läbivaatamine võiks võimaldada teabe tõhusamat kasutamist, tagades samal ajal andmekaitsealaste õigusaktide järgimise ja hõlbustades reisijate liikumist. Broneeringuinfo (PNR) on teave, mida reisijad

[114] EU INTCEN on ainus kanal, mille kaudu liikmesriikide luure- ja julgeolekuteenistused saavad pakkuda ELile luureandmetel põhinevat olukorrateadlikkust.
[115] EMPACT on kuritegevusega seotud ohte käsitlev valdkondadevaheline Euroopa platvorm.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.
[117] Nõukogu direktiiv 2004/82/EÜ veoettevõtjate kohustuse kohta edastada reisijaid käsitlevaid andmeid.

lennu broneerimisel esitavad. Broneeringuinfo direktiivi[118] rakendamine on võtmetähtsusega ning komisjon jätkab selle toetamist ja jõustamist. Lisaks algatab komisjon vahemeetmena **broneeringuinfo kolmandatele riikidele edastamist** käsitleva praeguse lähenemisviisi läbivaatamise.

Õigusalane koostöö on vajalik täiendus politsei jõupingutustele piiriülese kuritegevuse vastu võitlemisel. Õigusalases koostöös on viimase 20 aasta jooksul toimunud põhjalikum muutus. Sellistel asutustel nagu **Euroopa Prokuratuur** ja **Eurojust** peavad olema vahendid oma täielikuks toimimiseks või neid tuleb tugevdada. Samuti võiks tõhustada õigusalatöötajate koostööd, võttes täiendavaid meetmeid kohtuotsuste ja õigusalase koolituse vastastikuse tunnustamise ning teabevahetuse valdkonnas. Eesmärk peaks olema kohtunike ja prokuröride vastastikuse usalduse suurendamine, mis on keskse tähtsusega piiriüleste menetluste sujuvaks toimimiseks. Meie kohtusüsteemide tõhusust võib parandada ka **digitaaltehnoloogiate** kasutamine. Eurojusti toetusel on loomisel uus digitaalne teabevahetussüsteem Euroopa uurimismääruste, vastastikuse õigusabi taotluste ja sellega seotud teadete edastamiseks liikmesriikide vahel. Komisjon teeb liikmesriikidega koostööd, et kiirendada vajalike IT-süsteemide kasutuselevõttu riiklikul tasandil.

Tõhusa õiguskaitse ja õigusalase koostöö eeltingimuseks on ka rahvusvaheline koostöö. Peamiste partneritega sõlmitud kahepoolsetel lepingutel on oluline roll teabe ja tõendite hankimisel väljastpoolt ELi. Oluline roll on **Interpolil**, mis on üks suurimaid valitsustevahelisi kriminaalpolitsei organisatsioone. Komisjon uurib võimalusi tugevdada koostööd Interpoliga, sealhulgas võimalikku juurdepääsu Interpoli andmebaasidele ning operatiiv- ja strateegilise koostöö tugevdamist. ELi õiguskaitseasutused tuginevad kurjategijate ja terroristide avastamiseks ja uurimiseks ka peamistele partnerriikidele. **ELi ja kolmandate riikide vahelisi julgeolekupartnerlusi** võiks tugevdada, et tihendada koostööd selliste ühiste ohtude vastu võitlemisel nagu terrorism, organiseeritud kuritegevus, küberkuritegevus, laste seksuaalne kuritarvitamine ja inimkaubandus. Selline lähenemisviis põhineks ühistel julgeolekuhuvidel ning tugineks väljakujunenud koostöö- ja julgeolekudialoogidele.

Lisaks teabevahetusele võib eriti väärtuslik olla oskusteabe vahetamine, et suurendada õiguskaitseasutuste valmisolekut **mittetraditsioonilisteks ohtudeks**. Lisaks parimate tavade vahetamisele innustamisele uurib komisjon ka võimalikku **politseijõudude ELi tasandi koordineerimismehhanismi** vääramatu jõu juhtumite, näiteks pandeemiate korral. Pandeemia on samuti tõestanud, et digitaalkogukonna põhine politseitöö koos internetipolitseitööd hõlbustavate õigusraamistikega saab olema kuritegevuse ja terrorismi vastases võitluses keskse tähtsusega. Politsei ja kogukondade vahelised partnerlused nii internetis kui ka väljaspool seda võivad ennetada kuritegevust ning leevendada organiseeritud kuritegevuse, radikaliseerumise ja terroristliku tegevuse mõju. Kohalike ja piirkondlike ning riiklike ja ELi politseilahenduste vaheline side on ELi julgeolekuliidu kui terviku peamine edutegur.

Tugevate välispiiride tähtsus

Nüüdisaegne ja tõhus välispiiride haldamine hoiab Schengeni ala terviklikkust ja tagab meie kodanikele julgeoleku. Kõigi asjaomaste osalejate kaasamine võimalikult parema julgeoleku saavutamisse piiril võib aidata tõeliselt kaasa piiriülese kuritegevuse ja terrorismi

[118] Direktiivi (EL) 2016/681, mis käsitleb broneeringuinfo kasutamist terroriaktide ja raskete kuritegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks.

ennetamisele. Hiljuti tugevdatud Euroopa piiri- ja rannikuvalve[119] ühine operatiivtegevus aitab kaasa piiriülese kuritegevuse ennetamisele ja avastamisele **välispiiridel** ja väljaspool ELi. Tolli tegevus kõigi kaupade ohutus- ja julgeolekuriskide tuvastamiseks enne nende saabumist ELi ning kaupade kontrollimiseks nende saabumisel on otsustava tähtsusega võitluses piiriülese kuritegevuse ja terrorismi vastu. Tulevases tolliliidu tegevuskavas kuulutatakse välja meetmed, mille eesmärk on tugevdada ka riskijuhtimist ja tõhustada sisejulgeolekut, sealhulgas hinnates eelkõige asjaomaste infosüsteemide vahelise seose teostatavust julgeolekuriskide analüüsimiseks.

ELi justiits- ja siseküsimuste valdkonna **infosüsteemide koostalitlusvõime** raamistik võeti vastu 2019. aasta mais. Selle uue struktuuri eesmärk on parandada uute või ajakohastatud infosüsteemide tõhusust ja mõjusust[120]. See annab õiguskaitse-, piirivalve- ja rändeametnikele kiirema ja süstemaatilisema teabe. See aitab isikut õigesti tuvastada ja võidelda identiteedipettuste vastu. Selle saavutamiseks peaks koostalitlusvõime rakendamine olema prioriteet nii poliitilisel kui ka tehnilisel tasandil. ELi ametite ja kõigi liikmesriikide tihe koostöö on äärmiselt oluline, et saavutada 2023. aastaks täieliku koostalitlusvõime eesmärk.

Reisidokumentide võltsimist peetakse üheks kõige sagedamini toimepandavaks kuriteoks. See hõlbustab kurjategijate ja terroristide ebaseaduslikku liikumist ning mängib põhirolli inim- ja uimastikaubanduses[121]. Komisjon uurib, kuidas laiendada käimasolevat tööd ELi elamis- ja reisidokumentide turvastandarditega, sealhulgas digitaliseerimise kaudu. Alates 2021. aasta augustist hakkavad liikmesriigid väljastama ühtlustatud turvastandarditele vastavaid isikutunnistusi ja elamislubasid, millel on biomeetrilisi tunnuseid sisaldav kiip, ja mida saavad kontrollida kõik ELi piirivalveasutused. Komisjon jälgib nende uute eeskirjade rakendamist, sealhulgas praegu ringluses olevate dokumentide järkjärgulist asendamist.

Julgeolekualaste teadusuuringute ja innovatsiooni tõhustamine

Küberjulgeoleku tagamiseks ning organiseeritud kuritegevuse, küberkuritegevuse ja terrorismi vastu võitlemiseks tehtav töö sõltub suurel määral selle tuleviku jaoks vajalike vahendite väljatöötamisest, mis aitaksid luua ohutumaid ja turvalisemaid uusi tehnoloogiaid, lahendada tehnoloogiatest tulenevaid probleeme ning toetada õiguskaitse tööd. See omakorda sõltub erasektori partneritest ja tööstusest.

Innovatsiooni tuleks vaadelda strateegilise vahendina, mille abil võidelda praeguste ohtudega ning prognoosida nii tulevasi riske kui ka võimalusi. Uuenduslikud tehnoloogiad võivad pakkuda uusi vahendeid, et aidata õiguskaitsjaid ja muid julgeolekuvaldkonnas tegutsejaid. Tehisintellekti ja suurandmete analüüsi puhul võiks kasutada kõrgjõudlusega andmetöötlust, et võimaldada paremat avastamist ning kiiret ja põhjalikku analüüsi[122]. Usaldusväärsete tehnoloogiate väljatöötamise peamine eeltingimus on kvaliteetsed andmekogumid, mis on pädevatele asutustele kättesaadavad algoritmide treenimiseks, testimiseks ja valideerimiseks[123]. Üldisemas plaanis on tehnoloogilise sõltuvuse oht praegu

[119] Koosneb Euroopa Piiri- ja Rannikuvalve Ametist (Frontex) ning liikmesriikide piirivalve- ja rannikuvalveasutustest.

[120] Riiki sisenemise ja riigist lahkumise süsteem (EES), Euroopa reisiinfo ja -lubade süsteem (ETIAS), laiendatud Euroopa karistusregistrite infosüsteem (ECRIS–TCN), Schengeni infosüsteem, viisainfosüsteem ja tulevikus ajakohastatav Eurodac.

[121] Dokumendipettuse ja inimkaubanduse vaheline seos on esitatud teises aruandes inimkaubandusevastases võitluses tehtud edusammude kohta (COM (2018) 777) ja sellele lisatud töödokumendis SWD (2018) 473 ning Europoli 2016. aasta aruandes inimkaubanduse olukorra kohta ELis.

[122] See peaks tuginema komisjoni tehisintellektistrateegiale.

[123] Euroopa andmestrateegia (COM (2020) 66 final).

suur – EL on näiteks küberturvalisuse toodete ja teenuste netoimportija ning sellega kaasneb mõju majandusele ja elutähtsatele taristutele. Tehnoloogia arendamiseks ja tarnete järjepidevuse tagamiseks ka ebasoodsate sündmuste ja kriiside korral on Euroopal vaja kohalolu ja suutlikkust asjakohaste väärtusahelate olulistes osades.

ELi **teadusuuringud, innovatsioon ja tehnoloogiaarendus** pakuvad võimalust võtta nende tehnoloogiate ja nende rakenduste väljatöötamisel arvesse julgeolekumõõdet. Järgmise põlvkonna ELi rahastamisettepanekud võivad toimida olulise stiimulina[124]. Euroopa andmeruume ja pilvandmetöötluse taristuid käsitlevaid algatusi on algusest peale arvesse võetud. Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskuse ning riiklike koordineerimiskeskuste võrgustiku[125] eesmärk on luua tulemuslik ja tõhus struktuur küberturvalisuse alaste teadusuuringute alase suutlikkuse ja tulemuste koondamiseks ja jagamiseks. Liidu kosmoseprogrammiga osutatakse teenuseid, mis toetavad ELi, selle liikmesriikide ja üksikisikute julgeolekut[126].

Alates 2007. aastast on käivitatud üle 600 projekti koguväärtusega ligikaudu 3 miljardit eurot. ELi rahastatavad julgeolekualased teadusuuringud on peamine vahend, mille abil edendatakse tehnoloogiat ja teadmisi julgeolekulahenduste toetamiseks. Europoli volituste läbivaatamise raames uurib komisjon võimalust luua **Euroopa sisejulgeoleku innovatsioonikeskus**,[127] mille eesmärk oleks pakkuda ühiseid lahendusi ühistele julgeolekuprobleemidele ja võimalusi, mida liikmesriigid ei pruugi suuta üksi ära kasutada. Koostöö on väga oluline selleks, et investeeringud oleksid võimalikult mõjusad ja arendaksid uuenduslikke tehnoloogiaid, millest on kasu nii julgeolekule kui ka majandusele.

Oskuste omandamine ja teadlikkuse suurendamine

Teadlikkus julgeolekuküsimustest ja oskuste omandamine võimalike ohtudega toimetulekuks on väga olulised, et ehitada üles vastupanuvõimelisem ühiskond, kus on paremini ettevalmistatud ettevõtted, haldusasutused ja üksikisikud. IT-taristu ja e-süsteemidega seotud probleemid on toonud esile vajaduse parandada inimeste valmisolekut ja reageerimisvõimet küberturvalisuse valdkonnas. Pandeemia on juhtinud tähelepanu ka digitaliseerimise tähtsusele kõigis ELi majanduse ja ühiskonna valdkondades.

Isegi **põhiteadmised julgeolekuohtudest** ja sellest, kuidas nende vastu võidelda, võivad avaldada tõelist mõju ühiskonna vastupidavusvõimele. Küberkuritegevuse ohtude ja end selle eest kaitsmise vajaduse teadvustamine koos teenuseosutajate pakutava kaitsega võib aidata võidelda küberrünnakute vastu. Teave uimastikaubanduse ohtude kohta võib piirata kurjategijate edukust. EL saab ergutada parimate tavade levitamist, näiteks turvalisema

[124] Komisjoni ettepanekutega programmi „Euroopa horisont“, Sisejulgeolekufondi, integreeritud piirihalduse fondi, InvestEU programmi, Euroopa Regionaalarengu Fondi ja digitaalse Euroopa programmi kohta toetatakse uuenduslike julgeolekutehnoloogiate ja -lahenduste väljatöötamist ja kasutuselevõttu kogu julgeoleku väärtusahelas.

[125] 12. septembri 2018. aasta ettepanek luua Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus ning riiklike koordineerimiskeskuste võrgustik (COM (2018) 630).

[126] Näiteks Copernicus pakub teenuseid, mis võimaldavad ELi välispiiride valvamist ja mereseiret, mis aitab võidelda piraatluse ja salakaubanduse vastu, ning toetada elutähtsaid infrastruktuure. Kui see on täielikult toimiv, saab see olema tsiviil- ja sõjaliste missioonide ja operatsioonide peamine võimaldaja.

[127] See teeks koostööd ka Euroopa Piiri- ja Rannikuvalve Ameti/Frontexi, CEPOLi, eu-LISA ja Teadusuuringute Ühiskeskusega.

interneti keskuste[128] võrgustiku kaudu, ning tagada, et selliseid eesmärke võetakse arvesse ELi enda programmides.

Tulevane digiõppe tegevuskava peaks sisaldama sihtotstarbelisi meetmeid kogu elanikkonna IT-turvaoskuste arendamiseks. Hiljuti vastu võetud oskuste tegevuskava[129] toetab oskuste elukestvat arendamist. See hõlmab sihtotstarbelisi meetmeid, et suurendada kõrgkoolilõpetajate arvu loodusteaduste, tehnoloogia, inseneriteaduste, kunsti ja matemaatika erialadel, kuna neid vajatakse sellistes tipptehnoloogia valdkondades nagu küberturvalisus. Digitaalse Euroopa programmist rahastatavad lisameetmed võimaldavad spetsialistidel pidada sammu arengutega julgeolekuohtude maastikul ning samal ajal kõrvaldada puudujäägid ELi tööturul selles valdkonnas. Üldine mõju seisneb selles, et inimestel on võimalik omandada julgeolekuohtudega toimetulekuks vajalikke oskusi ning ettevõtjatel on võimalik leida endale selles valdkonnas vajalikke spetsialiste. Tulevased Euroopa teadusruum ja Euroopa haridusruum propageerivad ka karjääre loodusteaduste, tehnoloogia, inseneriteaduste, kunsti ja matemaatika valdkonnas.

Oluline on ka **ohvrite** võimalus oma õigusi kasutada; nad peavad saama vajalikku abi ja toetust, mida nad oma konkreetses olukorras vajavad. Erilist tähelepanu tuleb pöörata vähemustele ja kõige haavatavamatele ohvritele, nagu seksuaalse ärakasutamise eesmärgil inimkaubanduse ohvriks langenud või koduvägivalla ohvriks langenud lapsed ja naised[130].

Õiguskaitsealaste oskuste parandamisel on eriline roll. Praegused ja uued tehnoloogilised ohud nõuavad suuremaid investeeringuid õiguskaitsetöötajate oskuste täiendamisse kogu nende karjääri jooksul. CEPOL on oluline partner, kes abistab liikmesriike selle ülesande täitmisel. Rassismi ja ksenofoobiat ning kodanike õigusi üldisemalt käsitlev õiguskaitsealane koolitus peab olema ELi julgeolekukultuuri lahutamatu osa. Liikmesriikide kohtusüsteemid ja õigusala töötajad peavad olema samuti valmis enneolematute probleemidega kohanemiseks ja neile reageerimiseks. Koolitus on oluline, et ametiasutused kasutaksid neid vahendeid operatiivolukorras. Lisaks tuleks teha kõik jõupingutused, et tugevdada soolise aspekti arvestamist ja suurendada naiste osalemist õiguskaitses.

Peamised meetmed
• Europoli volituste laiendamine • ELi politseikoostöö seadustiku arendamine ja politseikoostöö kriisi ajal • Eurojusti tugevdamine kohtu- ja õiguskaitseasutuste sidumiseks • Reisijaid käsitleva eelteabe direktiivi läbivaatamine • Teatis broneeringuinfo välismõõtme kohta • ELi ja Interpoli koostöö tugevdamine • Raamistik läbirääkimiste pidamiseks oluliste kolmandate riikidega teabe jagamise üle • Reisidokumentide paremad turvastandardid • Euroopa sisejulgeoleku innovatsioonikeskuse loomise võimaluse uurimine

[128] Vt www.betterinternetforkids.eu – keskportaali ja riiklikke turvalisema interneti keskusi rahastatakse praegu Euroopa ühendamise rahastu telekommunikatsiooniprogrammist, tehtud on ettepanek jätkata rahastamist tulevikus digitaalse Euroopa programmi raames.

[129] Jätkusuutliku konkurentsivõime, sotsiaalse õigluse ja vastupanuvõime saavutamiseks on loodud Euroopa oskuste tegevuskava (COM (2020) 274 final).

[130] Vt soolise võrdõiguslikkuse strateegia (COM (2020) 152), ohvrite õiguste strateegia (COM (2020) 258) ning lastele parema interneti loomise Euroopa strateegia, (COM (2012) 196).

V. Järeldused

Üha ebastabiilsemas maailmas peetakse Euroopa Liitu endiselt üheks kindlamaks ja turvalisemaks kohaks. Seda ei saa aga võtta iseenesestmõistetavana.

Uus julgeolekuliidu strateegia paneb aluse julgeoleku ökosüsteemile, mis hõlmab kogu Euroopa ühiskonda. See põhineb teadmisel, et julgeolek on jagatud vastutus. Julgeolek on teema, mis mõjutab kõiki. Kõik valitsusasutused, ettevõtted, ühiskondlikud organisatsioonid, institutsioonid ja kodanikud peavad täitma oma kohustusi, et muuta meie ühiskond turvalisemaks.

Julgeolekuküsimusi tuleb nüüd vaadelda palju laiemast perspektiivist kui minevikus. Tuleb üle saada füüsilise ja digitaalse julgeoleku põhjendamatust eristamisest. ELi julgeolekuliidu strateegia koondab kõik julgeolekuvajadused ja keskendub ELi julgeoleku jaoks lähiaastatel kõige olulisematele valdkondadele. Selles tunnistatakse ka, et julgeolekuohud ei hooli geograafilistest piiridest, ning et sise- ja välisjulgeolek on omavahel üha tihedamalt seotud[131]. Sellega seoses on oluline, et EL teeks koostööd rahvusvaheliste partneritega, et kaitsta kõiki ELi kodanikke ja säilitada kõnealuse strateegia rakendamisel tihe koordineeritus ELi välistegevusega.

Meie julgeolek on seotud meie põhiväärtustega. Kõik käesolevas strateegias kavandatud meetmed ja algatused austavad täielikult põhiõigusi ja meie Euroopa väärtusi. Need on meie euroopaliku eluviisi alus ja peavad jääma kogu meie töö keskmesse.

Komisjon on täiesti teadlik sellest, et mis tahes poliitika või meede on ainult nii hea kui selle rakendamine. Seetõttu on vaja pidevalt rõhuda kehtivate ja tulevaste õigusaktide nõuetekohasele rakendamisele ja jõustamisele. Seda jälgitakse korrapäraste julgeolekuliidu aruannete kaudu ning komisjon hoiab Euroopa Parlamenti, nõukogu ja sidusrühmi täielikult kursis ja kaasab nad kõigisse asjakohastesse meetmetesse. Peale selle on komisjon valmis osalema ja korraldama koos institutsioonidega julgeolekuliidu strateegia ühiseid arutelusid, et hinnata tehtud edusamme, käsitledes samal ajal koos eesseisvaid väljakutseid.

Komisjon kutsub Euroopa Parlamenti ja nõukogu üles kinnitama käesolev julgeolekuliidu strateegia, kui julgeolekualase koostöö ja ühismeetmete alus järgmiseks viieks aastaks.

[131] Vt Euroopa Liidu üldine välis- ja julgeolekupoliitika strateegia