EUROPOS
KOMISIJA

Briuselis, 2020 07 24
COM(2020) 605 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, EUROPOS VADOVŲ TARYBAI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI

dėl ES saugumo sąjungos strategijos

I. Įvadas

Komisijos politinėse gairėse aiškiai nurodyta, jog turime padaryti viską, kad apsaugotume savo piliečius. Saugumas ne tik yra asmeninio saugumo pagrindas, bet ir užtikrina pagrindinių teisių apsaugą ir suteikia pagrindą pasitikėjimui ir dinamiškumui mūsų ekonomikoje, visuomenėje ir demokratijoje. Šiandien Europos piliečiai susiduria su nuolat kintančia saugumo padėtimi, kuriai poveikį daro kintančios grėsmės ir kiti veiksniai, įskaitant klimato kaitą, demografines tendencijas ir politinį nestabilumą už ES ribų. Globalizacija, laisvas judėjimas ir skaitmeninė transformacija toliau užtikrina gerovę, palengvina mūsų gyvenimą ir skatina inovacijas bei ekonomikos augimą. Tačiau šie privalumai yra taip pat neišvengiamai susiję su rizika ir išlaidomis. Jais gali būti manipuliuojama terorizmo, organizuoto nusikalstamumo, prekybos narkotikais ir prekybos žmonėmis tikslais, – visa tai kelia tiesioginę grėsmę piliečiams ir mūsų europinei gyvensenai. Kibernetinių išpuolių ir kibernetinių nusikaltimų skaičius toliau didėja. Be to, grėsmės saugumui tampa vis sudėtingesnės: palankias sąlygas joms atsirasti sudaro galimybė veikti tarpvalstybiniu mastu ir tarpusavio sujungiamumas; jos kyla, kai ribos tarp fizinio ir skaitmeninio pasaulio tampa neaiškios; joms atsirasti yra palankus tam tikrų grupių pažeidžiamumas ir socialiniai bei ekonominiai skirtumai. Išpuoliai gali įvykti per akimirką, o jų pėdsakų gali likti nedaug arba nelikti visai. Įvairias hibridines grėsmes gali sukelti tiek valstybiniai, tiek nevalstybiniai subjektai[1]. Be to, tai, kas vyksta už ES ribų, gali turėti lemiamos įtakos saugumui ES viduje.

COVID-19 krizė taip pat lėmė grėsmių saugai ir saugumui sampratos ir atitinkamos politikos pokyčius. Ji aiškiai parodė, kad reikia užtikrinti saugumą tiek fizinėje, tiek skaitmeninėje aplinkoje. Ji parodė atviro strateginio savarankiškumo svarbą mūsų tiekimo grandinėms, susijusioms su ypatingos svarbos produktais, paslaugomis, infrastruktūra ir technologijomis. Dėl krizės sustiprėjo poreikis kiekvieną sektorių ir kiekvieną asmenį įtraukti į bendras pastangas užtikrinti, kad ES visų pirma būtų geriau pasirengusi ir atsparesnė ir prireikus turėtų geresnių reagavimo priemonių.

Piliečiai negali būti apsaugoti, jeigu valstybės narės veiks tik pavieniui. Dar niekada nebuvo taip svarbu išnaudoti savo stiprybes bendradarbiavimo labui, o ES dar niekada nebuvo pajėgesnė padaryti pokyčių nei dabar. ES gali rodyti pavyzdį stiprindama savo bendrą krizių valdymo sistemą ir tiek viduje, tiek už savo ribų padėti siekti pasaulinio stabilumo. Nors pagrindinė atsakomybė už saugumą tenka valstybėms narėms, pastaraisiais metais padidėjo suvokimas, kad vienos valstybės narės saugumas yra visų saugumas. ES gali imtis daugiadalykių ir integruotų atsakomųjų veiksmų ir padėti valstybių narių saugumo subjektams suteikdama jiems reikiamų priemonių ir informacijos[2].

Siekdama politikos kryptims suteikti tinkamą pasitikėjimo pagrindą, ES taip pat gali užtikrinti, kad saugumo politika ir toliau būtų grindžiama mūsų bendromis Europos vertybėmis – pagarba teisinei valstybei, lygybei[3] ir pagrindinėms teisėms ir jų puoselėjimu, skaidrumo, atskaitomybės ir demokratinės kontrolės užtikrinimu. Ji gali sukurti veiksmingą

[1] Hibridinių grėsmių apibrėžtys gali būti įvairios, tačiau šia sąvoka siekiama apibūdinti prievartinės ir ardomosios veiklos, įprastų ir neįprastų (t. y. diplomatinių, karinių, ekonominių, technologinių) metodų derinį, kuriuo valstybiniai arba nevalstybiniai subjektai gali koordinuotai siekti konkrečių tikslų, oficialiai nepaskelbdami karo. Žr. JOIN(2016) 18 *final*.

[2] Pavyzdžiui, naudojantis paslaugomis, kurias teikia tokios ES kosmoso programos, kaip „Copernicus“, sudaranti sąlygas gauti Žemės stebėjimo duomenis ir suteikianti galimybę juos pritaikyti sienų stebėjimo, jūrų saugumo, teisėsaugos, kovos su piratavimu, atgrasymo nuo narkotikų kontrabandos ir ekstremaliųjų situacijų valdymo srityse.

[3] „Lygybės Sąjunga. 2020–2025 m. lyčių lygybės strategija“ (COM(2020) 152).

ir tikrą saugumo sąjungą, kurioje būtų tinkamai saugomos asmenų teisės ir laisvės. Saugumas ir pagarba pagrindinėms teisėms yra ne vienas kitam prieštaraujantys, o nuoseklūs ir vienas kitą papildantys tikslai. Saugumo politika turi būti grindžiama mūsų vertybėmis ir pagrindinėmis teisėmis, ja turi būti užtikrinamas būtinumo, proporcingumo ir teisėtumo principų laikymasis ir joje turi būti numatytos tinkamos atskaitomybės ir teisių gynimo priemonių garantijos, kartu sudarant sąlygas veiksmingai reaguoti asmenų, visų pirma pažeidžiamiausių asmenų, apsaugos tikslais.

Reikšmingos teisinės, praktinės ir paramos priemonės jau įdiegtos, tačiau jas reikia ne tik stiprinti, bet ir geriau įgyvendinti. Padaryta didelė pažanga gerinant keitimąsi informacija ir bendradarbiavimą su valstybėmis narėmis žvalgybos srityje, taip pat iš teroristų ir nusikaltėlių atimant galimybę veikti. Vis dėlto susiskaidymas išlieka.

Darbas turi vykti ir už ES ribų. Sąjungos ir jos piliečių apsauga reiškia ne tik tai, kad saugumas turi būti užtikrinamas ES viduje, bet ir tai, kad reikia imtis su saugumo išorės aspektu susijusių veiksmų. ES požiūris į išorės saugumą pagal bendrą užsienio ir saugumo politiką (BUSP) ir bendrą saugumo ir gynybos politiką (BSGP) ir toliau liks esminis ES pastangų didinti saugumą ES elementas. Bendradarbiavimas tiek su trečiosiomis šalimis, tiek pasauliniu lygmeniu siekiant spręsti bendras problemas yra svarbus siekiant veiksmingo ir visapusiško atsako, o stabilumas ir saugumas ES kaimynystėje yra itin svarbūs pačios ES saugumui.

Ši nauja strategija remiasi anksčiau Europos Parlamento[4], Tarybos[5] ir Komisijos[6] atlikto darbo rezultatais, ir iš jos matyti, kad tikrai ir veiksmingai saugumo sąjungai sukurti reikalingas tvirtas esminių priemonių ir politikos derinys, kuris padėtų praktiškai užtikrinti saugumą, kartu pripažįstant, kad saugumas daro poveikį visoms visuomenės dalims ir visoms viešosios politikos kryptims. ES turi užtikrinti saugią aplinką visiems, neatsižvelgiant į jų rasinę ar etninę kilmę, religiją, tikėjimą, lytį, amžių ar seksualinę orientaciją.

Šioje strategijoje aptariamas laikotarpis nuo 2020 iki 2025 m. ir daugiausia dėmesio skiriama pajėgumų ir gebėjimų užtikrinti ateities iššūkiams atsparią saugumo aplinką stiprinimui. Joje pateikiamas visą visuomenę apimantis požiūris į saugumą, kurio laikantis galima veiksmingai ir koordinuotai reaguoti į sparčiai kintančią grėsmių padėtį. Strategijoje apibrėžiami strateginiai prioritetai ir atitinkami veiksmai, kuriais visoje saugumo sąjungos ekosistemoje integruotai šalinama skaitmeninė ir fizinė rizika, daugiausia dėmesio skiriant sritims, kuriose ES gali suteikti papildomos naudos. Jos tikslas – suteikti saugumo garantijų, kad Europos Sąjungoje būtų apsaugoti visi.

II. Sparčiai kintanti grėsmių Europos saugumui padėtis

Piliečių saugumas, klestėjimas ir gerovė priklauso nuo jų saugumo. Tam saugumui kylančios grėsmės priklauso nuo piliečių gyvybės ir pragyvenimo šaltinių pažeidžiamumo

[4] Pavyzdžiui, Europos Parlamento Specialiojo komiteto terorizmo klausimais (TERR), kuris 2018 m. lapkričio mėn. pateikė ataskaitą, darbo rezultatai.

[5] Pradedant 2015 m. birželio mėn. Tarybos išvadomis dėl atnaujintos vidaus saugumo strategijos ir baigiant naujesnėmis 2019 m. gruodžio mėn. Tarybos posėdžių išvadomis.

[6] „Europos saugumo darbotvarkės įgyvendinimas siekiant kovoti su terorizmu ir sukurti tikrą veiksmingą saugumo sąjungą“ (COM(2016) 230 *final*, 2016 04 20). Žr. naujausią vidaus saugumo srities teisės aktų įgyvendinimo vertinimą: Vidaus reikalų teisės aktų įgyvendinimas vidaus saugumo srityje 2017–2020 m. (SWD(2020) 135).

masto. Kuo didesnis pažeidžiamumas, tuo didesnė rizika, kad juo bus galima pasinaudoti. Tiek pažeidžiamumas, tiek grėsmės nuolat kinta, todėl ES turi prisitaikyti.

Mūsų kasdienis gyvenimas priklauso nuo įvairių paslaugų: energetikos, transporto, finansų ir sveikatos. Jos priklauso ir nuo fizinės, ir nuo skaitmeninės infrastruktūros, todėl didėja pažeidžiamumas ir trikdžių tikimybė. Per COVID-19 pandemiją naujos technologijos daugeliui įmonių ir viešojo sektoriaus įstaigų padėjo tęsti veiklą: nesvarbu, ar užtikrindamos ryšį dirbant nuotolinį darbą, ar palaikydamos tiekimo grandinių logistiką. Tačiau dėl to taip pat gerokai padaugėjo piktavališkų išpuolių, bandymų pasinaudoti pandemijos sukeltais trikdžiais ir atvejų, kai prie nuotolinio darbo pasitelkiant skaitmenines priemones pereita nusikalstamais tikslais[7]. Dėl prekių trūkumo atsirado naujų galimybių organizuotam nusikalstamumui. Tuo metu, kai spaudimas buvo didžiausias, pasekmės galėjo būti mirtinos, o esminių sveikatos priežiūros paslaugų teikimas galėjo sutrikti.

Kadangi skaitmeninės technologijos mūsų gyvenimui teikia vis daugiau privalumų, strategiškai svarbiu klausimu taip pat tapo technologijų **kibernetinis saugumas**[8]. Kibernetiniai išpuoliai daro didelį poveikį namų ūkiams, bankams, finansinėms paslaugoms ir įmonėms (visų pirma mažosioms ir vidutinėms įmonėms). Galimą žalą dar labiau didina fizinių ir skaitmeninių sistemų tarpusavio priklausomybė: bet koks fizinis poveikis neabejotinai turės įtakos skaitmeninėms sistemoms, o dėl kibernetinių išpuolių prieš informacines sistemas ir skaitmeninę infrastruktūrą gali sustoti esminių paslaugų teikimas[9]. Daiktų interneto populiarėjimas ir išaugęs dirbtinio intelekto naudojimas atneš naujų privalumų, bet taip pat sukels naujų pavojų.

Mūsų pasaulis priklauso nuo skaitmeninės infrastruktūros, technologijų ir internetinių sistemų, kurios leidžia mums kurti verslą, vartoti produktus ir naudotis paslaugomis. Viskas priklauso nuo ryšių ir sąveikos. Priklausomybė nuo interneto sudarė sąlygas kilti **kibernetinių nusikaltimų** bangai[10]. Kibernetiniai nusikaltimai kaip paslauga ir šešėlinė kibernetinių nusikaltimų ekonomika suteikia nesudėtingą prieigą prie elektroninių nusikaltimų produktų ir paslaugų internete. Nusikaltėliai greitai prisitaiko ir naujas technologijas naudoja savo pačių reikmėms. Pavyzdžiui, į teisėtą vaistų tiekimo grandinę infiltruoti padirbti ir falsifikuoti vaistai[11]. Eksponentinis internete esančios vaikų seksualinio išnaudojimo medžiagos kiekio didėjimas[12] parodė besikeičiančių nusikalstamumo modelių socialines pasekmes. Neseniai atliktas tyrimas parodė, kad dauguma (55 %) ES gyventojų yra susirūpinę dėl to, kad prieigą prie jų duomenų gali turėti nusikaltėliai ir sukčiautojai[13].

---

7 Europol, *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (April 2020).

8 Komisijos rekomendacija „5G tinklų kibernetinis saugumas“ (C(2019) 2335); komunikatas „Saugaus 5G ryšio diegimas ES. ES priemonių rinkinio įgyvendinimas“ (COM(2020) 50).

9 2020 m. kovo mėn. Čekijoje Brno universitetinė ligoninė patyrė kibernetinį išpuolį, dėl kurio ji buvo priversta nukreipti pacientus į kitas įstaigas ir atidėti operacijas (Europol, *Pandemic Profiteering. How criminals exploit the COVID-19 crisis*). Dirbtiniu intelektu gali būti piktnaudžiaujama siekiant vykdyti skaitmeninius, politinius ir fizinius išpuolius, taip pat sekimą. Daiktų interneto prietaisų (išmaniųjų laikrodžių, virtualiųjų asistentų ir pan.) renkami duomenys gali būti naudojami asmenims stebėti.

10 Remiantis kai kuriomis prognozėmis, duomenų saugumo pažeidimų žala iki 2024 m. kasmet sieks 5 trln. JAV dolerių (USD) ir išaugs, palyginti su 3 trln. USD 2015 metais (Juniper Research, *The Future of Cybercrime & Security*).

11 2016 m. atlikto tyrimo (*Legiscript*) skaičiavimais, pasaulyje tik 4 % internetinių vaistinių veikia teisėtai, o 30 000–35 000 internete veikiančių neteisėtų internetinių vaistinių pagrindinis taikinys – ES vartotojai.

12 ES veiksmingesnės kovos su vaikų seksualiniu išnaudojimu strategija (COM(2020) 607).

13 European Union Agency for Fundamental Rights (2020), *Your rights matter: Security concerns and experiences, Fundamental Rights Survey*, Luxembourg, Publications Office.

Šios grėsmės tampa opesnės ir dėl **pasaulinės aplinkos**. Agresyvi trečiųjų šalių pramonės politika kartu su nuolatinėmis intelektinės nuosavybės vagystėmis pasinaudojant kibernetine erdve keičia Europos interesų apsaugos ir plėtojimo strateginę paradigmą. Prie to prisideda dvejopo naudojimo prietaikų populiarėjimas, todėl stiprus civilinių technologijų sektorius tampa stipriu gynybos ir saugumo pajėgumų pranašumu. Didelį poveikį ES ekonomikai, darbo vietų kūrimui ir ekonomikos augimui daro pramoninis šnipinėjimas: apskaičiuota, kad kibernetinės komercinių paslapčių vagystės ES kainuoja 60 mlrd. EUR[14]. Todėl reikia nuodugniai apsvarstyti, kaip priklausomybė ir padidėjusi kibernetinių grėsmių rizika veikia ES gebėjimą apsaugoti tiek asmenis, tiek įmones.

COVID-19 krizė taip pat parodė, kaip dėl socialinio susiskaldymo ir netikrumo saugumas tampa pažeidžiamas. Tai didina galimybes valstybiniams ir nevalstybiniams subjektams vykdyti sudėtingesnius ir **hibridinius išpuolius**, o pažeidžiamumu pasinaudojama derinant įvairius kibernetinius išpuolius, darant žalą ypatingos svarbos infrastruktūrai[15], vykdant dezinformacijos kampanijas ir radikalizuojant politinį naratyvą[16].

Tuo pačiu metu toliau vystosi anksčiau atsiradusios grėsmės. 2019 m. ES buvo pastebima **teroristinių išpuolių** mažėjimo tendencija. Tačiau grupuočių „Da'esh“ ir „Al-Qaeda“ vykdomų arba jų įkvėptų džihadistų išpuolių grėsmė ES piliečiams išlieka didelė[17]. Kartu didėja smurtinio dešiniojo ekstremizmo grėsmė[18]. Didelį susirūpinimą turėtų kelti rasizmo įkvėpti išpuoliai: Halės mieste surengti mirtini antisemitiniai teroristiniai išpuoliai priminė, kad reikia aktyviau reaguoti pagal 2018 m. Tarybos deklaraciją[19]. ES kas penktas asmuo nerimauja dėl to, kad per ateinančius 12 mėnesių gali būti įvykdytas teroristinis išpuolis[20]. Didžioji dauguma neseniai įvykdytų teroristinių išpuolių buvo „žemųjų technologijų“ išpuoliai, pavienių veikėjų surengti prieš asmenis viešosiose erdvėse, bet teroristinė propaganda internete įgijo naują reikšmę, kai buvo tiesiogiai transliuojami Kraistčerčo mieste įvykdyti išpuoliai[21]. Radikalių pažiūrų asmenų keliama grėsmė tebėra didelė – ją gali sustiprinti grįžtantys užsienio teroristai kovotojai ir iš įkalinimo vietų paleisti ekstremistai[22].

Krizė taip pat parodė, kaip naujomis aplinkybėmis esamos grėsmės gali kisti. **Organizuotos nusikalstamos** grupės pasinaudojo prekių trūkumu – palankiomis sąlygomis kurti naujas neteisėtas rinkas. Prekyba neteisėtais narkotikais išlieka didžiausia nusikalstama rinka ES,

---

[14] *The scale and impact of industrial espionage and theft of trade secrets through cyber*, 2018.

[15] Ypatingos svarbos infrastruktūros objektai yra ypač svarbūs esminėms visuomeninėms funkcijoms, sveikatai, saugai, saugumui, ekonominei ar socialinei gerovei, kurių veikimo sutrikdymas ir (arba) sunaikinimas turi didelį poveikį (Tarybos direktyva 2008/114/EB).

[16] 97 % ES piliečių yra susidūrę su melagingomis naujienomis, 38 % – kasdien. Žr. JOIN(2020) 8 *final*.

[17] 13 ES valstybių narių pranešė apie iš viso 119 užbaigtų, nepavykusių ir sužlugdytų teroristinių išpuolių, per kuriuos žuvo dešimt, o sužeisti 27 asmenys (Europol, *European Union Terrorism Situation and Trend Report*, 2020).

[18] 2019 m. surengti šeši dešiniojo sparno teroristiniai išpuoliai (trijose valstybėse narėse – vienas įvykdytas, vienas nepavykęs, keturi sužlugdyti), palyginti su tik vienu išpuoliu 2018 m., o kiti mirties atvejai nebuvo priskirti prie terorizmo (Europol, 2020).

[19] Taip pat žr. Tarybos deklaraciją dėl kovos su antisemitizmu ir bendro saugumo požiūrio siekiant geriau apsaugoti žydų bendruomenes ir institucijas Europoje plėtojimo.

[20] European Union Agency for Fundamental Rights, *Your rights matter: Security concerns and experiences*, 2020.

[21] Nuo 2015 m. liepos mėn. iki 2019 m. pabaigos Europolas aptiko teroristinį turinį 361 platformoje (Europol, 2020).

[22] Europol, *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism*, 2019.

kurios minimali mažmeninės prekybos vertė ES siekia 30 mlrd. EUR per metus[23]. Prekyba žmonėmis tęsiasi: apskaičiuota, kad iš visų formų išnaudojimo gaunamas bendras metinis pelnas siekia beveik 30 mlrd. EUR[24]. Iš tarptautinės prekybos suklastotais vaistais gaunamas pelnas pasiekė 38,9 mlrd. EUR[25]. Be to, atsižvelgiant į tai, kad konfiskavimo atvejų yra nedaug, nusikaltėliai gali toliau plėsti nusikalstamą veiklą ir skverbtis į teisėtą ekonomiką[26]. Nusikaltėliams ir teroristams yra lengviau gauti šaunamųjų ginklų iš interneto rinkos ir naudojantis naujomis technologijomis, pavyzdžiui, 3-D spausdinimu[27]. Dirbtinio intelekto, naujų technologijų ir robotikos priemonių naudojimas dar labiau padidins riziką, kad inovacijų teikiamais privalumais nusikaltėliai naudosis piktavališkais tikslais[28].

Šios grėsmės yra susijusios su skirtingomis kategorijomis ir įvairioms visuomenės grupėms daro nevienodą poveikį. Visa tai kelia didelę grėsmę asmenims ir įmonėms, todėl ES lygmeniu reikia imtis visapusiškų ir nuoseklių atsakomųjų veiksmų. Kadangi saugumo pažeidžiamumą gali sukelti net nedideli tarpusavyje susiję namų ūkio prietaisai, pavyzdžiui, prie interneto prijungtas šaldytuvas arba kavos aparatas, savo saugumui užtikrinti nebegalime pasikliauti vien tradiciniais valstybiniais subjektais. Ekonominės veiklos vykdytojai turi prisiimti didesnę atsakomybę už produktų ir paslaugų, kuriuos jie pateikia rinkai, kibernetinį saugumą. Tačiau asmenys taip pat turi turėti bent elementarių žinių apie kibernetinį saugumą, kad galėtų apsisaugoti.

III. ES koordinuotas atsakas visos visuomenės labui

ES jau parodė, kaip ji gali suteikti realios pridėtinės vertės. Nuo 2015 m. saugumo sąjunga padėjo susieti saugumo politikos įgyvendinimo ES lygmeniu būdus. Vis dėlto reikia dėti daugiau pastangų siekiant įtraukti visą visuomenę, įskaitant visų lygmenų valstybinės valdžios institucijas, visų sektorių įmones ir asmenis visose valstybėse narėse. Didėjantis informuotumas apie priklausomybės riziką[29] ir tvirtos Europos pramonės strategijos[30] poreikis rodo, kad ES būtinas atsparumas pramonės, technologijų gamybos ir tiekimo grandinės srityse. Tvirtumas taip pat reiškia visapusišką pagarbą pagrindinėms teisėms ir ES vertybėms – jos yra teisėtos, veiksmingos ir tvarios saugumo politikos prielaida. Šioje saugumo sąjungos strategijoje nustatomos konkrečios tolesnės veiklos kryptys. Ji grindžiama šiais bendrais tikslais:

- ***Stiprinti ankstyvo krizių nustatymo, prevencijos ir greito reagavimo į jas pajėgumus ir gebėjimus.*** Europa turi būti atsparesnė, kad galėtų užkirsti kelią būsimiems sukrėtimams, užtikrintų apsaugą nuo jų ir būtų jiems atspari. Turime stiprinti ankstyvo

[23] Europos narkotikų ir narkomanijos stebėsenos centro (EMCDDA) ir Europolo 2019 m. ataskaita apie ES narkotikų rinką.

[24] Europol, *Report on Trafficking in Human Beings, Financial Business Model* (2015).

[25] ES intelektinės nuosavybės tarnybos ir EBPO ataskaita apie prekybą suklastotais vaistais.

[26] Ataskaita „Turto susigrąžinimas ir konfiskavimas: užtikrinti, kad nusikaltimai neapsimokėtų“ (COM(2020) 217.

[27] 2017 metais šaunamieji ginklai buvo panaudoti 41 % visų teroristinių išpuolių (Europol, 2018).

[28] 2020 m. liepos mėn. Prancūzijos ir Nyderlandų teisėsaugos ir teisminės institucijos kartu su Europolu ir Eurojustu pristatė bendrą tyrimą, kurio tikslas – išardyti užšifruotą telefonų tinklą „EncroChat“, kuriuo naudojasi nusikaltėlių tinklai, susiję su smurtiniais išpuoliais, korupcija, pasikėsinimo nužudyti ir didelio masto narkotikų gabenimo atvejais.

[29] Priklausomybės nuo užsienio šalių rizika yra susijusi su didesne galimų grėsmių rizika – nuo IT infrastruktūrų pažeidžiamumo, kuris kelia pavojų ypatingos svarbos infrastruktūros objektams (pavyzdžiui, energetikos, transporto, bankininkystės, sveikatos priežiūros), ar pramoninių valdymo sistemų perėmimo iki išaugusių duomenų vagysčių ar šnipinėjimo pajėgumų.

[30] Komisijos komunikatas „Nauja Europos pramonės strategija“ (COM(2020) 102).

saugumo krizių nustatymo ir greito reagavimo į jas pajėgumus ir gebėjimus, laikydamiesi integruoto ir koordinuoto požiūrio, įgyvendindami tiek pasaulinio masto, tiek konkretiems sektoriams (pavyzdžiui, finansų, energetikos, teismų, teisėsaugos, sveikatos priežiūros, jūrų ir transporto sektoriams) skirtas iniciatyvas ir remdamiesi esamomis iniciatyvomis[31]. Komisija taip pat pateiks pasiūlymų dėl ES plataus masto krizių valdymo sistemos, kuri taip pat turėtų būtų svarbi saugumui.

- ***Skirti dėmesį rezultatams.*** Tam, kad mūsų pastangos būtų kuo veiksmingesnės, rezultatais grindžiama strategija turi būti paremta nuodugniu grėsmės ir rizikos vertinimu. Jai įgyvendinti turi būti nustatytos ir taikomos tinkamos taisyklės ir priemonės. Jai reikia patikimos strateginės žvalgybos informacijos, kuri būtų ES saugumo politikos pagrindas. Tais atvejais, kai reikia priimti ES teisės aktus, turi būti imamasi tolesnių su jais susijusių veiksmų, kad jie būtų visapusiškai įgyvendinti, būtų išvengta susiskaidymo ir neliktų spragų, kuriomis galima pasinaudoti. Šios strategijos įgyvendinimo veiksmingumas priklausys ir nuo to, ar kitu 2021–2027 m. programavimo laikotarpiu bus užtikrintas tinkamas finansavimas, įskaitant susijusioms ES agentūroms teikiamą finansavimą.
- ***Suburti visus viešojo ir privačiojo sektorių dalyvius siekti bendro tikslo.*** Pagrindiniai viešojo ir privačiojo sektorių subjektai nenoriai dalijasi su saugumu susijusia informacija, nes baiminasi pakenkti nacionaliniam saugumui arba konkurencingumui[32].Tačiau esame veiksmingiausi tada, kai visas priemones pasitelkiame tarpusavio paramai. Visų pirma tai reiškia intensyvesnį valstybių narių bendradarbiavimą, apimantį teisėsaugos institucijas, teismines ir kitas valdžios institucijas, taip pat bendradarbiavimą su ES institucijomis ir agentūromis siekiant sukurti pasitikėjimu grindžiamą atmosferą ir užtikrinti keitimąsi informacija, kurių reikia bendriems sprendimams. Ne mažiau svarbus yra bendradarbiavimas su privačiuoju sektoriumi, juo labiau kad pramonės sektoriui priklauso didelė skaitmeninės ir neskaitmeninės infrastruktūros dalis, kuri turi itin didelę reikšmę veiksmingai kovai su nusikalstamumu ir terorizmu. Patys asmenys taip pat gali prisidėti, pavyzdžiui, ugdydami kovai su elektroniniais nusikaltimais ar dezinformacija reikalingus įgūdžius ir didindami informuotumą. Galiausiai šių bendrų veiksmų turi būti imamasi ir už ES ribų, užmezgant glaudesnius ryšius su bendraminčiais partneriais.

IV. Visų apsauga ES: strateginiai saugumo sąjungos prioritetai

ES turi unikalią galimybę reaguoti į šias naujas pasaulines grėsmes ir problemas. Pirmiau pateiktoje grėsmių analizėje nurodyti keturi tarpusavyje susiję strateginiai prioritetai, kuriuos reikia įgyvendinti ES lygmeniu, visapusiškai paisant pagrindinių teisių: i) ateities iššūkiams atspari saugumo aplinka, ii) kova su kintančiomis grėsmėmis, iii) Europos piliečių apsauga nuo terorizmo ir organizuoto nusikalstamumo, iv) stipri Europos saugumo ekosistema.

[31] Pavyzdžiui, integruotą politinio atsako į krizes mechanizmą (IPCR), Reagavimo į nelaimes koordinavimo centro iniciatyvą, Komisijos rekomendaciją dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (C(2017) 6100), ES operatyvinių veiksmų protokolą dėl kovos su hibridinėmis grėsmėmis (ES scenarijus) (SWD(2016) 227).

[32] Bendras komunikatas „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ (JOIN(2017) 450).

1. Ateities iššūkiams atspari saugumo aplinka

Ypatingos svarbos infrastruktūros objektų apsauga ir atsparumas

Kasdieniame gyvenime asmenys pagrindiniais infrastruktūros objektais naudojasi keliaudami, dirbdami, naudodamiesi pagrindinėmis viešosiomis paslaugomis, pavyzdžiui, ligoninių, transporto, energijos tiekimo paslaugomis, arba įgyvendindami savo demokratines teises. Jei ši infrastruktūra nėra pakankamai apsaugota ir atspari, išpuoliai gali sukelti didžiulius – fizinius ar skaitmeninius – sutrikimus tiek atskirose valstybėse narėse, tiek potencialiai visoje ES.

Dabartinė ES ypatingos svarbos infrastruktūros objektų apsaugos ir atsparumo sistema[33] atsilieka nuo kintančios rizikos. Didėjanti tarpusavio priklausomybė reiškia, kad sutrikimai viename sektoriuje gali turėti tiesioginį poveikį operacijoms kituose sektoriuose: išpuolis elektros energijos gamybos sektoriuje galėtų sutrikdyti telekomunikacijų, ligoninių, bankų ar oro uostų veiklą, o išpuolis prieš skaitmeninę infrastruktūrą galėtų sukelti elektros energijos arba finansų tinklų sutrikimus. Kadangi mūsų ekonomika ir visuomenė vis labiau persikelia į internetą, tokie pavojai tampa dar aktualesni. Ši glaudesnių tarpusavio sąsajų ir priklausomybės problema turi būti sprendžiama teisės aktų priemonėmis, taikant griežtas ypatingos svarbos infrastruktūros kibernetinės bei fizinės apsaugos ir atsparumo stiprinimo priemones. Turi būti užtikrinama tinkama esminių paslaugų, įskaitant kosmoso infrastruktūra grindžiamas paslaugas, apsauga nuo dabartinių ir numatomų grėsmių, tačiau tos paslaugos taip pat turi būti atsparios. Tai reiškia, kad sistema turi būti pajėgi pasirengti nepageidaujamiems reiškiniams ir juos planuoti, absorbuoti, atsigauti nuo jų ir sėkmingiau prie jų prisitaikyti.

Tuo pačiu metu valstybės narės pasinaudojo diskrecija ir skirtingai įgyvendino galiojančius teisės aktus. Dėl atsirandančio susiskaidymo gali kilti pavojus vidaus rinkai ir pasunkėti tarpvalstybinis koordinavimas, visų pirma pasienio regionuose. Esmines paslaugas skirtingose valstybėse narėse teikiantiems veiklos vykdytojams taikoma skirtinga ataskaitų teikimo tvarka. Komisija nagrinėja, ar **naujos fizinės ir skaitmeninės infrastruktūros sistemos** galėtų užtikrinti didesnį nuoseklumą ir nuoseklesnį požiūrį į patikimo pagrindinių paslaugų teikimo užtikrinimą. Ši sistema turi būti papildyta **konkretiems sektoriams skirtomis iniciatyvomis**, kuriomis siekiama spręsti ypatingos svarbos, pavyzdžiui, transporto, kosmoso, energetikos, finansų ir sveikatos, infrastruktūros objektams kylančias specifinės rizikos problemas[34]. Atsižvelgiant į stiprią finansų sektoriaus priklausomybę nuo IT paslaugų ir didelį jo pažeidžiamumą kibernetinių išpuolių atveju, pirmasis žingsnis bus iniciatyva dėl finansų sektorių skaitmeninės veiklos atsparumo. Atsižvelgiant į ypatingą energetikos sistemos jautrumą ir poveikį, įgyvendinant specialią iniciatyvą bus teikiama parama didesniam ypatingos svarbos energetikos infrastruktūros objektų atsparumui fizinėms, kibernetinėms ir hibridinėms grėsmėms, energetikos operatoriams tarpvalstybiniu mastu užtikrinant vienodas sąlygas.

---

[33] Direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1); Tarybos direktyva 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo.

[34] Atsižvelgiant į tai, kad sveikatos sektorius patiria įtampą, ypač per COVID-19 krizę, Komisija taip pat apsvarstys iniciatyvas, kuriomis siekiama stiprinti ES sveikatos saugumo sistemą bei atsakingas ES agentūras, kad būtų galima reaguoti į dideles tarpvalstybines grėsmes sveikatai.

ES valstybės narės ir Komisija pagal naująją Europos tiesioginių užsienio investicijų tikrinimo sistemą[35] taip pat vertins su saugumu susijusį tiesioginių užsienio investicijų poveikį, kuris gali turėti įtakos ypatingos svarbos infrastruktūros objektams arba ypatingos svarbos technologijoms.

ES taip pat gali sukurti naujų ypatingos svarbos infrastruktūros objektų atsparumo paramos priemonių. Iki šiol pasaulinio interneto atsparumo lygis buvo didelis, visų pirma kiek tai susiję su gebėjimu palaikyti padidėjusį duomenų srautą. Vis dėlto turime būti pasirengę galimoms krizėms ateityje, keliančioms grėsmę interneto saugumui, stabilumui ir atsparumui. Siekiant užtikrinti, kad internetas tinkamai veiktų, reikia vykdyti griežtą kovos su kibernetiniais incidentais ir piktavališka veikla internete politiką ir riboti priklausomybę nuo infrastruktūros ir paslaugų, esančių už Europos ribų. Tam reikės priimti įvairių teisės aktų ir atlikti galiojančių taisyklių peržiūrą, kuria siekiama užtikrinti aukštą bendrą ES tinklų ir informacinių sistemų saugumo lygį; didinti investicijas į mokslinius tyrimus ir inovacijas; apsvarstyti pagrindinių interneto infrastruktūros objektų ir išteklių, visų pirma domenų vardų sistemos, diegimo arba stiprinimo klausimą[36].

Siekiant apsaugoti pagrindinius ES ir nacionalinius skaitmeninius išteklius, ypač svarbu ypatingos svarbos infrastruktūros objektams suteikti saugaus ryšio kanalą. Komisija bendradarbiauja su valstybėmis narėmis, kad sukurtų sertifikuotą saugią ištisinio ryšio kvantinę antžeminę ir kosminę infrastruktūrą kartu su saugia vyriausybinio palydovinio ryšio sistema, kaip nustatyta Kosmoso programos reglamente[37].

Kibernetinis saugumas

Kibernetinių išpuolių toliau daugėja[38]. Šie išpuoliai yra sudėtingesni nei bet kada anksčiau, pasireiškia iš įvairių šaltinių tiek ES viduje, tiek už jos ribų ir yra nukreipti į labiausiai pažeidžiamas sritis. Išpuolius neretai vykdo valstybiniai arba valstybės remiami subjektai, ir išpuolių objektas yra pagrindinės skaitmeninės infrastruktūros objektai, pavyzdžiui, pagrindiniai debesijos paslaugų teikėjai[39]. Didele grėsme finansų sistemai taip pat tapo kibernetiniam saugumui kylanti rizika. Tarptautinis valiutos fondas yra apskaičiavęs, kad dėl kibernetinių išpuolių visame pasaulyje per metus patiriami nuostoliai sudaro 9 % bankų grynųjų pajamų, arba apie 100 mlrd. USD[40]. Perėjimas prie prijungtų įrenginių naudotojams teiks didžiulių privalumų. Tačiau dėl to, kad duomenų centruose saugoma ir tvarkoma

---

[35] 2020 m. spalio 11 d. pradėjus visapusiškai taikyti 2019 m. kovo 19 d. Europos Parlamento ir Tarybos reglamentą (ES) 2019/452, kuriuo nustatoma tiesioginių užsienio investicijų į Sąjungą tikrinimo sistema, ES bus sukurtas naujas bendradarbiavimo tiesioginių ES nepriklausančių šalių investicijų, kurios gali daryti poveikį saugumui ar viešajai tvarkai, klausimais mechanizmas. Pagal reglamentą valstybės narės ir Komisija įvertins galimą riziką, susijusią su tokiomis tiesioginėmis užsienio investicijomis, ir atitinkamais atvejais, kai tai aktualu daugiau nei vienai valstybei narei, pasiūlys tinkamas tos rizikos mažinimo priemones.

[36] Domenų vardų sistema yra hierarchinė decentralizuota vardų sistema, skirta kompiuteriams, paslaugoms arba kitiems prie interneto arba privačiojo tinklo prijungtiems ištekliams. Ta sistema domenų vardus paverčia IP adresais, kurie reikalingi kompiuterinėms paslaugoms ir prietaisams rasti ir atpažinti.

[37] Pasiūlymas dėl Reglamento, kuriuo sudaroma Sąjungos kosmoso programa ir įsteigiama Europos Sąjungos kosmoso programos agentūra (COM(2018) 447).

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

[39] Nuolatine grėsme išlieka paskirstytojo paslaugos trikdymo atakos (DDoS atakos) – didieji paslaugos teikėjai turėjo sušvelninti tokias didelio masto DDoS atakas, kaip 2020 m. vasario mėn. surengtas išpuolis, kurio objektas – bendrovės *Amazon* interneto paslaugos.

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

mažiau duomenų, bet jie vis dažniau tvarkomi tinklo paribyje arčiau naudotojo[41], nebebus galima kibernetinio saugumo sukoncentruoti į centrinių punktų apsaugą[42].

2017 metais ES suformulavo požiūrį į kibernetinį saugumą, kurio pagrindas – atsparumo didinimas, greitas reagavimas ir veiksmingas atgrasymas[43]. Dabar ES turi imtis priemonių, kad, siekiant užtikrinti tiek atsparumą, tiek reagavimo pajėgumą, jos kibernetinio saugumo pajėgumai neatsiliktų nuo tikrovės. Tam reikia tikro visą visuomenę apimančio požiūrio, kurio laikantis ES institucijos, agentūros ir įstaigos, valstybės narės, pramonės subjektai, akademinė bendruomenė ir asmenys kibernetiniam saugumui teiktų reikiamą prioritetą[44]. Šį horizontalųjį požiūrį taip pat reikia papildyti konkretiems sektoriams skirtais požiūriais į kibernetinį saugumą tokiose srityse kaip energetika, finansinės paslaugos, transportas ar sveikata. Kitas ES darbo etapas turėtų būti įtrauktas į peržiūrėtą Europos kibernetinio saugumo strategiją.

Siekiant stiprinti kibernetinį saugumą ir kovoti su terorizmu, ekstremizmu, radikalizmu ir hibridinėmis grėsmėmis, turėtų būti ieškoma naujo ir glaudesnio žvalgybos tarnybų, ES žvalgybos ir situacijų centro (EU INTCEN) ir kitų saugumo srityje veikiančių organizacijų bendradarbiavimo formų.

Atsižvelgiant į tai, kad visoje ES diegiama **5G infrastruktūra**, ir į galimą daugelio ypatingos svarbos paslaugų priklausomybę nuo 5G tinklų, plataus masto sisteminio sutrikimo pasekmės būtų itin rimtos. Įgyvendindamos 2019 m. Komisijos rekomendacijoje „5G tinklų kibernetinis saugumas“[45] nustatytą procesą, šiuo metu valstybės narės ėmėsi konkrečių veiksmų, susijusių su 5G priemonių rinkinyje išdėstytomis pagrindinėmis priemonėmis[46].

Vienas iš svarbiausių ilgalaikių poreikių – sukurti **integruotojo kibernetinio saugumo** kultūrą, kuomet saugumo komponentas į produktus ir paslaugas integruojamas nuo pat pradžių. Prie to reikšmingai prisidės Kibernetinio saugumo akte numatyta nauja kibernetinio saugumo sertifikavimo sistema[47]. Sistema jau pradėta įgyvendinti: jau rengiamos dvi sertifikavimo schemos, o kitų schemų prioritetai bus nustatyti dar šiais metais. Šioje srityje itin didelę reikšmę turi ES kibernetinio saugumo agentūros (ENISA), duomenų apsaugos institucijų ir Europos duomenų apsaugos valdybos[48] bendradarbiavimas.

Komisija jau yra nustačiusi, jog reikalingas **bendras kibernetinio saugumo padalinys**, kuris užtikrintų struktūrizuotą ir koordinuotą operatyvinį bendradarbiavimą. ES lygmens krizės atveju jis galėtų veikti kaip savitarpio pagalbos mechanizmas. Remdamasis plano

---

41 Tinklo paribio kompiuterija – paskirstytoji atvira IT architektūra, kuriai būdinga decentralizuota duomenų apdorojimo galia, sudaranti sąlygas naudotis mobiliosios kompiuterijos ir daiktų interneto (DI) technologijomis. Tinklo paribio kompiuterijos atveju duomenys nėra perduodami duomenų centrui, bet juos tvarko pats įrenginys arba vietinis kompiuteris ar serveris.

42 Komunikatas „Europos duomenų strategija“ (COM(2020) 66 *final*).

43 Bendras komunikatas „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“ (JOIN(2017) 450).

44 Jungtinio tyrimų centro ataskaitoje *Cybersecurity – our digital Anchor* pateikiama su įvairiais aspektais susijusių įžvalgų apie kibernetinio saugumo augimą per pastaruosius 40 metų.

45 Komisijos rekomendacija „5G tinklų kibernetinis saugumas“ (C(2019) 2335 *final*). Rekomendacijoje numatyta, kad ji bus peržiūrėta 2020 metų paskutinį ketvirtį.

46 Žr. 2020 m. liepos 24 d. TIS bendradarbiavimo grupės ataskaitą dėl priemonių rinkinio įgyvendinimo.

47 Reglamentas (EB) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo (Kibernetinio saugumo aktas).

48 Komunikatas „Duomenų apsauga kaip daugiau galių suteikimo piliečiams ir ES požiūrio į perėjimą prie skaitmeninių technologijų pagrindas – dveji metai taikant Bendrąjį duomenų apsaugos reglamentą“ (COM(2020) 264).

rekomendacijos[49] įgyvendinimo rezultatais, bendras kibernetinio saugumo padalinys galėtų stiprinti įvairių Europos kibernetinio saugumo ekosistemos subjektų tarpusavio pasitikėjimą ir teikti valstybėms narėms pagrindinę paslaugą. Komisija pradės diskusijas su atitinkamais suinteresuotaisiais subjektais (pirmiausia su valstybėmis narėmis) ir iki 2020 m. pabaigos nustatys aiškų procesą, etapus ir tvarkaraštį.

Be to, svarbu, kad visoms ES institucijoms, įstaigoms ir agentūroms būtų taikomos bendros informacijos saugumo ir kibernetinio saugumo taisyklės. Turėtų būti siekiama sukurti privalomus aukštus bendrus saugaus keitimosi informacija ir skaitmeninės infrastruktūros bei sistemų saugumo standartus visose ES institucijose, įstaigose ir agentūrose. Šia nauja sistema turėtų būti grindžiamas tvirtas ir veiksmingas ES institucijų, įstaigų ir agentūrų operatyvinis bendradarbiavimas kibernetinio saugumo srityje, daugiausia dėmesio skiriant ES institucijų, įstaigų ir agentūrų kompiuterinių incidentų tyrimo tarnybos (CERT-EU) vaidmeniui.

Atsižvelgiant į pasaulinį tokios veiklos pobūdį, tam, kad būtų galima toliau užkirsti kelią kibernetiniams išpuoliams, atgrasyti nuo jų ir į juos reaguoti, labai svarbu užmegzti ir palaikyti tvirtus **tarptautinius partnerystės** ryšius. Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema (toliau – kibernetinio saugumo diplomatijos priemonių rinkinys)[50] nustato bendros užsienio ir saugumo politikos priemones, įskaitant ribojamąsias priemones (sankcijas), kurios gali būti taikomos kovojant su veikla, kenkiančia ES politiniams, saugumo ir ekonominiams interesams. ES taip pat turėtų intensyvinti veiklą pasitelkdama vystymosi ir bendradarbiavimo fondus, kad būtų stiprinamas gebėjimas teikti paramą valstybėms partnerėms jų skaitmeninių ekosistemų stiprinimui, nacionalinių teisėkūros reformų vykdymui ir tarptautinių standartų laikymuisi. Tai didina visos bendruomenės atsparumą ir gebėjimą veiksmingai kovoti su kibernetinėmis grėsmėmis ir į jas reaguoti. Šie veiksmai apima konkretų darbą, kuriuo siekiama skatinti laikytis ES standartų ir atitinkamų teisės aktų, kad kaimyninių šalių partnerių kibernetinis saugumas taptų didesnis[51].

Viešųjų erdvių apsauga

Neseniai įvykdyti teroristiniai išpuoliai buvo surengti **viešosiose erdvėse**, įskaitant religinių apeigų vietas ir transporto mazgus, pasinaudojant tuo, kad jos yra atviros ir lengvai prieinamos. Dėl terorizmo augimo, kurį skatina politinis ar ideologinis ekstremizmas, ši grėsmė tapo dar didesnė. Todėl reikia stiprinti tokių vietų fizinę apsaugą ir diegti tinkamas nustatymo sistemas, nepažeidžiant piliečių laisvių[52]. Komisija stiprins viešojo ir privačiojo sektorių bendradarbiavimą viešųjų erdvių apsaugos srityje, skirdama finansavimą, keisdamasi patirtimi ir gerąja praktika, teikdama konkrečias gaires[53] ir rekomendacijas[54]. Šie

---

[49] Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.

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

[51] Žr. 2018 m. birželio 26 d. priimtose Tarybos išvadose išdėstytas ES išorės kibernetinių pajėgumų stiprinimo gaires.

[52] Ypatingas dėmesys turi būti skiriamas nuotolinių biometrinio tapatybės nustatymo sistemų tikrinimui. Pirminė Komisijos nuomonė yra išdėstyta 2020 m. vasario 19 d. Komisijos baltojoje knygoje „Dirbtinis intelektas“ (COM(2020) 65).

[53] Pavyzdžiui, Gairės dėl tinkamų apsauginių užtvarų, skirtų viešajai erdvei apsaugoti, sprendimų pasirinkimo (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Gerosios praktikos gairės pateikiamos Komisijos tarnybų dokumente SWD(2019) 140, įskaitant skirsnį dėl viešojo ir privačiojo sektorių bendradarbiavimo. Ypatingas dėmesys viešojo ir privačiojo sektorių bendradarbiavimo stiprinimui skiriamas teikiant finansavimą pagal Vidaus saugumo fondo policijos priemonę.

veiksmai taip pat apims informuotumo didinimą, nustatymo įrangos eksploatacinių reikalavimų taikymą ir jos testavimą, taip pat patikimumo patikrinimų griežtinimą siekiant šalinti vidaus subjektų keliamą grėsmę. Svarbus aspektas, į kurį reikia atsižvelgti, yra tai, kad mažumoms ir pažeidžiamiems asmenims, įskaitant asmenis, prieš kuriuos nukreipti išpuoliai dėl jų religijos ar lyties, gali būti daromas neproporcingas poveikis, todėl jiems reikia skirti ypatingą dėmesį. Svarbus vaidmuo gerinant viešųjų erdvių saugumą tenka regioninėms ir vietos valdžios institucijoms. Komisija taip pat padeda skatinti miestų inovacijas viešųjų erdvių saugumo srityje[55]. 2018 m. lapkričio mėn. užmegzta Naujosios miestų darbotvarkės[56] saugumo viešosiose erdvėse srities partnerystė yra tvirto valstybių narių, Komisijos ir miestų įsipareigojimo tinkamiau spręsti saugumui miestų erdvėse kylančių grėsmių problemą pavyzdys.

Toliau besiplečianti **bepiločių orlaivių** rinka gali būti naudinga įvairiais vertingais ir teisėtais tikslais. Tačiau bepiločiais orlaiviais taip pat gali piktnaudžiauti nusikaltėliai ir teroristai, o viešosioms erdvėms kyla ypatinga grėsmė. Išpuoliai gali būti nukreipti prieš pavienius asmenis, žmonių susibūrimus, ypatingos svarbos infrastruktūros objektus, teisėsaugos institucijas, valstybių sienas ar viešąsias erdves. Žinios apie bepiločių orlaivių naudojimą konflikto atveju galėtų būti teikiamos Europai tiesiogiai (per grįžtančius užsienio teroristus kovotojus) arba internetu. Europos aviacijos saugos agentūros parengtos taisyklės yra svarbus pirmasis žingsnis tokiose srityse, kaip bepiločių orlaivių operatorių registravimas ir privalomas bepiločių orlaivių nuotolinis identifikavimas. Kadangi bepiločiai orlaiviai tampa vis prieinamesni, įperkamesni ir pajėgesni, reikia imtis papildomų veiksmų. Šie veiksmai galėtų apimti keitimąsi informacija, visiems, įskaitant teisėsaugos institucijas, skirtų gairių ir gerosios patirties apžvalgų skelbimą, taip pat bepiločiams orlaiviams taikomų atsakomųjų priemonių testavimo intensyvinimą[57]. Be to, turėtų būti toliau analizuojamas ir sprendžiamas bepiločių orlaivių naudojimo viešosiose erdvėse poveikio privatumui ir duomenų apsaugai klausimas.

Pagrindiniai veiksmai
• Priimti ypatingos svarbos infrastruktūros objektų apsaugos ir atsparumo didinimo srities teisės aktus • Atlikti Tinklų ir informacinių sistemų saugumo (TIS) direktyvos peržiūrą • Priimti iniciatyvą dėl finansų sektoriaus veiklos atsparumo • Užtikrinti ypatingos svarbos energetikos infrastruktūros apsaugą ir kibernetinį saugumą ir priimti tinklo kodeksą dėl tarpvalstybinių elektros energijos srautų kibernetinio saugumo • Įgyvendinti Europos kibernetinio saugumo strategiją • Imtis tolesnių veiksmų siekiant sukurti bendrą kibernetinio saugumo padalinį • ES institucijoms, įstaigoms ir agentūroms taikyti bendras informacijos saugumo ir kibernetinio saugumo taisykles • Stiprinti bendradarbiavimą viešųjų erdvių, įskaitant religinių apeigų vietas, apsaugos

[55] Įgyvendindami iniciatyvą „Inovatyvūs miestų sprendimai“, trys miestai – Pirėjas (Graikija), Tamperė (Suomija) ir Turinas (Italija), išbandys naujus sprendimus, kuriems bendras finansavimas teikiamas iš Europos regioninės plėtros fondo (ERPF).

[56] ES miestų darbotvarkė – tai naujas daugiapakopis darbo metodas, kuriuo skatinamas valstybių narių, miestų, Europos Komisijos ir kitų suinteresuotųjų subjektų bendradarbiavimas siekiant skatinti ekonomikos augimą, gyvenimo sąlygų gerinimą ir inovacijas Europos miestuose ir nustatyti bei sėkmingai spręsti socialines problemas.

[57] Neseniai buvo sukurta daugiametė testavimo programa, skirta padėti valstybėms narėms šioje srityje parengti bendrą metodiką ir testavimo platformą.

srityje
- Keistis geriausia praktika, susijusia su piktnaudžiavimo bepiločiais orlaiviais problemos sprendimu

2. Kova su kintančiomis grėsmėmis

Kibernetiniai nusikaltimai

Technologijos visuomenei atveria naujų galimybių. Jos taip pat suteikia naujų priemonių teismams ir teisėsaugos institucijoms. Tačiau kartu jos suteikia galimybių nusikaltėliams. Daugėja kenkimo programinės įrangos, asmens ar verslo duomenų vagysčių įsilaužimo būdu ir skaitmeninės veiklos sustabdymo atvejų, darančių finansinę žalą arba kenkiančių reputacijai. Pirmoji gynybos priemonė yra atspari aplinka, kurios prielaida yra aukšto lygio kibernetinis saugumas. Teisėsaugos institucijos turi gebėti veikti skaitmeninių tyrimų srityje ir nustatyti aiškias nusikalstamų veikų tyrimo ir baudžiamojo persekiojimo už jas taisykles, taip pat suteikti nukentėjusiesiems būtiną apsaugą. Šis darbas turėtų būti grindžiamas Europolo bendros kovos su kibernetiniais nusikaltimais veiksmų darbo grupės ir Teisėsaugos institucijų reagavimo į ekstremalias situacijas protokolo, kuris sukurtas siekiant koordinuoti atsaką į didelio masto kibernetinius išpuolius, veiklos rezultatais. Taip pat esminę reikšmę turi veiksmingi mechanizmai, kuriais sudaromos sąlygos viešojo ir privačiojo sektorių partnerystei ir bendradarbiavimui.

Be to, kova su kibernetiniais nusikaltimais visoje ES turėtų tapti strateginės komunikacijos prioritetu, kad Europos piliečiai būtų įspėjami apie riziką ir prevencines priemones, kurių jie galėtų imtis. Tai turėtų būti iniciatyvaus požiūrio dalis. Dar vienas esminis žingsnis yra visapusiškas dabartinių teisės aktų įgyvendinimas[58]: Komisija bus pasirengusi atitinkamais atvejais taikyti pažeidimo nagrinėjimo procedūrą ir nuolat peržiūrėti šiuos teisės aktus, siekdama užtikrinti, kad jie ir toliau atitiktų savo paskirtį. Be to, Komisija kartu su Europolu ir ES kibernetinio saugumo agentūra (ENISA) įvertins galimybę sukurti ES ankstyvojo perspėjimo apie kibernetinius nusikaltimus sistemą, kuri galėtų užtikrinti informacijos srautą ir galimybę greitai reaguoti į padidėjusį kibernetinių nusikaltimų skaičių.

Kibernetiniai nusikaltimai yra pasaulinio masto problema, kuriai spręsti būtina veiksmingai bendradarbiauti tarptautiniu mastu. ES remia Europos Tarybos Budapešto konvenciją dėl elektroninių nusikaltimų, kuri yra veiksmingas ir tinkamas pagrindas, leidžiantis visoms šalims nustatyti, kokias sistemas ir ryšių kanalus jos turi įdiegti, kad galėtų veiksmingai bendradarbiauti tarpusavyje.

Beveik pusei[59] ES piliečių didelį nerimą kelia netinkamas duomenų naudojimas ir **tapatybės vagystė**[60]. Apgaulingas naudojimasis tapatybe siekiant finansinės naudos yra vienas aspektas, tačiau jis taip pat gali sukelti rimtų asmeninių ir psichologinių pasekmių, kai kito asmens tapatybe prisidengusio asmens neteisėtai paskelbti įrašai internete gali išlikti ilgą

[58] Direktyva 2013/40/ES dėl atakų prieš informacines sistemas.

[59] 46 % (Eurobarometer, *Europeans' attitudes towards cyber security*, January 2020).

[60] Didžioji dauguma 2018 m. atliktos „Eurobarometro“ apklausos dėl Europos piliečių požiūrį į interneto saugumą respondentų (95 %) tapatybės vagystę įvertino kaip sunkų nusikaltimą, o septyni iš dešimties nurodė, kad tai labai sunkus nusikaltimas. Iš 2020 m. sausio mėn. paskelbtos „Eurobarometro“ apklausos matyti, kad esama susirūpinimo dėl kibernetinių nusikaltimų, sukčiavimo internete ir tapatybės vagysčių: dviem trečdaliams respondentų kelia nerimą sukčiavimas bankininkystės srityje (67 %) arba tapatybės vagystė (66 %).

laiką. Atsižvelgdama į būsimą Europos skaitmeninės tapatybės iniciatyvą[61], Komisija išnagrinės galimas praktines nukentėjusiųjų apsaugos nuo visų formų tapatybės vagysčių priemones.

Kova su kibernetiniais nusikaltimais reiškia, kad reikia planuoti ateitį. Kadangi naujais technologinės plėtros rezultatais naudojamasi tam, kad sustiprėtų ekonomika ir visuomenė, nusikaltėliai taip pat gali ieškoti būdų panaudoti šias priemones neigiamiems tikslams pasiekti. Pavyzdžiui, nusikaltėliai gali naudotis dirbtiniu intelektu, kad nustatytų ir identifikuotų slaptažodžius arba supaprastintų kenkimo programinės įrangos kūrimą, pasinaudotų vaizdo ir garso įrašais, kurie vėliau gali būti naudojami tapatybės vagystei ar sukčiavimui.

Šiuolaikinė teisėsauga

Teisėsaugos ir teisingumo srities specialistai turi prisitaikyti prie naujų technologijų. Dėl technologinės plėtros ir kylančių grėsmių teisėsaugos institucijos turi turėti galimybę naudotis naujomis priemonėmis, įgyti naujų įgūdžių ir kurti alternatyvius tyrimo metodus. Siekdama papildyti teisėkūros veiklą, kuria siekiama gerinti tarpvalstybinę prieigą prie elektroninių įrodymų atliekant nusikalstamų veikų tyrimą, ES gali padėti teisėsaugos institucijoms plėtoti reikiamus gebėjimus nustatyti, apsaugoti ir nuskaityti duomenis, reikalingus nusikalstamoms veikoms tirti, ir juos naudoti kaip įrodymus teisme. Komisija išnagrinės priemones, kuriomis **stiprinami teisėsaugos pajėgumai atliekant skaitmeninius tyrimus**, ir nustatys, kaip kuo geriau pasinaudoti moksliniais tyrimais ir technologine plėtra, kad būtų sukurtos naujos teisėsaugos priemonės; taip pat kaip mokymas gali suteikti tinkamų įgūdžių teisėsaugos ir teisminėms institucijoms. Be kita to, Komisijos Jungtinis tyrimų centras nustatys griežtus mokslinio vertinimo ir testavimo metodus.

Taikant bendrus metodus taip pat galima užtikrinti, kad **dirbtinis intelektas, kosmoso pajėgumai, didieji duomenys** ir **itin našios kompiuterinės sistemos būtų integruoti** į saugumo politiką taip, kad būtų veiksmingai kovojama su nusikalstamumu ir užtikrinamos pagrindinės teisės. Dirbtinis intelektas galėtų būti galinga kovos su nusikalstamumu priemonė, kuri sukurtų milžiniškus tyrimo pajėgumus analizuodama didelius informacijos kiekius ir nustatydama modelius bei anomalijas[62]. Jis taip pat gali suteikti konkrečių priemonių, pavyzdžiui, padėti nustatyti teroristinį turinį internete, išaiškinti įtartinus pavojingų produktų pirkimo–pardavimo sandorius arba ekstremaliosios situacijos atveju teikti pagalbą piliečiams. Išnaudoti šį potencialą galima sutelkiant mokslinius tyrimus, inovacijas ir dirbtinio intelekto naudotojus, kartu užtikrinant tinkamą valdymą ir techninę infrastruktūrą, taip pat aktyviai įtraukiant privatųjį sektorių ir akademinę bendruomenę. Tai taip pat reiškia, kad reikia užtikrinti aukščiausius pagarbos pagrindinėms teisėms standartus ir veiksmingą piliečių apsaugą. Visų pirma, sprendimus, kurie daro poveikį asmenims, turi peržiūrėti žmogus, ir jie turi atitikti atitinkamus taikytinus ES teisės aktus[63].

Apie 85 % sunkių nusikaltimų tyrimų reikia elektroninės informacijos ir įrodymų, o 65 % visų prašymų pateikiami kitoje valstybėje įsisteigusiems informacijos teikėjams[64]. Tai, kad tradiciniai fiziniai pėdsakai persikėlė į internetą, dar labiau padidina atotrūkį tarp teisėsaugos

[61] 2020 m. vasario 19 d. komunikatas „Europos skaitmeninės ateities formavimas“ (COM(2020) 67).

[62] Pavyzdžiui, finansinių nusikaltimų atveju.

[63] Tai reiškia, kad turi būti laikomasi galiojančių teisės aktų, įskaitant Bendrąjį duomenų apsaugos reglamentą (Reglamentą (ES) 2016/679) ir Duomenų apsaugos teisėsaugos srityje direktyvą (Direktyvą (ES) 2016/680), kuri reglamentuoja asmens duomenų tvarkymą nusikalstamų veikų nustatymo, jų užkardymo ir patraukimo baudžiamojon atsakomybėn už jas arba bausmių vykdymo tikslais.

[64] Komisijos tarnybų dokumentas SWD(2018) 118 *final*.

institucijų ir nusikaltėlių pajėgumų. Ypač svarbu nustatyti aiškias tarpvalstybinės prieigos prie elektroninių įrodymų atliekant nusikalstamų veikų tyrimus taisykles. Todėl tam, kad specialistams būtų suteikta galimybė naudotis veiksminga priemone, yra ypač svarbu, kad Europos Parlamentas ir Taryba greitai priimtų pasiūlymus dėl e. įrodymų. Be to, daugiašalėmis ir dvišalėmis tarptautinėmis derybomis sulygta tarpvalstybinė prieiga prie e. įrodymų yra itin svarbi tam, kad tarptautiniu lygmeniu būtų nustatytos suderinamos taisyklės[65].

Prieiga prie skaitmeninių įrodymų taip pat priklauso nuo informacijos prieinamumo. Jei duomenys ištrinami per anksti, gali išnykti svarbūs įrodymai, todėl nebelieka galimybės nustatyti įtariamųjų ir nusikaltėlių tinklų (taip pat nukentėjusiųjų) tapatybę ir buvimo vietą. Kita vertus, dėl duomenų saugojimo sistemų kyla privatumo apsaugos klausimų. Atsižvelgdama į Europos Teisingumo Teismo nagrinėjamų bylų baigtį, Komisija įvertins tolesnius veiksmus duomenų saugojimo srityje.

Prieiga prie interneto domenų vardų registravimo informacijos (toliau – WHOIS duomenys)[66] yra svarbi nusikalstamų veikų tyrimui, kibernetiniam saugumui ir vartotojų apsaugai. Tačiau kol Interneto vardų ir numerių paskyrimo korporacija (ICANN) nėra priėmusi naujos WHOIS politikos, prieiga prie šios informacijos tampa vis sudėtingesnė. Komisija toliau bendradarbiaus su ICANN ir įvairių suinteresuotųjų subjektų bendruomene, siekdama užtikrinti, kad teisėti subjektai, prašantys suteikti prieigą, įskaitant teisėsaugos institucijas, galėtų gauti veiksmingą prieigą prie WHOIS duomenų pagal ES ir tarptautines duomenų apsaugos taisykles. Tai apims galimų sprendimų vertinimą, įskaitant tai, ar gali prireikti priimti teisės aktus, kuriais būtų patikslintos prieigos prie tokios informacijos taisyklės.

Teisėsaugos ir teisminės institucijos turi būti pajėgios gauti būtinus duomenis ir įrodymus ir tada, kai ES **judriojo ryšio 5G architektūra** bus visiškai įdiegta taip, kad būtų užtikrinamas ryšių konfidencialumas. Komisija rems tvirtesnį ir koordinuotą požiūrį rengiant tarptautinius standartus, apibrėžiant geriausią praktiką, procesą ir techninį sąveikumą tokiose pagrindinėse technologijų srityse kaip dirbtinis intelektas, daiktų internetas ar blokų grandinės technologijos.

Šiandien didelė visų formų nusikalstamų veikų ir terorizmo atvejų tyrimų dalis yra susijusi su **užšifruota informacija**. Šifravimas yra labai svarbus skaitmeniniam pasauliui, nes jis užtikrina skaitmeninių sistemų ir sandorių saugumą, taip pat padeda apsaugoti įvairias pagrindines teises, įskaitant saviraiškos laisvę, privatumą ir duomenų apsaugą. Tačiau jei šifravimas naudojamas nusikalstamais tikslais , jis taip pat gali paslėpti nusikaltėlių tapatybę ir nuslėpti jų pranešimų turinį. Komisija įvertins subalansuotus techninius, operatyvinius ir teisinius problemų sprendimus ir jiems teiks paramą, taip pat skatins laikytis požiūrio, kuriuo būtų išlaikytas šifravimo veiksmingumas apsaugant privatumą ir ryšių saugumą ir kartu užtikrinamas veiksmingas atsakas į nusikalstamumą ir terorizmą.

Kova su neteisėtu turiniu internete

Interneto ir fizinės aplinkos saugumo suderinimas reiškia, kad reikia tęsti **kovą su neteisėtu turiniu internete**. Vis dažniau su pagrindinėmis grėsmėmis, pavyzdžiui, terorizmu, ekstremizmu arba vaikų seksualiniu išnaudojimu, piliečiai susiduria skaitmeninėje aplinkoje. Todėl tam reikia konkrečių veiksmų ir sistemos, kuriais užtikrinama pagarba pagrindinėms

[65] Tai visų pirma Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų Antrasis papildomas protokolas ir ES ir Jungtinių Amerikos Valstijų susitarimas dėl tarpvalstybinės prieigos prie e. įrodymų.

[66] Saugoma visame pasaulyje veikiančių 2 500 registrų ir registratorių tvarkomose duomenų bazėse.

teisėms. Svarbus pirmasis žingsnis – greitai užbaigti derybas dėl siūlomo teisės akto dėl teroristinio turinio internete[67] ir užtikrinti jo įgyvendinimą. Siekiant kovoti su teroristų, smurtinių ekstremistų ir nusikaltėlių piktnaudžiavimu internetu, taip pat labai svarbu stiprinti savanorišką teisėsaugos institucijų ir privačiojo sektoriaus bendradarbiavimą **ES interneto forume**. Europolo ES internetinės informacijos žymėjimo padaliniui ir toliau teks esminis vaidmuo stebint teroristinių grupių veiklą internete ir veiksmus, kurių imasi platformos[68], taip pat toliau plėtojant **ES krizių protokolą**[69]. Be to, Komisija toliau bendradarbiaus su tarptautiniais partneriais, be kita ko, dalyvaudama **Pasauliniame kovos su terorizmu interneto forume**, kad šios problemos būtų sprendžiamos pasauliniu lygmeniu. Vykdant Pilietinės visuomenės galimybių didinimo programą[70] bus toliau remiamas alternatyvaus ir atsvaros naratyvo kūrimas.

Siekdama užkirsti kelią neapykantą kurstančių kalbų plitimui internete ir kovoti su šiuo reiškiniu, 2016 metais Komisija priėmė Kovos su neapykantos kurstymu internete elgesio kodeksą, o interneto platformos savanoriškai įsipareigojo pašalinti neapykantą kurstančių kalbų turinį. Iš naujausio vertinimo matyti, kad bendrovės per 24 valandas įvertina 90 % pažymėto turinio ir pašalina 71 % turinio, kuris laikomas neapykantą kurstančia kalba. Tačiau platformos turi toliau didinti skaidrumą ir teikti grįžtamąją informaciją naudotojams, taip pat užtikrinti, kad pažymėtas turinys būtų vertinamas nuosekliai[71].

ES interneto forumas taip pat sudarys palankesnes sąlygas keistis informacija apie esamas ir kuriamas technologijas, skirtas spręsti su vaikų seksualiniu išnaudojimu internete susijusioms problemoms. Kova su vaikų seksualiniu išnaudojimu internete yra svarbiausia naujos strategijos, kurios tikslas – stiprinti **kovą su vaikų seksualiniu išnaudojimu**[72] ir kuria bus siekiama kuo geriau panaudoti ES lygmeniu turimas kovos su šiais nusikaltimais priemones, dalis. Bendrovės turi būti pajėgios toliau internete aptikti ir pašalinti vaikų seksualinio išnaudojimo medžiagą, o dėl šios medžiagos daromos žalos reikia sukurti sistemą, kurioje būtų nustatytos aiškios ir nuolatinės pareigos spręsti šią problemą. Be to, strategijoje bus paskelbta, kad Komisija taip pat pradės rengti konkretiems sektoriams skirtus teisės aktus, kuriais siekiama, visapusiškai paisant pagrindinių teisių, veiksmingiau kovoti su vaikų seksualiniu išnaudojimu internete.

Apskritai būsimajame Skaitmeninių paslaugų akte taip pat bus patikslintos ir atnaujintos su skaitmeninėmis paslaugomis susijusios atsakomybės ir saugos taisyklės ir pašalintos atgrasomosios priemonės, kurios užlaiko neteisėto turinio, prekių ar paslaugų šalinimo veiksmus.

Be to, Komisija toliau bendradarbiaus su tarptautiniais partneriais ir **Pasauliniu kovos su terorizmu interneto forumu**, be kita ko, pasitelkdama nepriklausomą patariamąjį komitetą, siekdama aptarti, kaip šalinti šias problemas pasauliniu lygmeniu, kartu išsaugant ES vertybes ir pagrindines teises. Taip pat reikėtų aptarti naujus klausimus, pavyzdžiui, dėl algoritmų ar internetinių žaidimų[73].

Hibridinės grėsmės

---

67 Pasiūlymas dėl teroristinio turinio sklaidos internete prevencijos (COM(2018) 640, 2018 09 12).

68 (Europol, November 2019)

69 *A Europe that protects - EU Crisis Protocol: responding to terrorist content online* (October 2019).

70 Susijusi su Informacijos apie radikalizaciją programos darbu, žr. IV skyriaus 3 skirsnį.

71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf.

72 ES veiksmingesnės kovos su vaikų seksualiniu išnaudojimu strategija (COM(2020) 607).

73 Teroristai ryšių palaikymo tikslais vis dažniau naudoja lošimų platformų pranešimų sistemą, o jauni teroristai vaizdo žaidimuose taip pat atkartoja smurtinius išpuolius.

Šiandien kylančių hibridinių grėsmių mastas ir įvairovė neturi precedento. Tai dar labiau pasitvirtino per COVID-19 krizę, kai keli valstybiniai ir nevalstybiniai subjektai siekė pasinaudoti pandemija, visų pirma manipuliuodami informacine aplinka ir silpnindami pagrindines infrastruktūras. Dėl to kyla rizika, kad silpnės socialinė sanglauda ir bus pakirstas pasitikėjimas ES institucijomis bei valstybių narių vyriausybėmis.

ES požiūris į hibridines grėsmes išdėstytas 2016 m. bendroje sistemoje[74] ir 2018 m. bendrame komunikate dėl atsparumo hibridinėms grėsmėms didinimo[75]. Veiksmai ES lygmeniu vykdomi remiantis nemažu priemonių rinkiniu, apimančiu vidaus ir išorės sąsają, grindžiamą visos visuomenės elementų įtraukimu ir glaudžiu bendradarbiavimu su strateginiais partneriais, visų pirma NATO ir G 7. Kartu su šia strategija skelbiama ES požiūrio į hibridines grėsmes įgyvendinimo ataskaita[76]. Remdamosi tuo pačiu metu kaip ir ši strategija teikiama apžvalga[77], Komisijos tarnybos ir Europos išorės veiksmų tarnyba sukurs **ribotos prieigos interneto platformą**, kad valstybės narės turėtų informacijos apie ES lygmens kovos su hibridinėmis grėsmėmis priemones.

Nors dėl neatsiejamų sąsajų su nacionaline saugumo ir gynybos politika atsakomybė už kovą su hibridinėmis grėsmėmis tenka visų pirma valstybėms narėms, kai kurios pažeidžiamumo sritys yra bendros visoms valstybėms narėms, o kai kurios grėsmės, pavyzdžiui, nukreiptos prieš tarpvalstybinius tinklus ar infrastruktūrą, peržengia valstybių sienas. Komisija ir vyriausiasis įgaliotinis nustatys ES požiūrį į hibridines grėsmes, pagal kurį išorės ir vidaus aspektai integruojami į nenutrūkstamą srautą ir sujungiami nacionaliniai ir ES lygmens klausimai. Tai turi apimti visą veiksmų spektrą – nuo ankstyvo nustatymo, analizės, informuotumo, atsparumo didinimo ir prevencijos iki reagavimo į krizes ir padarinių valdymo.

Be sustiprinto įgyvendinimo, kai hibridinės grėsmės nuolat kinta, ypatingas dėmesys bus skiriamas **hibridinių grėsmių klausimų įtraukimui į politikos formavimą,** siekiant neatsilikti nuo dinamiškų pokyčių ir užtikrinti, kad nė viena potencialiai svarbi iniciatyva neliktų nepastebėta. Naujų iniciatyvų, įskaitant sričių, kurios iki šiol nepateko į kovos su hibridinėmis grėsmėmis sistemos taikymo sritį, pavyzdžiui, švietimo, technologijų ir mokslinių tyrimų, iniciatyvas, poveikis taip pat bus vertinamas pagal hibridinių grėsmių kriterijus. Šiam požiūriui būtų naudingas su hibridinių grėsmių konceptualizacija susijęs darbas, padedantis susidaryti išsamų vaizdą apie įvairias priemones, kurias gali naudoti priešininkai[78]. Turėtų būti siekiama užtikrinti, kad sprendimų priėmimo procesas būtų grindžiamas reguliariomis, išsamiomis žvalgybos informacija grindžiamomis ataskaitomis apie hibridinių grėsmių raidą. Tai labai priklausys nuo valstybių narių žvalgybos informacijos ir nuo tolesnio bendradarbiavimo su valstybių narių kompetentingomis tarnybomis žvalgybos srityje stiprinimo pasitelkiant EU INTCEN.

Siekdamos didinti **informuotumą apie padėtį**, Komisijos tarnybos ir Europos išorės veiksmų tarnyba išnagrinės galimybes racionalizuoti iš įvairių šaltinių, įskaitant valstybes nares, taip pat ES agentūras, pavyzdžiui, ENISA, Europolą ir FRONTEX, gaunamos informacijos srautus. ES hibridinių grėsmių analizės ir informavimo centras ir toliau bus

[74] „Bendra kovos su mišriomis grėsmėmis sistema. Europos Sąjungos atsakas“, JOIN (2016) 18.

[75] „Atsparumo didinimas ir kovos su hibridinėmis grėsmėmis pajėgumų plėtra“, JOIN (2018) 16.

[76] 2016 m. Bendros kovos su mišriomis grėsmėmis sistemos ir 2018 m. bendro komunikato „Atsparumo didinimas ir kovos su hibridinėmis grėsmėmis pajėgumų plėtra“ įgyvendinimo ataskaita (SWD(2020) 153).

[77] Priemonių, susijusių su atsparumo didinimu ir kova su hibridinėmis grėsmėmis, apžvalga (SWD(2020) 152).

[78] *The Landscape of Hybrid Threats: A conceptual Model*, JRC117280, parengtas Jungtinio tyrimų centro kartu su Europos kovos su hibridinėmis grėsmėmis centru.

pagrindinis ES hibridinių grėsmių vertinimo centras. Siekiant užkirsti kelią hibridinėms grėsmėms ir apsaugoti nuo jų, labai svarbu **didinti atsparumą**. Todėl itin svarbu sistemingai stebėti ir objektyviai vertinti šioje srityje daromą pažangą. Pirmiausia reikės nustatyti tiek valstybių narių, tiek ES institucijų ir įstaigų sektorių atsparumo hibridinėms grėsmėms bazines vertes. Galiausiai, siekiant sustiprinti **parengtį reaguoti į hibridines krizes**, dabartinis protokolas turėtų būti peržiūrėtas, kaip nustatyta 2016 m. ES scenarijuje[79], – tai būtų platesnės šiuo metu svarstomos ES reagavimo į krizes sistemos peržiūros ir stiprinimo dalis[80]. Siekiama kuo labiau padidinti ES veiksmų poveikį greitai sutelkiant sektorių atsakomuosius veiksmus ir užtikrinant sklandų bendradarbiavimą su mūsų partneriais, visų pirma NATO.

Pagrindiniai veiksmai
• Užtikrinti, kad kibernetinius nusikaltimus reglamentuojantys teisės aktai būtų įgyvendinami ir atitiktų paskirtį • Parengti Veiksmingesnės kovos su vaikų seksualiniu išnaudojimo strategiją • Pateikti pasiūlymų dėl vaikų seksualinio išnaudojimo medžiagos nustatymo ir šalinimo • Suformuluoti ES požiūrį į kovą su hibridinėmis grėsmėmis • Atlikti ES operatyvinių veiksmų protokolo dėl kovos su hibridinėmis grėsmėmis (ES scenarijaus) peržiūrą • Įvertinti, kaip padidinti teisėsaugos pajėgumus vykdant skaitmeninius tyrimus

3. Europos piliečių apsauga nuo terorizmo ir organizuoto nusikalstamumo

Terorizmas ir radikalėjimas

Terorizmo grėsmė ES tebėra didelė. Nors bendras išpuolių skaičius sumažėjo, jie vis dar gali turėti pražūtingą poveikį. Radikalėjimas taip pat gali platesniu mastu poliarizuoti ir destabilizuoti socialinę sanglaudą. Pagrindinė atsakomybė kovojant su terorizmu ir radikalėjimu tenka valstybėms narėms. Tačiau dėl vis didėjančio tarpvalstybinio ir (arba) tarpsektorinio grėsmės aspekto reikia imtis tolesnių ES bendradarbiavimo ir koordinavimo veiksmų. Vienas iš prioritetų yra ES kovos su terorizmu teisės aktų, įskaitant ribojamąsias priemones[81], veiksmingas įgyvendinimas. Vienas iš tikslų tebėra išplėsti Europos prokuratūros įgaliojimus, kad jie apimtų tarpvalstybinius teroristinius nusikaltimus.

Kova su terorizmu prasideda nuo pagrindinių priežasčių šalinimo. Radikalių teiginių poveikį žmonėms gali padidinti visuomenės poliarizacija, reali ar numanoma diskriminacija ir kiti psichologiniai bei sociologiniai veiksniai. Šiomis aplinkybėmis kova su **radikalėjimu** yra glaudžiai susijusi su socialinės sanglaudos skatinimu vietos, nacionaliniu ir Europos lygmenimis. Per pastarąjį dešimtmetį parengtos kelios svarbios iniciatyvos ir politikos priemonės, visų pirma pasitelkiant Informacijos apie radikalizaciją tinklą ir iniciatyvą „ES

[79] ES operatyvinių veiksmų protokolas dėl kovos su hibridinėmis grėsmėmis (ES scenarijus) (SWD(2016) 227).

[80] Po 2020 m. kovo 26 d. vaizdo konferencijos Europos Vadovų Tarybos nariai priėmė pareiškimą dėl ES veiksmų reaguojant į COVID-19 protrūkį, kuriame paprašė Komisijos pateikti pasiūlymus dėl platesnio užmojo ir didelio masto krizių valdymo sistemos ES.

[81] Taryba yra priėmusi ribojamąsias priemones dėl ISIL („Da'esh“) ir „Al-Qaida“, taip pat specialias ribojamąsias priemones, taikomas tam tikriems asmenims ir subjektams siekiant kovoti su terorizmu. Visų ribojamųjų priemonių apžvalga pateikta ES sankcijų žemėlapyje (https://www.sanctionsmap.eu/#/main).

miestai prieš radikalizaciją“[82]. Atėjo laikas apsvarstyti veiksmus, kuriais būtų racionalizuota ES politika, iniciatyvos ir lėšos, skirti kovai su radikalėjimu. Tokie veiksmai gali padėti ugdyti gebėjimus ir įgūdžius, bendradarbiavimą padaryti glaudesnį, sustiprinti įrodymų bazę ir padėti vertinti pažangą, įtraukiant visus susijusius suinteresuotuosius subjektus, įskaitant pirminės grandies specialistus, politikos formuotojus ir akademinę bendruomenę[83]. Švelniosios politikos priemonėmis, pavyzdžiui, švietimo, kultūros, jaunimo ir sporto politika, galėtų būti prisidedama prie radikalizacijos prevencijos, suteikiant galimybių rizikos grupėms priklausantiems jaunuoliams ir užtikrinant sanglaudą ES[84]. Prioritetinės sritys apima darbą, susijusį su ankstyvu nustatymu ir rizikos valdymu, atsparumo didinimu ir dalyvavimo nutraukimu, taip pat reabilitacija ir reintegracija į visuomenę.

Teroristai yra siekę įsigyti **cheminių, biologinių, radiologinių ir branduolinių** (ChBRB)[85] medžiagų ir jas naudoti kaip ginklus, taip pat plėsti jų naudojimo žinias ir gebėjimus[86]. ChBRB išpuolių galimybės aiškiai minimos teroristų propagandoje. Atsižvelgiant į didelę galimą žalą, šiam klausimui reikia skirti ypač daug dėmesio. Remdamasi požiūriu, kurio laikomasi siekiant reglamentuoti prieigą prie sprogstamųjų medžiagų pirmtakų, Komisija svarstys galimybę apriboti prieigą prie tam tikrų pavojingų cheminių medžiagų, kurios galėtų būti naudojamos išpuoliams vykdyti. Taip pat bus labai svarbu plėtoti ES civilinės saugos reagavimo („rescEU“) pajėgumus ChBRB srityje. Siekiant stiprinti bendrą ChBRB saugos ir saugumo kultūrą, taip pat svarbu bendradarbiauti su trečiosiomis šalimis, visapusiškai pasinaudojant ES pasauliniais ChBRB kompetencijos centrais. Šis bendradarbiavimas aprėps nacionalinius spragų ir rizikos vertinimus, paramą nacionaliniams ir regioniniams ChBRB srities veiksmų planams, keitimąsi gerąja patirtimi ir ChBRB srities gebėjimų stiprinimo veiklą.

ES yra parengusi pažangiausius pasaulyje teisės aktus, kuriais ribojama prieiga prie **sprogstamųjų medžiagų pirmtakų**[87] ir išaiškinami įtartini sandoriai, kuriais siekiama sukurti savadarbius sprogstamuosius užtaisus. Tačiau savadarbių sprogmenų grėsmė tebėra didelė, jie naudojami daugelyje išpuolių visoje ES[88]. Pirmasis žingsnis turi būti taisyklių įgyvendinimas, taip pat užtikrinimas, kad internetinė aplinka neleistų apeiti kontrolės.

Svarbus kovos su terorizmu politikos elementas yra ir veiksmingas asmenų, įvykdžiusių teroristinius nusikaltimus, įskaitant šiuo metu Sirijoje ir Irake esančius **užsienio teroristus kovotojus**, baudžiamasis persekiojimas. Nors šiuos klausimus pirmiausia sprendžia valstybės narės, ES koordinavimas ir parama gali padėti valstybėms narėms spręsti bendras problemas. Žengiami svarbūs žingsniai siekiant visiškai įgyvendinti sienų saugumo teisės aktus[89] ir

[82] Bandomąja iniciatyva „ES miestai prieš radikalizaciją“ siekiama dvejopo tikslo – skatinti ES miestus keistis patirtimi ir rinkti grįžtamąją informaciją apie tai, kaip geriausiai remti vietos bendruomenes ES lygmeniu.

[83] Pavyzdžiui, finansavimas iš Europos saugumo fondo ir Pilietybės programos lėšų.

[84] ES veiksmai, pavyzdžiui, „Erasmus +“ virtualieji mainai, iniciatyva „eTwinning“.

[85] Pavyzdžiui, per pastaruosius dvejus metus buvo keli atvejai Europoje (Prancūzijoje, Vokietijoje, Italijoje) ir kitose šalyse (Tunise, Indonezijoje), kai buvo panaudotos biologinės medžiagos (paprastai augaliniai toksinai).

[86] Taryba yra priėmusi ribojamąsias priemones, kuriomis siekiama kovoti su cheminio ginklo platinimu ir naudojimu.

[87] Cheminės medžiagos, kurios gali būti netinkamai naudojamos savadarbiams sprogmenims gaminti. Jos reglamentuojamos 2019 m. Reglamentu (ES) 2019/1148 dėl prekybos sprogstamųjų medžiagų pirmtakais ir jų naudojimo.

[88] Keletas tokių pražūtingų išpuolių pavyzdžių yra išpuoliai Osle (2011 m.), Paryžiuje (2015 m.), Briuselyje (2016 m.) ir Mančesteryje (2017 m.). Per išpuolį naudojant savadarbius sprogmenis Lione (2019 m.) buvo sužeista 13 žmonių.

[89] Įskaitant naujus Europos sienų ir pakrančių apsaugos agentūros (FRONTEX) įgaliojimus.

visapusiškai naudotis visomis atitinkamomis ES duomenų bazėmis, kad būtų dalijamasi informacija apie žinomus įtariamuosius. Reikia ne tik identifikuoti didelę riziką keliančius asmenis, bet ir vykdyti reintegracijos ir reabilitacijos politiką. Bendradarbiavimas su įvairių profesijų atstovais, be kita ko, su kalėjimų ir probacijos darbuotojais, padės teismams suprasti radikalėjimo procesus, privedančius prie smurtinio ekstremizmo, ir sustiprins teismų sektoriaus požiūrį į bausmių skyrimą ir sulaikymui alternatyvias priemones.

Užsienio teroristų kovotojų keliamas iššūkis simbolizuoja vidaus ir **išorės saugumo** sąsajos svarbą. Bendradarbiavimas kovos su terorizmu ir radikalėjimo bei smurtinio ekstremizmo prevencijos ir kovos su jais srityse yra labai svarbus ES vidaus saugumui[90]. Reikia imtis tolesnių veiksmų siekiant plėtoti kovos su terorizmu partnerystės ryšius ir bendradarbiavimą su kaimyninėmis ir kitomis šalimis, remiantis ES kovos su terorizmu ir saugumo ekspertų tinklo patirtimi. Geras tokio tikslinio bendradarbiavimo orientyras yra Bendras veiksmų planas dėl Vakarų Balkanų kovos su terorizmu. Visų pirma turėtų būti dedamos pastangos siekiant remti šalių partnerių gebėjimus nustatyti užsienio teroristų kovotojų tapatybę ir buvimo vietą. ES taip pat toliau skatins daugiašalį bendradarbiavimą, bendradarbiaudama su pagrindiniais pasauliniais šios srities veikėjais, pavyzdžiui, Jungtinėmis Tautomis, NATO, Europos Taryba, Interpolu ir ESBO. Ji taip pat dalyvaus Pasaulinio kovos su terorizmu forumo ir Tarptautinės kovos su „Da'esh“ koalicijos, taip pat atitinkamų pilietinės visuomenės subjektų veikloje. Sąjungos išorės politikos priemonės, įskaitant vystymosi ir bendradarbiavimo politiką, taip pat atlieka svarbų vaidmenį kartu su trečiosiomis šalimis siekiant užkirsti kelią terorizmui ir piratavimui. Tarptautinis bendradarbiavimas taip pat yra labai svarbus siekiant panaikinti visus **terorizmo finansavimo** šaltinius, pavyzdžiui, pasitelkiant Finansinių veiksmų darbo grupę.

Organizuotas nusikalstamumas

Organizuotas nusikalstamumas turi didelį finansinį poveikį ekonomikai ir asmenims. Apskaičiuota, kad ekonominiai nuostoliai dėl organizuoto nusikalstamumo ir korupcijos kasmet sudaro 218–282 mlrd. EUR[91]. 2017 m. Europoje buvo atliekamas tyrimas dėl daugiau kaip 5 000 organizuotų nusikalstamų grupių, t. y. 50 % daugiau nei 2013 m.[92]. Organizuotas nusikalstamumas vis dažniau peržengia valstybių sienas, be kita ko, plinta iš artimiausių ES kaimyninių šalių, todėl reikia aktyviau koordinuoti operatyvinę veiklą ir keistis informacija su kaimyninių šalių partneriais.

Atsiranda naujų iššūkių, o nusikalstamumas persikelia į internetą: per COVID-19 pandemiją labai padaugėjo į pažeidžiamas grupes nukreipto sukčiavimo internetu atvejų, taip pat sveikatos ir sanitarijos produktų vagysčių ir įsilaužimų siekiant juos pavogti[93]. ES turi aktyviau kovoti su organizuotu nusikalstamumu, be kita ko, tarptautiniu lygmeniu, naudodama daugiau priemonių organizuoto nusikalstamumo verslo modeliui išardyti. Kovojant su organizuotu nusikalstamumu taip pat reikia glaudžiai bendradarbiauti su vietos ir regionų valdžios institucijomis, taip pat pilietine visuomene – pagrindiniais partneriais vykdant nusikalstamumo prevenciją, taip pat teikiant pagalbą ir paramą nukentėjusiesiems, –

[90] 2020 m. birželio 16 d. Tarybos išvadose pabrėžta, kad reikia apsaugoti ES piliečius nuo visų formų terorizmo ir smurtinio ekstremizmo, nepriklausomai nuo jų kilmės, ir toliau stiprinti ES išorės bendradarbiavimą ir veiksmus, kiek tai susiję su kova su terorizmu, prioritetinėse geografinėse ir teminėse srityse.

[91] Pagal bendrąjį vidaus produktą (BVP); Europolo ataskaita *Does crime still pay? – Criminal asset recovery in the EU*, 2016.

[92] Europol, *Serious and Organised Threat Assessments (SOCTA)*, 2013 and 2017.

[93] (Europol, 2020)

to ypač reikia pasienio regionų valdžios institucijoms. Šis darbas bus įtrauktas į **kovos su organizuotu nusikalstamumu darbotvarkę**.

Daugiau kaip trečdalis ES veikiančių organizuotų nusikalstamų grupių užsiima narkotikų gamyba, prekyba jais ar jų platinimu. Dėl priklausomybės nuo narkotikų 2019 m. ES nuo perdozavimo mirė daugiau kaip aštuoni tūkstančiai žmonių. Didžioji dalis **prekybos narkotikais** vyksta tarpvalstybiniu mastu, o didelė dalis pelno patenka į teisėtą ekonomiką[94]. Nauja ES kovos su narkotikais darbotvarke[95] bus stiprinamos ES ir valstybių narių pastangos narkotikų paklausos ir pasiūlos mažinimo srityse, bus apibrėžti bendri veiksmai, kuriais sprendžiama bendra problema, stiprinamas ES ir išorės partnerių dialogas ir bendradarbiavimas narkotikų klausimais. Atlikusi Europos narkotikų ir narkomanijos stebėsenos centro veiklos vertinimą Komisija įvertins, ar reikia atnaujinti jo įgaliojimus, kad jie atitiktų naujus iššūkius.

Organizuotos nusikalstamos grupės ir teroristai taip pat yra pagrindiniai prekybos **neteisėtais šaunamaisiais ginklais** dalyviai. 2009–2018 m. Europoje įvykdyti 23 masinės šaudynės, per kurias žuvo daugiau kaip 340 žmonių[96]. Šaunamieji ginklai į ES dažnai neteisėtai patenka per artimiausias kaimynines šalis[97]. Tai rodo, kad, siekiant suderinti informacijos apie konfiskuotus šaunamuosius ginklus rinkimą ir ataskaitų teikimą, reikia stiprinti veiklos koordinavimą ir bendradarbiavimą tiek ES viduje, tiek su tarptautiniais partneriais, visų pirma Interpolu. Taip pat labai svarbu pagerinti ginklų atsekamumą, be kita ko, internete, ir užtikrinti, kad licencijavimo ir teisėsaugos institucijos keistųsi informacija. Komisija teikia naują **ES kovos su neteisėta prekyba šaunamaisiais ginklais veiksmų planą**[98] ir įvertins, ar šaunamųjų ginklų eksporto leidimų sistema ir importo bei tranzito priemonės vis dar atitinka paskirtį[99].

Nusikalstamos organizacijos su migrantais ir asmenimis, kuriems reikia tarptautinės apsaugos, elgiasi taip, tarsi jie būtų prekės. 90 % atvykstančių migrantų neteisėtai patekti į ES padeda nusikalstamas tinklas[100]. Neteisėtas migrantų gabenimas taip pat dažnai yra susijęs su kitų formų organizuotu nusikalstamumu, visų pirma prekyba žmonėmis[101]. Be to, kad prekyba žmonėmis reikalauja labai daug gyvybių, Europolas yra apskaičiavęs, kad visame pasaulyje dėl visų formų išnaudojimo, susijusio su prekyba žmonėmis, kasmet gaunama 29,4 mlrd. EUR pelno. Tai tarpvalstybinis nusikaltimas, kuriuo tenkinami neteisėti poreikiai tiek ES viduje, tiek už jos ribų ir kuris daro poveikį visoms ES valstybėms narėms. Dėl prastų rezultatų, susijusių su šių nusikaltimų nustatymu, patraukimu baudžiamojon atsakomybėn už juos ir juos padariusių asmenų nuteisimu, reikia naujo požiūrio, kuriuo būtų sustiprinti veiksmai. Naujas **visapusiškas požiūris į prekybą žmonėmis** sujungs pavienius veiksmus. Be to, Komisija pateiks **naują ES kovos su neteisėtu migrantų gabenimu veiksmų planą**, skirtą 2021–2025 m. laikotarpiui. Abiejose srityse daugiausia dėmesio bus

---

94 EMCDDA and Europol, *EU Drug Markets Report 2019* (November 2019).

95 ES kovos su narkotikais darbotvarkė ir veiksmų planas (2021–2025 m.) (COM(2020) 606).

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

97 Nuo 2002 m. ES finansuoja kovą su šaulių ir lengvųjų ginklų platinimu ir neteisėta prekyba jais regione; ji visų pirma finansuoja Pietryčių Europos šaunamųjų ginklų ekspertų tinklą (SEEFEN). Nuo 2019 m. Vakarų Balkanų šalys partnerės visapusiškai dalyvauja įgyvendinant Europos kovos su nusikalstamumo grėsmėmis tarpdisciplininės platformos (EMPACT) prioritetą šaunamųjų ginklų srityje.

98 COM(2020) 608.

99 Reglamentas (ES) Nr. 258/2012, kuriuo įgyvendinamas Jungtinių Tautų protokolo prieš neteisėtą šaunamųjų ginklų gamybą ir prekybą jais 10 straipsnis.

100 Šaltinis: Europolas.

101 Europol, EMSC, *4th Annual Report*.

skiriama kovai su nusikaltėlių tinklais, bendradarbiavimo skatinimui ir teisėsaugos darbo rėmimui.

Organizuotos nusikalstamos grupės, kaip ir teroristai, ieško galimybių ir kitose srityse, visų pirma tose, kuriose pelnas didelis, o nusikaltimų išaiškinimo rizika – maža, pavyzdžiui, **nusikaltimų aplinkai** atveju. Neteisėta laukinių gyvūnų medžioklė ir prekyba jais, neteisėta kasyba, medienos ruoša, neteisėtas atliekų šalinimas ir vežimas tapo ketvirta pagal mastą nusikalstama veikla visame pasaulyje[102]. Taip pat būta atvejų, kai buvo nusikalstamai naudojamos apyvartinių taršos leidimų prekybos sistemos ir energijos sertifikatų sistemos ir netinkamai naudojamos aplinkos atsparumui didinti ir darniam vystymuisi skirtos lėšos. Komisija ne tik skatina ES, valstybes nares ir tarptautinę bendruomenę stiprinti kovą su nusikaltimais aplinkai[103], bet ir vertina, ar Nusikaltimų aplinkai direktyva[104] vis dar atitinka savo paskirtį. **Neteisėta prekyba kultūros vertybėmis** taip pat tapo viena iš pelningiausių nusikalstamų veikų; ji yra teroristų ir organizuoto nusikalstamumo finansavimo šaltinis ir jos mastas didėja. Reikėtų išnagrinėti, kaip vidaus rinkoje geriau atsekti kultūros vertybes internete ir realiame gyvenime, sustiprinti bendradarbiavimą su trečiosiomis šalimis, kuriose kultūros vertybės grobiamos, ir aktyviai remti teisėsaugos ir akademines bendruomenes.

Ekonominiai ir finansiniai nusikaltimai yra labai sudėtingi, tačiau kasmet ES jie paveikia milijonus piliečių ir tūkstančius įmonių. Kova su sukčiavimu yra labai svarbi ir reikalauja ES lygmens veiksmų. Europolas, Eurojustas, Europos prokuratūra ir Europos kovos su sukčiavimu tarnyba padeda valstybėms narėms ir ES apsaugoti ekonomikos ir finansų rinkas ir ES mokesčių mokėtojų pinigus. 2020 m. pabaigoje Europos prokuratūra pradės visapusiškai veikti ir tirti nusikaltimus, susijusius su ES biudžetu, pavyzdžiui, sukčiavimą, korupciją ir pinigų plovimą, vykdyti baudžiamąjį persekiojimą už juos ir perduoti bylas teismui. Ji taip pat kovos su tarpvalstybiniu sukčiavimu PVM, dėl kurio mokesčių mokėtojai netenka bent 50 mlrd. EUR per metus.

Komisija taip pat rems ekspertinių žinių plėtrą ir kylančiai rizikai, pavyzdžiui, susijusiai su kriptoturtu ir naujomis mokėjimo sistemomis, skirtų teisės aktų rengimą. Visų pirma Komisija išnagrinės, kaip reaguoti į kriptoturto, pavyzdžiui, bitkoino, atsiradimą ir kokį poveikį šios naujos technologijos turės finansinio turto išleidimo, keitimosi juo, dalijimosi juo ir prieigos prie jo būdams.

Europos Sąjungoje neteisėti pinigai turėtų būti visiškai netoleruojami. Per trisdešimt metų ES, visapusiškai atsižvelgdama į poreikį apsaugoti asmens duomenis, sukūrė tvirtą **pinigų plovimo** ir teroristų finansavimo prevencijos ir kovos su jais reguliavimo sistemą. Vis dėlto vis labiau sutariama, kad dabartinės sistemos įgyvendinimą reikia gerokai pagerinti. Reikia pašalinti pagrindinius jos taikymo skirtumus ir didelius taisyklių vykdymo užtikrinimo trūkumus. Kaip išsamiai išdėstyta 2020 m. gegužės mėn. veiksmų plane[105], vyksta darbas siekiant įvertinti galimybes stiprinti ES kovos su pinigų plovimu ir teroristų finansavimu sistemą. Tarp tirtinų sričių yra nacionalinių centralizuotų banko sąskaitų registrų sujungimas, kuris galėtų gerokai pagreitinti finansinės žvalgybos padalinių ir kompetentingų institucijų prieigą prie finansinės informacijos.

[102] UNEP ir Interpolo skubiai atliktas vertinimas (*Rapid Response Assessment: The Rise of Environmental Crime*, June 2016).
[103] Žr. Europos žaliąjį kursą (COM(2019) 640 *final*).
[104] Direktyva 2008/99/EB dėl aplinkos apsaugos pagal baudžiamąją teisę.
[105] Pinigų plovimo ir teroristų finansavimo prevencijos veiksmų planas (COM(2020) 2800).

Apskaičiuota, kad **organizuotų nusikalstamų grupių pelnas** ES siekia 110 mlrd. EUR per metus. Dabartinis atsakas apima suderintus teisės aktus dėl konfiskavimo ir turto susigrąžinimo[106], siekiant pagerinti nusikalstamu būdu įgyto turto įšaldymą ir konfiskavimą ES, padidinti valstybių narių tarpusavio pasitikėjimą ir palengvinti veiksmingą tarpvalstybinį bendradarbiavimą. Tačiau tik maždaug 1 % šio pelno yra konfiskuojama[107], ir tai leidžia organizuotoms nusikalstamoms grupėms investuoti į savo nusikalstamos veiklos plėtrą ir įsiskverbti į teisėtą ekonomiką: pagrindinis pinigų plovimo taikinys visų pirma yra mažosios ir vidutinės įmonės, kurioms sunku gauti kreditą. Komisija išnagrinės teisės aktų įgyvendinimą[108] ir galimą papildomų bendrų taisyklių, be kita ko, dėl ne apkaltinamuoju nuosprendžiu pagrįsto konfiskavimo, poreikį. Turto susigrąžinimo tarnybos[109], kurios yra pagrindiniai turto susigrąžinimo proceso dalyviai, taip pat galėtų būti numatyta geresnių priemonių turtui visoje ES greičiau identifikuoti ir atsekti ir taip padidinti konfiskavimo normą.

Organizuotas nusikalstamumas ir **korupcija** yra glaudžiai susiję. Apskaičiuota, kad vien dėl korupcijos ES ekonomika per metus praranda 120 mlrd. EUR[110]. Korupcijos prevencija ir kova su ja ir toliau bus reguliariai stebimos pagal teisinės valstybės mechanizmą ir per Europos semestrą. Per Europos semestrą įvertinti kovos su korupcija iššūkiai, pavyzdžiui, viešųjų pirkimų, viešojo administravimo, verslo aplinkos ar sveikatos priežiūros srityse. Naujojoje Komisijos metinėje teisinės valstybės principo taikymo ataskaitoje bus aptariama kova su korupcija ir ji sudarys sąlygas vykdyti prevencinį dialogą su nacionalinėmis valdžios institucijomis ir suinteresuotaisiais subjektais ES ir nacionaliniu lygmenimis. Pilietinės visuomenės organizacijos taip pat gali atlikti svarbų vaidmenį skatinant valdžios institucijų veiksmus organizuoto nusikalstamumo ir korupcijos prevencijos ir kovos su jais srityje, todėl būtų naudinga, jei jos galėtų būti sujungtos į bendrą forumą. Dėl savo tarpvalstybinio pobūdžio kitas svarbus aspektas yra bendradarbiavimas su ES kaimyniniais regionais ir pagalba jiems organizuoto nusikalstamumo ir korupcijos klausimais.

Pagrindiniai veiksmai
• Įgyvendinti ES kovos su terorizmu darbotvarkę, įskaitant atnaujintus ES kovos su radikalėjimu veiksmus • Užmegzti naują bendradarbiavimą su pagrindinėmis trečiosiomis šalimis ir tarptautinėmis organizacijomis kovos su terorizmu srityje • Įgyvendinti kovos su organizuotu nusikalstamumu, įskaitant prekybą žmonėmis, darbotvarkę • Įgyvendinti ES kovos su narkotikais darbotvarkę ir 2021–2025 m. veiksmų planą • Įvertinti Europos narkotikų ir narkomanijos stebėsenos centro veiklą • Įgyvendinti 2020–2025 m. ES kovos su neteisėta prekyba šaunamaisiais ginklais veiksmų planą • Peržiūrėti teisės aktus dėl įšaldymo ir konfiskavimo ir dėl turto susigrąžinimo tarnybų • Peržiūrėti Nusikaltimų aplinkai direktyvą

[106] Pagal ES teisę reikalaujama, kad turto susigrąžinimo tarnybos būtų įsteigtos visose valstybėse narėse.

[107] Ataskaita „Turto susigrąžinimas ir konfiskavimas: užtikrinti, kad nusikaltimai neapsimokėtų“ (COM(2020) 217 *final*).

[108] Direktyva 2014/42/ES dėl nusikaltimų priemonių ir pajamų iš nusikaltimų įšaldymo ir konfiskavimo.

[109] Tarybos sprendimas 2007/845/JHA dėl valstybių narių turto susigrąžinimo tarnybų bendradarbiavimo nusikalstamu būdu įgytų pajamų bei kito susijusio turto paieškos ir nustatymo srityje..

[110] Nors bendrą korupcijos poveikį ekonomikai įvertinti sunku, jį mėgino apskaičiuoti įvairios įstaigos, įskaitant Tarptautinius prekybos rūmus, „Transparency International“, JT pasaulinį susitarimą ir Pasaulio ekonomikos forumą, ir galima daryti išvadą, kad korupcija sudaro 5 % pasaulinio BVP.

- Įgyvendinti ES kovos su neteisėtu migrantų gabenimu veiksmų planą (2021–2025 m.)

4. Stipri Europos saugumo ekosistema

Tikra ir efektyvi saugumo sąjunga turi būti bendras visų visuomenės grupių siekis. Kad būtų užtikrinta visų, pirmiausia pažeidžiamiausių grupių, nukentėjusiųjų ir liudytojų, parengtis ir atsparumas, vyriausybės, teisėsauga, privatusis sektorius, švietimo sistema ir patys piliečiai turi būti aktyvūs, turėti tinkamų priemonių ir tinkamai palaikyti ryšius.

Į visų krypčių politiką reikia įtraukti saugumo elementą, o ES gali prisidėti visais lygmenimis. Vienas iš didžiausių pavojų saugumui namuose – smurtas šeimoje. 22 % moterų ES yra patyrusios partnerio smurtą[111]. Vienas iš svarbiausių prioritetų tebėra ES prisijungimas prie Stambulo konvencijos dėl smurto prieš moteris ir smurto šeimoje prevencijos ir kovos su juo. Jeigu derybos liks įstrigusios, Komisija imsis kitų priemonių, kad pasiektų tuos pačius tikslus, kurių siekiama Konvencija, be kita ko, pasiūlys smurtą prieš moteris įtraukti į Sutartyje apibrėžtų nusikaltimų sąrašą.

Bendradarbiavimas ir informacijos mainai

Vienas iš svarbiausių būdų, kuriuo ES gali prisidėti prie piliečių apsaugos, – tai padėti už saugumą atsakingiems subjektams tinkamai dirbti kartu. Bendradarbiavimas ir dalijimasis informacija yra galingiausios priemonės kovoti su nusikalstamumu ir terorizmu ir vykdyti teisingumą. Kad tos priemonės būtų efektyvios, jos turi būti tikslingos ir savalaikės. Kad jomis būtų galima pasitikėti, jas reikia naudoti taikant bendras apsaugos priemones ir kontrolę.

Siekiant toliau plėtoti valstybių narių **operatyvinį teisėsaugos bendradarbiavimą** sukurta nemažai ES priemonių ir sektoriams skirtų strategijų[112]. Viena iš pagrindinių ES priemonių, kuriomis remiamas valstybių narių teisėsaugos bendradarbiavimas, yra Šengeno informacinė sistema, naudojama realiuoju laiku keistis duomenimis apie ieškomus ir dingusius asmenis ir daiktus. Naudojant šią priemonę pasiekta rezultatų – sulaikomi nusikaltėliai, konfiskuojami narkotikai ir išgelbėjami potencialūs nukentėjusieji[113]. Tačiau bendradarbiavimo lygis dar gali būti pakeltas supaprastinant ir atnaujinant turimas priemones. Didžioji dalis ES teisės aktų, kuriais grindžiamas operatyvinis bendradarbiavimas, parengti prieš 30 metų. Sudėtinga valstybių narių dvišalių susitarimų, iš kurių daugelis yra pasenę ar nepakankamai taikomi, struktūra kelia susiskaidymo riziką. Mažesnių ar žemyninių šalių teisėsaugos pareigūnai, atlikdami tarpvalstybinius operatyvinius veiksmus, tam tikrais atvejais turi laikytis net septynių skirtingų taisyklių rinkinių, todėl kai kurios operacijos, pavyzdžiui, aktyvus įtariamųjų persekiojimas kertant vidaus sienas, paprasčiausiai nevykdomos. Operatyvinis bendradarbiavimas taikant naujas technologijas, pavyzdžiui, bepiločius orlaivius, taip pat neįtrauktas į dabartinę ES sistemą.

Operatyvinį veiksmingumą gali padidinti konkretus teisėsaugos institucijų bendradarbiavimas, kuris taip pat gali padėti teikti esminę paramą siekiant kitų politikos tikslų, pavyzdžiui, teikti saugumo informaciją, reikalingą atliekant naująjį tiesioginių užsienio investicijų vertinimą. Komisija išnagrinės, kaip tai pasiekti gali padėti Policijos

[111] „Lygybės sąjunga. 2020–2025 m. lyčių lygybės strategija“ (COM(2020) 152).

[112] Pavyzdžiui, ES jūrų saugumo strategijos veiksmų planu pasiekta svarbių rezultatų, susijusių su atitinkamų ES agentūrų bendradarbiavimu pakrančių apsaugos funkcijų klausimais.

[113] ES kova su organizuotu nusikalstamumu 2019 m. (Taryba, 2020).

bendradarbiavimo kodeksas. Valstybių narių teisėsaugos institucijos vis dažniau naudojasi ES lygmens parama ir ekspertinėmis žiniomis, o EU INTCEN atlieka svarbų vaidmenį skatinant valstybių narių žvalgybos ir saugumo tarnybas keistis strategine žvalgybos informacija, didindamas žvalgybos informacija grindžiamą ES institucijų informuotumą apie padėtį[114]. **Europolas** taip pat gali atlikti svarbų vaidmenį plėsdamas bendradarbiavimą su trečiosiomis šalimis kovos su nusikalstamumu ir terorizmu tikslais, kartu taikant kitas ES išorės politikos strategijas ir priemones. Tačiau šiuo metu Europolas susiduria su keliais rimtais apribojimais, visų pirma susijusiais su tiesioginiu keitimusi asmens duomenimis su privačiais subjektais, – tai trukdo Europolui veiksmingai remti valstybes nares kovojant su terorizmu ir nusikalstamumu. Šiuo metu vertinami Europolo įgaliojimai, siekiant nustatyti, kaip juos reikėtų patobulinti, kad Agentūra galėtų visapusiškai vykdyti savo užduotis. Atsižvelgiant į tai, glaudžiau bendradarbiauti ir gerinti keitimąsi informacija taip pat turėtų atitinkamos ES lygmens institucijos (pavyzdžiui, OLAF, Europolas, Eurojustas ir Europos prokuratūra).

Kita svarbi sąsaja – tolesnis **Eurojusto** plėtojimas siekiant kuo didesnės teisėsaugos institucijų bendradarbiavimo ir teisminio bendradarbiavimo sinergijos. ES būtų naudingas ir didesnis strateginis nuoseklumas: **EMPACT**[115] – kovos su organizuotu ir sunkių formų tarptautiniu nusikalstamumu ES politikos ciklas – yra valdžios institucijoms skirta kriminalinės žvalgybos informacija grindžiama metodika, kuria remdamosi jos galėtų bendrai kovoti su svarbiausiomis kriminalinėmis grėsmėmis, kylančiomis ES. Per pastarąjį dešimtmetį buvo pasiekta svarbių operatyvinės veiklos rezultatų[116]. Remiantis specialistų patirtimi, dabartinis mechanizmas turėtų būti racionalizuotas ir supaprastintas, kad per naują 2022–2025 m. politikos ciklą būtų galima geriau reaguoti į aktualiausias ir labiausiai kintančias nusikalstamumo grėsmes.

Laiku teikiama aktuali **informacija** yra labai svarbi kasdieniam darbui, susijusiam su persekiojimu už nusikaltimus. Nors ES lygmeniu sukurta naujų saugumo ir sienų valdymo duomenų bazių, vis dar daug informacijos laikoma nacionalinėse duomenų bazėse arba keičiamasi nesinaudojant ES priemonėmis. To pasekmė – didelis papildomas darbo krūvis, vėlavimai ir didesnė rizika, kad esminė informacija bus praleista. Geresnių rezultatų būtų pasiekta visą saugumo bendruomenę įtraukiančiais geresniais, spartesniais ir paprastesniais procesais. Siekiant pasinaudoti visu informacijos mainų potencialu vykdant veiksmingą persekiojimą už nusikaltimus ir kartu įdiegti reikiamas apsaugos priemones, kad dalijantis informacija būtų paisoma duomenų apsaugos teisės aktų ir pagrindinių teisių, labai svarbu turėti tinkamas priemones. Atsižvelgdama į technologijų, teismo ekspertizės ir duomenų apsaugos pokyčius ir pasikeitusius naudojimo poreikius, ES galėtų apsvarstyti, ar reikia modernizuoti tokias priemones kaip **2008 m. Priumo sprendimai**, kuriais nustatomas automatinis keitimasis DNR, pirštų atspaudų ir transporto priemonių registracijos duomenimis, kad nusikalstamų veikų tyrimo tikslais būtų galima automatiškai keistis papildomų kategorijų duomenimis, kurie jau yra teistumo ar kitose valstybių narių duomenų bazėse. Be to, Komisija išnagrinės galimybę keistis informacija apie teistumą, kad padėtų nustatyti, ar yra kokios nors su asmeniu susijusios informacijos apie teistumą kitose valstybėse narėse, ir palengvintų prieigą prie šios informacijos, kai ji bus nustatyta, taikant visas būtinas apsaugos priemones.

[114] EU INTCEN yra vienintelis valstybių narių žvalgybos ir saugumo tarnybų portalas, kuris padeda didinti žvalgybos informacija grindžiamą ES informuotumą apie padėtį.

[115] EMPACT – Europos kovos su nusikalstamumo grėsmėmis daugiadalykė platforma.

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

Informacija apie keliautojus padėjo pagerinti sienų kontrolę, sumažinti neteisėtą migraciją ir nustatyti pavojų saugumui keliančius asmenis. Išankstinės informacijos apie keleivius duomenys – kiekvieno keleivio biografiniai duomenys, kuriuos oro vežėjai surenka registracijos metu ir iš anksto išsiunčia paskirties vietos sienų kontrolės institucijoms. Peržiūrėjus teisinę bazę[117] būtų galima veiksmingiau naudoti informaciją, kartu užtikrinant atitiktį duomenų apsaugos teisės aktams ir palengvinant keleivių srautą. Keleivio duomenų įrašai (PNR) – duomenys, kuriuos keleiviai pateikia rezervuodami skrydžius. PNR direktyvos[118] įgyvendinimas labai svarbus, todėl Komisija toliau rems šį procesą ir užtikrins jo vykdymą. Be to, vidutinės trukmės laikotarpiu Komisija pradės dabartinio **PNR duomenų perdavimo trečiosioms šalims** metodo peržiūrą.

Policijos pastangas kovoti su tarpvalstybiniu nusikalstamumu būtina papildyti **teisminiu bendradarbiavimu**. Per pastaruosius 20 metų teisminis bendradarbiavimas iš esmės pasikeitė. Tokioms įstaigoms kaip **Europos prokuratūra** ir **Eurojustas** reikia turėti priemonių, kad galėtų veikti visu pajėgumu arba būtų sustiprintos. Praktikuojančių teisėjų bendradarbiavimas taip pat galėtų būti stiprinamas imantis tolesnių veiksmų, susijusių su teismo sprendimų tarpusavio pripažinimu, teisėjų mokymu ir informacijos mainais. Turėtų būti siekiama teisėjų ir prokurorų tarpusavio pasitikėjimo, nes tai esminis sklandaus tarpvalstybinio bylų nagrinėjimo veiksnys. Mūsų teisingumo sistemų veiksmingumą taip pat gali padidinti **skaitmeninių technologijų** naudojimas. Remiant Eurojustui kuriama nauja skaitmeninė keitimosi informacija sistema, kuria būtų galima perduoti Europos tyrimo orderius, savitarpio teisinės pagalbos prašymus ir susijusius valstybių narių pranešimus. Komisija bendradarbiaus su valstybėmis narėmis, kad paspartintų reikiamų IT sistemų diegimą nacionaliniu lygmeniu.

Siekiant veiksmingo teisėsaugos ir teisminio bendradarbiavimo, taip pat labai svarbus yra tarptautinis bendradarbiavimas. Dvišaliai susitarimai su pagrindiniais partneriais atlieka pagrindinį vaidmenį užtikrinant, kad iš ES nepriklausančių šalių būtų galima gauti informaciją ir įrodymus. Svarbų vaidmenį atlieka **Interpolas** – viena iš didžiausių tarpvyriausybinių kriminalinės policijos organizacijų. Komisija išnagrinės galimybes sustiprinti bendradarbiavimą su Interpolu, įskaitant galimybę gauti prieigą prie Interpolo duomenų bazių ir sustiprinti operatyvinį ir strateginį bendradarbiavimą. ES teisėsaugos institucijos taip pat kliaujasi šalimis, kurios yra pagrindinės partnerės, kad atskleistų nusikaltėlius ir teroristus ir atliktų nusikalstamų veikų tyrimą. Siekiant stiprinti bendradarbiavimą kovojant su bendromis grėsmėmis, pavyzdžiui, terorizmu, organizuotu nusikalstamumu, kibernetiniais nusikaltimais, vaikų seksualiniu išnaudojimu ir prekyba žmonėmis, galėtų būti sustiprinta **ES ir trečiųjų šalių partnerystė saugumo srityje**. Toks požiūris būtų grindžiamas bendrais saugumo interesais ir nusistovėjusiu bendradarbiavimu bei dialogu saugumo klausimais.

Keitimasis ne tik informacija, bet ir patirtimi gali būti ypač vertingas didinant teisėsaugos parengtį reaguoti į **netradicines grėsmes**. Komisija ne tik skatins keistis geriausia patirtimi, bet ir išnagrinės galimą **ES lygmens koordinavimo mechanizmą, skirtą policijos pajėgoms** *force majeure* įvykių, pavyzdžiui, pandemijos, atveju. Pandemija taip pat parodė, kad kovojant su nusikalstamumu ir terorizmu itin svarbus vaidmuo teks skaitmeninės bendruomenės tvarkos palaikymui ir teisinei bazei, palengvinančiai viešosios tvarkos palaikymą internete. Policijos ir bendruomenių partnerystė realiame gyvenime ir internete

[117] Tarybos direktyva 2004/82/EB dėl vežėjų įpareigojimo perduoti keleivių duomenis.

[118] Direktyva (ES) 2016/681 dėl keleivio duomenų įrašo (PNR) duomenų naudojimo teroristinių nusikaltimų ir sunkių nusikaltimų prevencijos, nustatymo, tyrimo ir patraukimo už juos baudžiamojon atsakomybėn tikslais.

gali užkirsti kelią nusikalstamumui ir sumažinti organizuoto nusikalstamumo, radikalėjimo ir teroristinės veiklos poveikį. Ryšys tarp vietos ir regioninių bei nacionalinių ir ES lygmens policijos sprendimų yra pagrindinis visos ES saugumo sąjungos sėkmės veiksnys.

Tvirtų išorės sienų reikšmė

Šiuolaikiškas ir veiksmingas išorės sienų valdymas teikia dvejopą naudą – išlaikomas Šengeno erdvės vientisumas ir užtikrinamas mūsų piliečių saugumas. Visų susijusių subjektų įtraukimas siekiant kuo labiau pasinaudoti sienų saugumu gali turėti realų poveikį tarpvalstybinio nusikalstamumo ir terorizmo prevencijai. Neseniai sustiprintų Europos sienų ir pakrančių apsaugos pajėgų[119] bendra operatyvine veikla prisidedama prie tarpvalstybinio nusikalstamumo prie **išorės sienų** ir už ES ribų prevencijos ir atskleidimo. Muitinių veikla nustatant visų prekių saugos ir saugumo riziką prieš jas įvežant į ES ir atliekant įvežamų prekių tikrinimą, yra labai svarbi kovojant su tarpvalstybiniu nusikalstamumu ir terorizmu. Būsimajame Muitų sąjungos veiksmų plane bus paskelbti veiksmai, kuriais taip pat bus stiprinamas rizikos valdymas ir didinamas vidaus saugumas, be kita ko, visų pirma įvertinant atitinkamų saugumo rizikos analizei skirtų informacinių sistemų sąsajos galimybes.

2019 m. gegužės mėn. priimta **ES informacinių sistemų** teisingumo ir vidaus reikalų srityje **sąveikumo** sistema. Šia nauja struktūra siekiama padidinti naujų arba atnaujintų informacinių sistemų veiksmingumą ir efektyvumą[120]. Taip teisėsaugos pareigūnams, sienos apsaugos pareigūnams ir migracijos pareigūnams bus teikiama greitesnė ir sistemingesnė informacija. Tai padės teisingai nustatyti tapatybę ir kovoti su tapatybės klastojimu. Kad tai taptų realybe, sąveikumo įgyvendinimui turėtų būti skiriama pirmenybė tiek politiniu, tiek techniniu lygmeniu. Kad iki 2023 m. būtų pasiektas visiško sąveikumo tikslas, itin svarbus bus glaudus ES agentūrų ir visų valstybių narių bendradarbiavimas.

Kelionės dokumentų klastojimas laikomas vienu iš dažniausių nusikaltimų. Jis palengvina neteisėtą nusikaltėlių ir teroristų judėjimą ir atlieka pagrindinį vaidmenį prekybos žmonėmis ir narkotikais srityje[121]. Komisija išnagrinės, kaip išplėsti vykdomą darbą, susijusį su ES gyvenamosios vietos ir kelionės dokumentų saugumo standartais, be kita ko, pasitelkdama skaitmeninimą. Nuo 2021 m. rugpjūčio mėn. valstybės narės pradės išduoti tapatybės korteles ir teisę gyventi šalyje patvirtinančius dokumentus pagal suderintus saugumo standartus, įskaitant lustą su biometriniais identifikatoriais, kuriuos gali patikrinti visos ES sienos apsaugos institucijos. Komisija stebės, kaip įgyvendinamos šios naujos taisyklės, įskaitant laipsnišką šiuo metu naudojamų dokumentų keitimą.

Saugumo mokslinių tyrimų stiprinimas ir inovacijų didinimas

Siekiant užtikrinti kibernetinį saugumą ir kovoti su organizuotu nusikalstamumu, kibernetiniais nusikaltimais ir terorizmu, ateityje labai svarbu plėtoti šias priemones: padėti kurti saugesnes ir labiau apsaugotas naujas technologijas, spręsti technologijų keliamus

[119] Jį sudaro Europos sienų ir pakrančių apsaugos agentūra (FRONTEX) ir valstybių narių sienų apsaugos ir pakrančių apsaugos institucijos.

[120] Atvykimo ir išvykimo sistema (AIS), Europos kelionių informacijos ir leidimų sistema (ETIAS), išplėsta Europos nuosprendžių registrų informacinė sistema (ECRIS-TCN), Šengeno informacinė sistema, Vizų informacinė sistema ir būsima atnaujinta sistema EURODAC

[121] Dokumentų klastojimo ir prekybos žmonėmis sąsaja aptarta Antrojoje kovos su prekyba žmonėmis pažangos ataskaitoje (COM(2018) 777) ir prie jos pridėtame tarnybų darbiniame dokumente (SWD(2018) 473), taip pat Europolo prekybos žmonėmis padėties ES ataskaitoje (Europol, *Situation Report Trafficking in human beings in the EU*, 2016).

iššūkius ir remti teisėsaugos darbą. Tai savo ruožtu priklauso nuo privačių partnerių ir pramonės įmonių.

Inovacijos turėtų būti laikomos strategine kovos su dabartinėmis grėsmėmis ir būsimos rizikos bei galimybių numatymo priemone. Novatoriškos technologijos gali suteikti naujų priemonių, padėsiančių teisėsaugai ir kitiems saugumo srities subjektams. Dirbtinis intelektas ir didžiųjų duomenų analizė galėtų padėti pasinaudoti itin našios kompiuterijos teikiama nauda, kad būtų galima užtikrinti geresnį nustatymą ir greitai atlikti išsamią analizę[122]. Pagrindinė patikimų technologijų kūrimo prielaida yra aukštos kokybės duomenų rinkiniai, kuriais gali naudotis kompetentingos institucijos, kad parengtų, išbandytų ir patvirtintų algoritmus[123]. Apskritai šiandien technologinės priklausomybės rizika yra didelė, pavyzdžiui, ES yra grynoji kibernetinio saugumo produktų ir paslaugų importuotoja, o visa tai turi įtakos ekonomikai ir ypatingos svarbos infrastruktūros objektams. Kad įvaldytų technologijas ir užtikrintų tiekimo tęstinumą taip pat ir nepageidaujamų įvykių ar krizių atveju, Europa turi dalyvauti ir turėti pajėgumų svarbiausiose atitinkamų vertės grandinių dalyse.

Vykdydama **mokslinius tyrimus, inovacijas ir technologinę plėtrą** ES turi progą į saugumo aspektą atsižvelgti tuo metu, kai technologijos ir jų taikymas yra rengiami. Naujos kartos ES finansavimo pasiūlymai gali būti svarbi paskata[124]. Į saugumo aspektą nuo pat pradžių atsižvelgta iniciatyvose dėl Europos duomenų erdvių ir debesijos infrastruktūros. Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas[125] siekia sukurti veiksmingą ir rezultatyvią kibernetinio saugumo mokslinių tyrimų pajėgumų ir rezultatų telkimo ir dalijimosi jais struktūrą. Pagal ES kosmoso programą teikiamos paslaugos, kuriomis stiprinamas ES, jos valstybių narių ir asmenų saugumas[126].

Nuo 2007 m. pradėta daugiau kaip 600 projektų, kurių bendra vertė siekia beveik 3 mlrd. EUR, todėl ES finansuojami saugumo moksliniai tyrimai yra pagrindinė technologijų ir žinių skatinimo priemonė, kuria remiami saugumo sprendimai. Peržiūrėdama Europolo įgaliojimus, Komisija svarstys galimybę sukurti **Europos vidaus saugumo inovacijų centrą**[127], kuris ieškotų bendrų sprendimų, kuriais būtų atsižvelgiama į bendrus saugumo iššūkius ir galimybes, kuriomis valstybės narės vienos gali nesugebėti pasinaudoti. Bendradarbiavimas yra labai svarbus siekiant kuo veiksmingiau sutelkti investicijas ir plėtoti novatoriškas technologijas, kurios duotų tiek saugumo, tiek ekonominės naudos.

Įgūdžių ugdymas ir informuotumo didinimas

[122] Tai turėtų būti grindžiama Komisijos dirbtinio intelekto strategija.

[123] Europos duomenų strategija (COM(2020) 66 *final*).

[124] Visais Komisijos pasiūlymais dėl programos „Europos horizontas“, Vidaus saugumo fondo, Integruoto sienų valdymo fondo, programos „EUInvest“, Europos regioninės plėtros fondo ir Skaitmeninės Europos programos bus remiamas novatoriškų saugumo technologijų ir sprendimų kūrimas ir diegimas visoje saugumo vertės grandinėje.

[125] 2018 m. rugsėjo 12 d. pasiūlymas dėl reglamento, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras ir Nacionalinių koordinavimo centrų tinklas (COM(2018) 630).

[126] Pavyzdžiui, pagal programą „Copernicus“ teikiamos paslaugos, kuriomis sudaromos sąlygos stebėti ES išorės sienas ir vykdyti jūrų stebėjimą, o tai padeda kovoti su piratavimu ir neteisėtu žmonių gabenimu, taip pat remti ypatingos svarbos infrastruktūros objektus. Pradėjus veikti visu pajėgumu, tai bus pagrindinis civilinių ir karinių misijų ir operacijų veiksnys.

[127] Tai taip pat papildytų Europos sienų ir pakrančių apsaugos agentūros (FRONTEX), Europos policijos koledžo (CEPOL), „eu-LISA“ ir Jungtinių tyrimų centro veiklą.

Norint kurti atsparesnę visuomenę, kurioje įmonės, administracijos ir asmenys būtų geriau pasirengę, labai svarbu žinoti saugumo problemas ir įgyti kovoti su galimomis grėsmėmis reikalingų įgūdžių. Su IT infrastruktūra ir e. sistemomis susiję iššūkiai parodė, kad reikia gerinti mūsų kibernetinio saugumo parengties ir reagavimo srities žmogiškuosius pajėgumus. Pandemija taip pat išryškino skaitmeninimo svarbą visose ES ekonomikos ir visuomenės srityse.

Net **pagrindinės žinios apie grėsmes saugumui** ir apie tai, kaip su jomis kovoti, gali padaryti realų poveikį visuomenės atsparumui. Kibernetinių nusikaltimų rizikos ir poreikio apsisaugoti nuo jų suvokimas gali sustiprinti paslaugų teikėjų apsaugą kovojant su kibernetiniais išpuoliais. Informacija apie prekybos narkotikais pavojus ir riziką gali sutrukdyti nusikaltėliams įgyvendinti savo užmojus. ES gali skatinti geriausios patirties sklaidą, pavyzdžiui, per Saugesnio interneto centrų tinklą[128], ir užtikrinti, kad į tokius tikslus būtų atsižvelgta jos pačios programose.

Į būsimą Skaitmeninio švietimo veiksmų planą turėtų būti įtrauktos tikslinės priemonės, kuriomis būtų ugdomi visų gyventojų IT saugumo įgūdžiai. Neseniai priimta Įgūdžių darbotvarke[129] remiamas įgūdžių ugdymas visą gyvenimą. Ji apima tikslinius veiksmus, kuriais siekiama, kad mokslo, technologijų, inžinerijos, meno ir matematikos srities studijas baigtų daugiau absolventų, nes jų reikia pažangiausiose srityse, pavyzdžiui, kibernetinio saugumo srityje. Papildomi veiksmai, finansuojami pagal Skaitmeninės Europos programą, leis specialistams neatsilikti nuo grėsmių saugumui raidos ir kartu sumažinti šios srities specialistų trūkumą ES darbo rinkoje. Bendras poveikis bus tas, kad asmenys galės įgyti įgūdžių, kad galėtų kovoti su grėsmėmis saugumui, o įmonės – rasti reikiamų šios srities specialistų. Būsimoje Europos mokslinių tyrimų erdvėje ir Europos švietimo erdvėje taip pat bus skatinama karjera mokslo, technologijų, inžinerijos, meno ir matematikos srityse.

Taip pat svarbu, kad **nukentėjusieji** galėtų naudotis savo teisėmis; atsižvelgiant į konkrečias aplinkybes, jie turi gauti reikiamą pagalbą ir paramą. Ypatingų pastangų reikia mažumų ir pažeidžiamiausių asmenų grupėms priklausančių nukentėjusiųjų, pavyzdžiui, vaikų ar moterų, kuriais prekiaujama seksualinio išnaudojimo tikslais arba kurie patiria smurtą šeimoje, atžvilgiu[130].

Ypatingas vaidmuo tenka geresniems **teisėsaugos įgūdžiams**. Atsižvelgiant į dabartines ir naujas technologines grėsmes, reikia daugiau investuoti į teisėsaugos darbuotojų kvalifikacijos kėlimą ankstyviausiame etape ir per visą jų karjerą. CEPOL yra labai svarbus partneris, padedantis valstybėms narėms vykdyti šią užduotį. Teisėsaugos pareigūnų mokymas, susijęs su rasizmu ir ksenofobija bei apskritai su piliečių teisėmis, turi būti esminė ES saugumo kultūros dalis. Nacionalinės teisingumo sistemos ir teisingumo specialistai taip pat turi būti pasirengę prisitaikyti prie precedento neturinčių iššūkių ir į juos reaguoti. Mokymas yra labai svarbus, kad vietos valdžios institucijos galėtų naudotis šiomis priemonėmis susidarius operatyvinei padėčiai. Be to, turėtų būti dedamos visos pastangos stiprinti lyčių aspekto integravimą ir moterų dalyvavimo teisėsaugos veikloje didinimą.

[128] Žr. www.betterinternetforkids.eu. Centrinis portalas ir nacionaliniai saugesnio interneto centrai šiuo metu finansuojami pagal EITP telekomunikacijų paprogramę, o būsimas finansavimas pasiūlytas pagal Skaitmeninės Europos programą.

[129] Europos įgūdžių darbotvarkė, kuria siekiama tvaraus konkurencingumo, socialinio sąžiningumo ir atsparumo (COM(2020) 274 *final*).

[130] Žr. Lyčių lygybės strategiją (COM(2020) 152); Strategiją dėl nusikaltimų aukų teisių (COM(2020) 258) ir Europos strategiją dėl vaikams geresnio interneto (COM(2012) 196).

Pagrindiniai veiksmai
• Stiprinti Europolo įgaliojimus • Apsvarstyti galimybę priimti ES policijos bendradarbiavimo kodeksą ir ištirti policijos veiklos koordinavimo per krizę galimybę • Stiprinti Eurojustą, siekiant susieti teismines ir teisėsaugos institucijas • Atlikti Išankstinės informacijos apie keleivius direktyvos peržiūrą • Priimti komunikatą dėl keleivio duomenų įrašų išorės aspekto • Stiprinti ES ir Interpolo bendradarbiavimą • Parengti derybų su pagrindinėmis trečiosiomis šalimis dėl keitimosi informacija programą • Įgyvendinti geresnius kelionės dokumentų saugumo standartus • Ištirti Europos vidaus saugumo inovacijų centro galimybes

V. Išvados

Vis neramesniame pasaulyje Europos Sąjunga tebėra plačiai laikoma viena saugiausių ir geriausiai apsaugotų vietų. Tačiau tai negali būti laikoma savaime suprantamu dalyku.

Naujoji saugumo sąjungos strategija yra saugumo ekosistemos, kuri apima visą Europos visuomenę, pagrindas. Ji grindžiama žinojimu, kad saugumas yra bendra atsakomybė. Saugumas yra visiems aktualus klausimas. Visos valdžios įstaigos, verslo įmonės, socialinės organizacijos, institucijos ir piliečiai turi vykdyti jiems tenkančias pareigas, kad mūsų visuomenė taptų saugesnė.

Dabar saugumo klausimus reikia vertinti iš daug platesnės perspektyvos nei anksčiau. Reikia atsisakyti klaidingo skirstymo į fizinį ir skaitmeninį turinį. ES saugumo sąjungos strategija sujungia visus saugumo poreikius ir joje daugiausia dėmesio skiriama sritims, kurios artimiausiais metais bus svarbiausios ES saugumui. Joje taip pat pripažįstama, kad grėsmės saugumui nepaiso geografinių sienų, taip pat tai, kad didėja vidaus ir išorės saugumo tarpusavio ryšys.[131]. Todėl įgyvendinant šią strategiją bus svarbu, kad ES bendradarbiautų su tarptautiniais partneriais siekdama apsaugoti visus ES piliečius ir kad toliau glaudžiai koordinuotų savo veiksmus su ES išorės veiksmais.

Mūsų saugumas susijęs su mūsų pagrindinėmis vertybėmis. Visais šioje strategijoje siūlomais veiksmais ir iniciatyvomis bus visapusiškai paisoma pagrindinių teisių ir puoselėjamos mūsų Europos vertybės. Jomis yra grindžiama mūsų europinė gyvensena ir jos turi likti visos mūsų veiklos pagrindas.

Galiausiai Komisija puikiai suvokia, kad bet kokia politika ar veiksmai yra naudingi tik tiek, kiek jie yra įgyvendinami. Todėl reikia nuolat pabrėžti, kad reikia tinkamai įgyvendinti esamus ir būsimus teisės aktus ir užtikrinti jų vykdymą. Tai bus stebima reguliariai teikiant saugumo sąjungos ataskaitas, o Komisija išsamiai informuos Europos Parlamentą, Tarybą ir suinteresuotuosius subjektus ir juos įtrauks į visus atitinkamus veiksmus. Be to, Komisija yra pasirengusi dalyvauti bendrose diskusijose su institucijomis dėl saugumo sąjungos strategijos ir jas rengti, kad kartu įvertintų padarytą pažangą ir išnagrinėtus būsimus iššūkius.

[131] Žr. Visuotinę ES strategiją.

Komisija ragina Europos Parlamentą ir Tarybą patvirtinti šią saugumo sąjungos strategiją kaip bendradarbiavimo ir bendrų veiksmų saugumo srityje pagrindą ateinantiems penkeriems metams.