Europos Sąjungos Taryba

Briuselis, 2025 m. balandžio 3 d.
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2025 m. balandžio 2 d.
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	COM(2025) 148 final
Dalykas:	KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI, TARYBAI, EUROPOS EKONOMIKOS IR SOCIALINIŲ REIKALŲ KOMITETUI IR REGIONŲ KOMITETUI „ProtectEU“ – Europos vidaus saugumo strategija

Delegacijoms pridedamas dokumentas COM(2025) 148 final.

Pridedama: COM(2025) 148 final

EUROPOS
KOMISIJA

Strasbūras, 2025 04 01
COM(2025) 148 final

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

„ProtectEU“ – Europos vidaus saugumo strategija

1. „ProtectEU“ – Europos vidaus saugumo strategija

Saugumas yra visų mūsų laisvių pagrindas. Demokratija, teisinė valstybė, pagrindinės teisės, europiečių gerovė, konkurencingumas ir klestėjimas – visa tai priklauso nuo mūsų gebėjimo suteikti pagrindinę saugumo garantiją. Naujajame grėsmių saugumui amžiuje, kuriame dabar gyvename, ES valstybių narių gebėjimas užtikrinti savo piliečių saugumą labiau nei bet kada priklauso **nuo bendro europinio požiūrio į mūsų vidaus saugumo apsaugą**. Kintančioje geopolitinėje aplinkoje Europa turi ir toliau tesėti ilgalaikį taikos pažadą.

Jau imtasi pirmųjų žingsnių kuriant Europos saugumo aparatą. Per pastarąjį dešimtmetį apginklavome Sąjungą geresniais kolektyviniais veiksmų mechanizmais teisėsaugos ir teisminio bendradarbiavimo, sienų saugumo, kovos su sunkių formų ir organizuotu nusikalstamumu, kovos su terorizmu ir smurtiniu ekstremizmu ir ES ypatingos svarbos fizinės ir skaitmeninės infrastruktūros apsaugos srityse. Tebėra labai svarbu tinkamai įgyvendinti anksčiau priimtus teisės aktus ir parengtą politiką.

Dėl šiandienos grėsmių pobūdžio ir esminio ES vidaus ir išorės saugumo ryšio turime dėti daugiau pastangų.

Grėsmės yra rimtos. Nebeaiški **hibridinių grėsmių** ir atviro karo perskyra. Rusija internete ir realiame gyvenime vykdo hibridinę kampaniją prieš ES ir jos partnerius, siekdama sutrikdyti visuomenės sanglaudą ir demokratinius procesus bei jiems pakenkti ir išbandyti ES solidarumą su Ukraina. Priešiškos užsienio valstybės ir valstybių remiami subjektai siekia įsiskverbti į mūsų ypatingos svarbos infrastruktūrą ir tiekimo grandines ir jas sutrikdyti, neteisėtai pasisavinti neskelbtinus duomenis ir įsitvirtinti, kad ateityje galėtų vykdyti kuo didesnio masto trikdymo veiklą. Jie nusikaltimus naudoja kaip paslaugą, o nusikaltėlius – kaip įgaliotinius. Be to, dėl savo priklausomybės nuo trečiųjų valstybių tiekimo grandinių esame labiau pažeidžiami priešiškų valstybių prieš mus vykdomoms hibridinėms kampanijoms.

Kaip pabrėžta neseniai Europolo pateiktame ES sunkių formų ir organizuoto nusikalstamumo grėsmių vertinime (SOCTA)[1], Europoje plinta galingi **organizuoti nusikaltėlių tinklai**, kurie veikia internete, įsilieja į mūsų ekonomiką ir kenkia mūsų visuomenei. Kai organizuotas nusikalstamumas įsitvirtina bendruomenėje ar ekonomikos sektoriuje, jį panaikinti yra labai sunku: trečdalis didžiausią grėsmę keliančių nusikaltėlių tinklų veikia daugiau kaip dešimt metų. Kriptovaliutos ir lygiagrečios finansų sistemos padeda jiems plauti ir slėpti nusikalstamu būdu įgytas pajamas.

Terorizmo grėsmės lygis Europoje ir toliau smarkiai didėja. Regioninės krizės už ES ribų daro didelį poveikį ir suteikia naujų motyvų viso ideologinio spektro teroristiniams subjektams verbuoti, sutelkti ar stiprinti savo pajėgumus. Radikalizacijos skatinimo ir verbavimo pastangas jie nukreipia konkrečiai į pažeidžiamiausias mūsų visuomenės grupes, visų pirma į kai kuriuos jaunuolius. Jie skatina pavienių veikėjų išpuolius ir prieš sistemą nukreipto ekstremizmo augimą, kurio tikslas – sužlugdyti demokratinę teisinę tvarką.

Neįtikėtinai sparti **technologinė pažanga** yra labai svarbi mūsų saugumo aparato tobulinimo priemonė. Vis dėlto kibernetinių išpuolių ir užsienio vykdomo manipuliavimo informacija atvejų vis daugėja ir šie veiksmai vykdomi naudojant naujas technologijas, pavyzdžiui, dirbtinį intelektą. Ypač didelis pavojus internete kyla vaikams, jaunimui ir vyresnio amžiaus žmonėms, o neapykantos sklaida internete kelia grėsmę saviraiškos laisvei ir socialinei sanglaudai.

Mūsų gyvenimas tapo ne toks saugus ir tai vis labiau jaučia europiečiai, kurių **saugos ir saugumo suvokimas ES** susilpnėjo tiek, kad, paklausus apie ateitį, 64 proc. jų nurodė, jog yra

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

linkę nerimauti dėl ES saugumo[2]. Vis didesnį nerimą jaučia ir įmonės; klaidinga informacija ir dezinformacija, nusikalstamumas ir neteisėta veikla bei kibernetinis šnipinėjimas yra vieni iš dešimties didžiausių rizikos veiksnių, nustatytų Pasaulio ekonomikos forumo 2025 m. pranešime dėl visuotinių grėsmių[3].

Europiečiai turėtų **galėti gyventi nepatirdami baimės**, kad ir kur jie būtų – gatvėje, namuose, viešosiose erdvėse, metro ar internete. Žmonių, ypač asmenų, kurie yra pažeidžiamiausi dėl išpuolių, paprastai darančių neproporcingą poveikį vaikams, moterims ir mažumoms, įskaitant žydų ir musulmonų bendruomenes, apsauga yra ES veiklos saugumo srityje pagrindas. Tai labai svarbu siekiant sukurti atsparią ir darnią visuomenę.

Komisija pristato **Europos vidaus saugumo strategiją**, kuria siekiama ateityje geriau kovoti su grėsmėmis. Naudodami griežtesnių teisinių priemonių rinkinį, glaudžiau bendradarbiaudami ir aktyviau dalydamiesi informacija didinsime savo atsparumą ir kolektyvinį gebėjimą numatyti grėsmes saugumui, užkirsti joms kelią, jas nustatyti ir veiksmingai į jas reaguoti. Vadovaujantis bendru požiūriu į vidaus saugumą galima padėti valstybėms narėms išnaudoti technologijų galią siekiant sustiprinti, o ne susilpninti saugumą, kartu skatinant saugią skaitmeninę erdvę visiems. Be to, juo remiamas bendras valstybių narių atsakas į pasaulinius politinius ir ekonominius pokyčius, darančius poveikį Sąjungos vidaus saugumui.

Šioje strategijoje vadovaujamasi **trimis principais**, o jos pagrindas – pagarba teisinei valstybei ir pagrindinėms teisėms.

Pirma, ja užsibrėžiamas siekis keisti kultūrą saugumo srityje. Mums reikia **visos visuomenės požiūrio**, aprėpiančio visus piliečius ir suinteresuotuosius subjektus, įskaitant pilietinę visuomenę, mokslinių tyrimų įstaigas, akademinę bendruomenę ir privačius subjektus. Todėl įgyvendinant strategijoje numatytus veiksmus, kai įmanoma, bus laikomasi integruoto požiūrio, apimančio įvairius suinteresuotuosius subjektus.

Antra, **saugumo aspektai turi būti įtraukti ir integruoti į visus ES teisės aktus, politiką ir programas**, įskaitant ES išorės veiksmus. Teisės aktai, politika ir programos turės būti rengiami, peržiūrimi ir įgyvendinami atsižvelgiant į saugumo perspektyvą, užtikrinant, kad būtų atsižvelgta į būtinus saugumo aspektus, kad būtų skatinamas nuoseklus ir visapusiškas požiūris į saugumą.

Galiausiai, kad Europa būtų saugi, patikima ir atspari, reikia **didelių ES, jos valstybių narių ir privačiojo sektoriaus investicijų**. Šioje strategijoje išdėstytiems prioritetams ir veiksmams įgyvendinti reikia pakankamai žmogiškųjų ir finansinių išteklių, kad būtų užtikrintas jų įgyvendinimas. Kaip nustatyta komunikate „Rengiantis kitai daugiametei finansinei programai“[4], Europa turės didinti viešąsias išlaidas saugumui ir skatinti saugumo srities mokslinius tyrimus ir investicijas, didindama savo strateginį savarankiškumą.

Ši strategija papildo **ES pasirengimo krizėms strategiją**[5], kurioje išdėstytas integruotas visus pavojus apimantis požiūris į pasirengimą konfliktams, žmogaus sukeltoms ir gaivalinėms nelaimėms ir krizėms, ir **Baltąją knygą dėl Europos gynybos ateities**[6], kuria remiamas gynybos pajėgumų plėtojimas ir įgijimas visoje ES, siekiant atgrasyti užsienio priešininkus. Komisija taip pat pasiūlys **Europos demokratijos skydą** demokratiniam atsparumui ES stiprinti. Šiomis iniciatyvomis kartu nustatoma saugios, patikimos ir atsparios ES vizija.

[2] Greitoji „Eurobarometro“ apklausa FL550: ES uždaviniai ir prioritetai.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, p. 17.
[4] COM(2025) 46 *final*.
[5] JOIN(2025) 130 *final*.
[6] JOIN(2025) 120 *final*.

Naujas Europos vidaus saugumo valdymas

Komisija glaudžiai bendradarbiaus su valstybėmis narėmis ir ES agentūromis, kad patobulintų ES požiūrį į vidaus saugumą tiek strateginiu, tiek operatyviniu lygmenimis.

Tai bus daroma:

- **nuo pat pradžių ir viso derybų proceso laikotarpiu nuosekliai nustatant galimą naujų ir peržiūrėtų Komisijos iniciatyvų poveikį saugumui ir parengčiai;**
- **reguliariai rengiant Komisijos Europos vidaus saugumo projekto grupės posėdžius, remiantis visoje Komisijoje vykdomu strateginiu tarpsektoriniu bendradarbiavimu;**
- **pristatant su vidaus saugumu susijusių grėsmių analizes Saugumo koledžo darbui remti;**
- **Taryboje rengiant su valstybėmis narėmis diskusijas dėl kintančių vidaus saugumo iššūkių, grindžiamas grėsmių analize, ir keičiantis informacija apie pagrindinius politikos prioritetus;**
- **reguliariai teikiant ataskaitas Europos Parlamentui ir Tarybai, siekiant stebėti ir remti sistemingą pagrindinių saugumo iniciatyvų įgyvendinimą.**

2. Integruotas informuotumas apie padėtį ir grėsmių analizė

Pateiksime ES naujų būdų dalytis informacija ir ją derinti, taip pat reguliarią ES vidaus saugumo grėsmių analizę, taip prisidėdami prie išsamaus rizikos ir grėsmių vertinimo.

Saugumas prasideda nuo **veiksmingo numatymo**. ES turi remtis išsamiu, pakankamai savarankišku ir naujausia informacija grindžiamu informuotumu apie padėtį ir grėsmių analize. Gynybinė žvalgyba, kurią valstybės narės raginamos toliau stiprinti pasitelkiant Bendrą žvalgybinės informacijos analizės centrą (SIAC), kuris yra vienas bendras valstybių narių žvalgybos informacijos centras, yra labai svarbi vertinant grėsmes ir kovojant su jomis bei galiausiai pagrindžiant politikos ir teisėkūros veiksmus[7]. Turime veiksmingiau ir daugiau bendradarbiaudami naudoti **žvalgybos informacija grindžiamą analizę** ir **grėsmių vertinimus** ES lygmeniu.

Remdamasi įvairiais ES lygmeniu ir konkretiems sektoriams parengtais rizikos ir grėsmių vertinimais[8], Komisija **reguliariai** rengs **grėsmių ES vidaus saugumui analizes**, kad nustatytų pagrindinius saugumo iššūkius ir būtų galima pagrįsti politikos prioritetus. Šios analizės padės plėtoti lanksčią ir reaktyvią saugumo politiką, kuria veiksmingai kovojama su kintančiomis grėsmėmis, žmonės ir įmonės geriau apsaugomi nuo išpuolių ir sudaromos sąlygos laiku imtis tikslinių politikos intervencinių priemonių. Šiomis ES grėsmių vidaus saugumui analizėmis taip pat bus prisidedama prie **ES išsamaus (tarpsektorinio, visus pavojus apimančio) rizikos ir grėsmių vertinimo** – jį rengs Komisija ir vyriausiasis įgaliotinis, kaip nustatyta ES pasirengimo krizės strategijoje.

Dalijantis informacija labai svarbus pasitikėjimas ir saugus tvarkymas, todėl tam reikia patikimos ir saugios infrastruktūros. ES institucijos, įstaigos ir agentūros turi užtikrinti savo

[7] *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness* („Saugiau kartu. Europos civilinio ir karinio pasirengimo ir parengties stiprinimas“), p. 23.

[8] Sektorių grėsmių vertinimai, kuriais numatyta remtis atliekant šią grėsmių analizę, apima ES sunkių formų ir organizuoto nusikalstamumo grėsmių vertinimą (SOCTA), ES ataskaitą dėl terorizmo padėties ir tendencijų (TE-SAT ataskaita), bendrą kibernetinio vertinimo ataskaitą (JCAR) ir būsimus pinigų plovimo ir teroristų finansavimo grėsmių, rizikos ir metodų vertinimus, kuriuos turi atlikti Komisija ir Kovos su pinigų plovimu institucija.

gebėjimą naudotis **saugiais ryšių kanalais**, kuriais tarpusavyje ir su valstybėmis narėmis keistųsi neskelbtina ir įslaptinta informacija. Investuojant į **sąveikias saugias sistemas** ir patikimas technologijas bus sustiprintas ES savarankiškumas ir gebėjimas valdyti krizes bei užtikrinti veiklos atsparumą. Atsižvelgdama į tai, Komisija primygtinai ragina teisėkūros institucijas užbaigti derybas dėl **siūlomo reglamento dėl informacijos saugumo Sąjungos institucijose, įstaigose, organuose ir agentūrose**, visų pirma siekiant užtikrinti, kad būtų sukurta bendra neskelbtinos neįslaptintos ir įslaptintos informacijos tvarkymo sistema[9].

Siekdama užtikrinti savo veiklos saugumą ir informuotumą apie padėtį, Komisija peržiūrės savo organizacijos saugumo valdymo sistemą ir įsteigs **integruotą saugumo operacijų centrą (ISOC)**, kad būtų apsaugoti visose Komisijos vietose esantys žmonės ir materialusis turtas ir jose vykdoma veikla. Komisija taip pat didins savo operatyvinius ir analitinius gebėjimus nustatyti ir švelninti hibridines grėsmes.

Laikantis ES pasirengimo krizėms strategijos, pasirengimo ir saugumo aspektai bus įtraukti ir integruoti į ES teisės aktus, politiką ir programas. Rengdama arba peržiūrėdama teisės aktus, politiką ar programas Komisija atsižvelgs į pasirengimo ir saugumo perspektyvą ir nuosekliai nustatys galimą tinkamiausios politikos galimybės poveikį pasirengimui ir saugumui. Be to, bus rengiami reguliarūs Komisijos politikos formuotojų mokymai.

Siekdama padėti valstybėms narėms, Komisija aptars kintančius vidaus saugumo iššūkius ir pagrindinius politikos prioritetus su Taryba ir reguliariai informuos ją apie strategijos įgyvendinimą. Be to, Komisija informuos Europos Parlamentą ir atitinkamus suinteresuotuosius subjektus ir įtrauks juos į visus atitinkamus veiksmus.

Pagrindiniai veiksmai

Komisija:

- **reguliariai rengs ir teiks grėsmių ES vidaus saugumui analizes.**

Valstybės narės primygtinai raginamos:

- **stiprinti dalijimąsi žvalgybos informacija su SIAC ir užtikrinti geresnį dalijimąsi informacija su ES agentūromis ir įstaigomis.**

Europos Parlamentas ir Taryba raginami:

- **užbaigti derybas dėl siūlomo reglamento dėl informacijos saugumo Sąjungos institucijose, įstaigose, organuose ir agentūrose.**

3. Sustiprinti ES saugumo pajėgumai

Parengsime naujas teisėsaugos priemones, pavyzdžiui, pertvarkytą Europolą, ir geresnius būdus koordinuoti ir užtikrinti saugų keitimąsi duomenimis ir teisėtą prieigą prie duomenų.

Kad galėtų veiksmingai kovoti su kintančiomis grėsmėmis, ES turi stiprinti savo saugumo pajėgumus ir skatinti inovacijas. Greitam ir veiksmingam teisėsaugos ir teisminių institucijų, kurios yra pagrindiniai subjektai kovojant su grėsmėmis vidaus saugumui, veikimui reikia tinkamų operatyvinių priemonių ir pajėgumų. Svarbu, kad šios institucijos galėtų palaikyti ryšius ir koordinuoti veiksmus tarpvalstybiniu ir tarpžinybiniu mastu, veiksmingai užkirsti kelią nusikaltimams, juos nustatyti, tirti ir vykdyti baudžiamąjį persekiojimą už juos.

[9] COM(2022) 119 *final*.

ES vidaus saugumo agentūros ir įstaigos

ES teisingumo, vidaus reikalų ir kibernetinio saugumo agentūros ir įstaigos atlieka ES saugumo struktūroje svarbų vaidmenį, kuris, plečiantis jų atsakomybės sritims, toliau didėja.

Šiandien, praėjus 25 metams nuo **Europolo** įsteigimo, jis yra kaip niekada svarbus ES saugumo sistemai. Europolas padeda atlikti sudėtingus tarpvalstybinius tyrimus, sudaro palankesnes sąlygas keistis informacija, kuria novatoriškas viešosios tvarkos palaikymo priemones ir teikia pažangių ekspertinių žinių teisėsaugos institucijoms. Vis dėlto yra keletas veiksnių, trukdančių Europolui visapusiškai išnaudoti savo operatyvinį potencialą remiant tiriamąją ir operatyvinę veiklą, kuria siekiama kovoti su tarpvalstybiniu nusikalstamumu: jie įvairūs – nuo nepakankamų išteklių iki to, kad dabartiniai jo įgaliojimai neapima naujų grėsmių saugumui, pavyzdžiui, sabotažo, hibridinių grėsmių ar manipuliavimo informacija. Todėl Komisija pasiūlys atlikti **plataus užmojo užduotį – iš esmės persvarstyti Europolo įgaliojimus**, kad jis taptų tikrai gerai veikiančia policijos agentūra, geriau remiančia valstybes nares. Tuo siekiama sustiprinti Europolo technologinę kompetenciją ir pajėgumą remti nacionalines teisėsaugos agentūras, gerinti koordinavimą su kitomis agentūromis ir įstaigomis bei valstybėmis narėmis, stiprinti strateginę partnerystę su šalimis partnerėmis ir privačiuoju sektoriumi ir užtikrinti griežtesnę Europolo priežiūrą.

Be to, Komisija sieks **toliau didinti ES vidaus saugumo agentūrų ir įstaigų veiksmingumą ir papildomumą ir stiprinti sklandų** jų tarpusavio **bendradarbiavimą**.

Bus įvertinti ir sustiprinti **Eurojusto** įgaliojimai, siekiant užtikrinti veiksmingą teisminį bendradarbiavimą, sustiprinti papildomumą ir bendradarbiavimą su Europolu. Be kita ko, bus siekiama padidinti Eurojusto veiksmingumą ir pajėgumą aktyviai teikti paramą ir analizę valstybių narių teisminėms institucijoms. Be to, atsižvelgdama į išskirtinę **Europos prokuratūros** kompetenciją tirti Sąjungos finansiniams interesams kenkiančius nusikaltimus ir vykdyti baudžiamąjį persekiojimą už juos, Komisija apsvarstys, kaip geriausiai padidinti Europos prokuratūros pajėgumą apsaugoti Sąjungos lėšas. Tuo tikslu, be kita ko, bus sustiprintas Europos prokuratūros ir Europolo bendradarbiavimas.

Bendradarbiaujant labai svarbu, kad **agentūros veiksmingai ir saugiai tarpusavyje keistųsi informacija**. Europolui ir FRONTEX reikia greitai tarpusavyje keistis informacija, be kita ko, operatyviniais tikslais, atsižvelgiant į 2024 m. sausio mėn. bendrą pareiškimą[10]. **eu-LISA** atlieka labai svarbų vaidmenį užtikrinant saugų duomenų saugojimą ir prieinamumą, kad agentūros galėtų geriau tarpusavyje koordinuoti veiklą ir veiksmingiau keistis informacija. **ES pagrindinių teisių agentūra** teikia ekspertines žinias apie pagrindinių teisių apsaugą rengiant ir įgyvendinant saugumo politiką.

ES kovos su pinigų plovimu institucijai (AMLA) suteikti įgaliojimai remiantis principu „yra atitiktis / nėra atitikties“ sutikrinti duomenis su Europolo, Europos prokuratūros, Eurojusto ir ES kovos su sukčiavimu tarnybos pateikta informacija, kad būtų galima rengti bendras tarpvalstybinių bylų analizes.

ENISA atlieka labai svarbų vaidmenį įgyvendinant Europos kibernetinio saugumo teisės aktus. Per būsimą **Kibernetinio saugumo akto peržiūrą** Komisija įvertins šios agentūros įgaliojimus ir pasiūlys ją modernizuoti siekiant padidinti jos teikiamą ES pridėtinę vertę.

Priėmus pasiūlymą pagal ES muitinės reformos dokumentų rinkinį sukurti **ES muitinę** ir **ES muitinės duomenų platformą**, bus sustiprintas muitinių ir kitų teisėsaugos institucijų tarpusavio bendradarbiavimas. Būsimos platformos informacija ir duomenys, kuriuos teikia Europolas,

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf

Eurojustas, Europos prokuratūra, OLAF, AMLA ir FRONTEX, atsižvelgiant į jų atitinkamą kompetenciją, padės pagerinti bendrą analizę ir prisidės prie nuoseklesnės operatyvinės veiklos, visų pirma prie išorės sienų. Komisija ragina teisėkūros institucijas greitai užbaigti derybas dėl ES muitų reformos ir toliau padės joms šiuo tikslu.

Europos prokuratūros, OLAF, Europolo, Eurojusto, AMLA ir siūlomos ES muitinės papildomumo didinimas taip pat bus grindžiamas vykdomos **ES kovos su sukčiavimu struktūros** peržiūros rezultatais. Gali būti naudinga taikyti šį holistinį požiūrį saugumo srityje, daugiausia dėmesio skiriant tinkamesniam baudžiamųjų ir administracinių priemonių naudojimui, IT sistemų sąveikumui ir geresniam bendradarbiavimui.

Ypatingos svarbos ryšių sistema

Šiuo metu **ypatingos svarbos ryšių sistemos**[11] dažniausiai nacionaliniu lygmeniu veikia savarankiškai. Tai reiškia, kad pirmieji reaguotojai dažnai negali komunikuoti su kolegomis, kai kerta sieną vykdami į kitas valstybes nares. Kai kuriose valstybėse narėse taip pat yra apribojimų, susijusių su įvairių rūšių pirmųjų reaguotojų (pvz., policijos ir greitosios pagalbos automobilių) tarpusavio komunikacija. Daugumos sistemų standartai neatitinka šiandienos reikalavimų dėl funkcionalumo ir atsparumo, o tai labai riboja pirmųjų reaguotojų reagavimo pajėgumus, ypač tarpvalstybiniu mastu.

Kad padidintų ES pajėgumą reaguoti į krizes, Komisija pasiūlys teisės aktą, kuriuo siekiama sukurti **Europos ypatingos svarbos ryšių sistemą**, sujungiančią valstybių narių naujos kartos ypatingos svarbos ryšių sistemas ES. Siekiama, kad Europos ypatingos svarbos ryšių sistema būtų grindžiama trimis strateginiais ramsčiais: operatyviniu judumu, dideliu atsparumu ir strateginiu savarankiškumu. Europos ypatingos svarbos ryšių sistemos iniciatyva bus nustatyti suderinti reikalavimai ir ji padės modernizuoti valstybių narių ypatingos svarbos ryšių sistemas, kad jos galėtų sklandžiai veikti. Be to, taikant būsimą IRIS^{212} daugiaorbitinę sistemą, bus išplėsta sistemos aprėptis. ES finansuojamais projektais bus stiprinami Europos ypatingos svarbos ryšių sistemos techniniai pajėgumai, visų pirma pasitelkiant Europos technologijų teikėjus, kad būtų skatinamas ES strateginis savarankiškumas šiame jautriame sektoriuje.

Teisėta prieiga prie duomenų

Teisėsaugos ir teisminės institucijos turi turėti galimybę tirti nusikaltimus ir imtis kovos su jais veiksmų. Šiandien beveik visų formų sunkūs ir organizuoti nusikaltimai turi skaitmeninį pėdsaką[13]. Šiuo metu maždaug 85 proc. nusikalstamų veikų tyrimų priklauso nuo teisėsaugos institucijų gebėjimo gauti skaitmeninę informaciją[14].

Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio grupė savo baigiamojoje ataskaitoje[15] pabrėžė, kad pastarąjį dešimtmetį teisėsaugos ir teisminės institucijos atsilieka nuo nusikaltėlių, nes nusikaltėliai naudojasi kitų jurisdikcijų priemonėmis ir produktais, teikiamais paslaugų teikėjų, įdiegusių priemones, kuriomis iš jų atimama galimybė bendradarbiauti nagrinėjant teisėtus prašymus atskirose baudžiamosiose bylose. Todėl sistemingas teisėsaugos institucijų ir privačių šalių, įskaitant paslaugų teikėjus,

[11] Tai yra tinklai, kuriais naudojasi teisėsaugos institucijos, sienos apsaugos pareigūnai, muitinės, civilinės saugos tarnybos, ugniagesiai, greitosios medicinos pagalbos teikėjai ir kiti svarbūs subjektai visuomenės saugumo ir saugos srityje.

[12] ES atsparumo, junglumo ir saugumo naudojant palydovus infrastruktūra.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

[14] https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52019PC0070.

[15] Prieigos prie duomenų veiksmingos teisėsaugos tikslais aukšto lygio grupės baigiamoji ataskaita, 2024 11 15, 4802e306-c364-4154-835b-e986a9a49281_en.

bendradarbiavimas yra labai svarbus, stengiantis ateityje sutrikdyti didžiausią grėsmę keliančių nusikaltėlių tinklų ir asmenų veiklą Sąjungoje ir už jos ribų.

Kadangi skaitmenizacija plinta vis plačiau ir tampa vis didesniu naujų priemonių šaltiniu nusikaltėliams, labai svarbu sukurti prieigos prie duomenų sistemą, kuri atitiktų poreikius užtikrinti mūsų teisės aktų vykdymą ir apsaugoti mūsų vertybes. Be to, siekiant išsaugoti kibernetinį saugumą ir apsisaugoti nuo naujų grėsmių saugumui, taip pat labai svarbu užtikrinti, kad skaitmeninės sistemos išliktų apsaugotos nuo neteisėtos prieigos. Taikant tokias prieigos sistemas taip pat turi būti gerbiamos pagrindinės teisės, užtikrinant, *inter alia*, tinkamą privatumo ir asmens duomenų apsaugą.

Pastaraisiais metais ES, priimdama elektroninių įrodymų taisykles, visapusiškai taikysimas nuo 2026 m. rugpjūčio mėn.[16], ėmėsi veiksmų, kuriais siekiama tiek kovoti su **nusikalstamumu internete,** tiek **palengvinti prieigą prie skaitmeninių įrodymų, susijusių su visais nusikaltimais**. Jas papildys tarptautinės keitimosi informacija ir įrodymais priemonės. Komisija netrukus pasiūlys pasirašyti ir sudaryti naują **JT konvenciją dėl kovos su elektroniniais nusikaltimais**.

Atsižvelgdama į aukšto lygio grupės rekomendacijas[17], Komisija 2025 m. pirmąjį pusmetį pateiks **veiksmų gaires, kuriose išdėstomos jos siūlomos teisinės ir praktinės priemonės teisėtai ir veiksmingai prieigai prie duomenų užtikrinti**. Vykdydama tolesnę veiklą, susijusią su šiomis veiksmų gairėmis, Komisija pirmenybę teiks **duomenų saugojimo taisyklių** poveikio ES lygmeniu vertinimui ir **Šifravimo technologijų veiksmų gairių** rengimui, kad būtų nustatyti ir įvertinti technologiniai sprendimai, kurie sudarytų sąlygas teisėsaugos institucijoms teisėtai gauti užšifruotus duomenis, užtikrinant kibernetinį saugumą ir pagrindines teises.

Operatyvinis bendradarbiavimas

Komisija bendradarbiaus su valstybėmis narėmis, ES agentūromis ir įstaigomis bei šalimis partnerėmis, kad sustiprintų operatyvinį bendradarbiavimą, kuris yra labai svarbus siekiant nustatyti veiksmingesnį požiūrį į kovą su tarptautiniu organizuotu nusikalstamumu ir terorizmu.

Europos kovos su nusikalstamumo grėsmėmis daugiadalykė platforma (EMPACT), pagrindinė ES bendrų kovos su sunkių formų ir organizuotu nusikalstamumu veiksmų sistema, pasiekė svarbių veiklos rezultatų. Kitas 2026–2029 m. EMPACT ciklas suteikia galimybę dar labiau sustiprinti šią sistemą. Kad galėtų sutrikdyti didžiausią grėsmę keliančių nusikaltėlių tinklų ir asmenų veiklą, Sąjunga turi racionalizuoti savo pastangas, naudoti jas neatidėliotinai spręsdama prioritetinius klausimus, stiprinti valstybių narių įsipareigojimus ir užtikrinti veiksmingą išteklių naudojimą.

Tuo tikslu Komisija bendradarbiaus su Tarybai pirmininkaujančiomis valstybėmis narėmis ir valstybėmis narėmis, kad **kuo labiau padidintų EMPACT potencialą ir įgyvendintų pagrindinius kito 2026–2029 m. EMPACT ciklo prioritetus**. Šiose prioritetinėse srityse reikia žvalgybos informacijos apie didžiausią grėsmę keliančius nusikaltėlių tinklus, bendrų tyrimų ir operatyvinių darbo grupių bei tvirto teisminio atsako, įskaitant lėšų sekimo metodą. Be to, Sąjunga turi kovoti su nusikaltėlių verbavimu ir įsiskverbimu ir stiprinti tarpžinybinį ir tarptautinį teisėsaugos bendradarbiavimą ir mokymą.

[16] 2023 m. liepos 12 d. Europos Parlamento ir Tarybos reglamentas (ES) 2023/1543 dėl Europos įrodymų pateikimo orderių ir Europos įrodymų saugojimo orderių elektroniniams įrodymams baudžiamajame procese ir laisvės atėmimo bausmių vykdymui pasibaigus baudžiamajam procesui, OL L 191, 2023 7 28.

[17] Tarybos išvados dėl prieigos prie duomenų veiksmingos teisėsaugos tikslais (2024 m. gruodžio 12 d.) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/lt/pdf.

Komisija taip pat rems kitų formų **tarpvalstybinį operatyvinį valstybių narių ir Šengeno asocijuotųjų šalių bendradarbiavimą teisėsaugos srityje**. Šengeno erdvėje, kurioje nėra vidaus sienų kontrolės, reikia glaudaus valstybių narių teisėsaugos institucijų bendradarbiavimo ir keitimosi informacija, kad būtų užtikrintas aukštas vidaus saugumo lygis. Šiandien teisėsaugos pareigūnams vis dar kyla sunkumų vykdant skubius intervencinius veiksmus tarpvalstybiniu mastu[18], o kovojant su hibridinėmis grėsmėmis taip pat reikalingas tvirtesnis tarpvalstybinis bendradarbiavimas. Turėtų būti sukurta **operatyvinio teisėsaugos bendradarbiavimo ateities aukšto lygio grupė**, kuri parengtų bendrą strateginę viziją.

Veiksmingam tarpvalstybiniam bendradarbiavimui taip pat labai svarbu, kad teisėsaugos institucijos veiksmingai keistųsi duomenimis. Sukūrus **sąveikumo architektūrą**, teisėsaugos institucijoms ir Europolui bus suteikta veiksminga prieiga prie labai svarbios informacijos. Be to, ES ir jos valstybės narės, bendradarbiaudamos su eu-LISA ir Europolu, turėtų teikti pirmenybę dvišaliam ir daugiašaliam keitimuisi informacija, teisiniu ir techniniu požiūriais įgyvendindamos **reglamentą „Priumas II“**[19]. Taip bus sudarytos sąlygos saugiai automatizuotai keistis pirštų atspaudais, DNR analitėmis, transporto priemonių registracijos duomenimis, veido atvaizdais ir policijos įrašais per ES maršruto parinktuvus. Nacionaliniu lygmeniu valstybės narės turi įgyvendinti **Keitimosi informacija direktyvą**[20], kuria stiprinami keitimosi informacija kanalai sklandžiam tarpvalstybiniam informacijos srautui užtikrinti, kartu užtikrinant jų integraciją į Sąjungos lygmens sistemas, pavyzdžiui, SIENA[21].

Veiksmingas tarpvalstybinis bendradarbiavimas taip pat priklauso nuo **bendros ES teisėsaugos kultūros** puoselėjimo. Siekiant šio tikslo labai svarbūs bendri mokymai, kompetencijos centrai ir judumo programos. Komisija išnagrinės, kaip ES galėtų geriausiai remti valstybių narių valdžios institucijų mokymą, remdamasi **CEPOL** kaip ES teisėsaugos mokymo agentūra.

Sienų saugumo stiprinimas

Siekiant kovoti su hibridinėmis grėsmėmis, pavyzdžiui, naudojimusi migracija kaip ginklu, užkirsti kelią priešiškų subjektų ir grėsmę keliančių prekių patekimui į ES ir veiksmingai kovoti su tarpvalstybiniu nusikalstamumu ir terorizmu, labai svarbu stiprinti išorės sienų atsparumą ir saugumą. 2026 m. **planuojama patobulinti Šengeno informacinę sistemą (SIS)**, kad valstybės narės galėtų įvesti perspėjimus apie trečiųjų šalių piliečius, susijusius su terorizmu, įskaitant užsienio teroristus kovotojus, ir kitais sunkiais nusikaltimais, remiantis duomenimis, kuriais trečiosios šalys dalijasi su Europolu.

Užtikrinus geresnį didelės apimties ES informacinių sistemų **sąveikumą** valstybėms narėms bus teikiama esminė informacija apie išorės sienas kertančius arba ketinančius kirsti asmenis iš trečiųjų šalių, padedant valdžios institucijoms įvertinti leidimo atvykti į valstybių narių teritoriją sąlygas[22]. Komisija toliau glaudžiai bendradarbiaus su valstybėmis narėmis ir eu-

[18] Kaip nurodyta Komisijos atliktame 2022 m. birželio 9 d. Tarybos rekomendacijos (ES) 2022/915 dėl operatyvinio teisėsaugos bendradarbiavimo įgyvendinimo valstybėse narėse vertinime (dok. 5909/25).

[19] 2024 m. kovo 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/982 dėl automatinės duomenų paieškos ir keitimosi duomenimis policijos bendradarbiavimo srityje, kuriuo iš dalies keičiami Tarybos sprendimai 2008/615/TVR ir 2008/616/TVR ir Europos Parlamento ir Tarybos reglamentai (ES) 2018/1726, (ES) 2019/817 ir (ES) 2019/818 (reglamentas „Priumas II“), OL L, 2024/982, 2024 4 5.

[20] 2023 m. gegužės 10 d. Europos Parlamento ir Tarybos direktyva (ES) 2023/977 dėl valstybių narių teisėsaugos institucijų keitimosi informacija, kuria panaikinamas Tarybos pamatinis sprendimas 2006/960/TVR, OL L 134, 2023 5 22, p. 1–24.

[21] Saugaus keitimosi informacija tinklo programa.

[22] Visų pirma atvykimo ir išvykimo sistema (AIS) suteiks valstybėms narėms galimybę nustatyti trečiųjų šalių piliečių tapatybę prie Šengeno erdvės išorės sienų ir registruoti jų atvykimą ir išvykimą, kad būtų galima sistemingai nustatyti užsibuvusių asmenų tapatybę. Prieš trečiosios šalies piliečiui atvykstant prie išorės sienų, valstybės narės, naudodamosi Europos kelionių informacijos ir leidimų sistema (ETIAS) ir Vizų informacine sistema (VIS), galės iš anksto įvertinti, ar trečiosios šalies piliečio buvimas ES teritorijoje keltų pavojų saugumui.

LISA, kad šios sistemos, visų pirma **atvykimo ir išvykimo sistema (AIS), Europos kelionių informacijos ir leidimų sistema (ETIAS) ir peržiūrėta Vizų informacinė sistema (VIS)**, būtų greitai įdiegtos ir būtų užtikrintas sklandus jų veikimas ir nauda saugumui.

Siekdama toliau stiprinti sienų saugumą ir ES bendradarbiavimą kintančių grėsmių akivaizdoje, **Komisija pasiūlys sustiprinti FRONTEX**. Europos sienų ir pakrančių apsaugos pajėgos ilgainiui turėtų padidėti tris kartus iki 30 000 darbuotojų. Agentūra turėtų būti aprūpinta pažangiomis stebėjimo ir informuotumo apie padėtį technologijomis, įskaitant Europos integruotam sienų valdymui svarbią žvalgybos informaciją, ir sienos kontrolės tikslais turėti prieigą prie patikimų ES Žemės stebėjimo vyriausybinių paslaugų, kurios turi būti įdiegtos iki 2027 m. Tai turėtų dar labiau sustiprinti gebėjimą nustatyti tarpvalstybinius nusikaltimus prie išorės sienų, užkirsti jiems kelią ir su jais kovoti, taip pat padėti valstybėms narėms vykdyti grąžinimą, visų pirma susijusį su trečiųjų šalių piliečiais, kurie kelia pavojų saugumui.

Dokumentų ir tapatybės klastojimas palengvina neteisėtą migrantų gabenimą, prekybą žmonėmis, slaptus nusikalstamus judėjimus ir prekybą neteisėtomis prekėmis. Pradėjus veikti **daugybinių tapatybių detektoriui (DTD)**[23] pagerės nacionalinių institucijų gebėjimas nustatyti daugybines tapatybes naudojančių asmenų tapatybę ir kovoti su tapatybės klastojimu. Komisija išnagrinės būdus, kaip padidinti ES piliečiams ir trečiųjų šalių piliečiams išduodamų kelionės dokumentų ir teisę gyventi šalyje patvirtinančių dokumentų saugumą. Be to, Komisija įvertins, kaip ES skaitmeninės tapatybės dėklės, kurios turi būti įdiegtos pagal Europos skaitmeninės tapatybės sistemą iki 2026 m. pabaigos, gali padėti padidinti kelionės dokumentų saugumą ir pagerinti tapatybės tikrinimą. Taip bus papildyti pasiūlymai dėl skaitmeninių kelionės kredencialų ir ES skaitmeninių kelionės duomenų programėlės[24].

Kelionių informacija yra labai svarbi valdžios institucijoms, kad jos galėtų nustatyti ir tirti nusikaltėlių, teroristų ir kitų asmenų, keliančių grėsmę saugumui, judėjimą. Nors egzistuoja ES komercinių kelionių oro transportu informacijos sistema[25], kelionių kitų rūšių transportu duomenų tvarkymas teisėsaugos tikslais yra fragmentiškas. Todėl nusikaltėliai ir teroristai gali naudotis įvairių rūšių transportu neteisėtai veiklai vykdyti ir nebūti susekti. Komisija bendradarbiaus su valstybėmis narėmis ir transporto sektoriumi, kad **sustiprintų kelionių informacijos sistemą**, nagrinėdama Sąjungos sistemą, pagal kurią privačių skrydžių operatoriai būtų įpareigoti rinkti ir perduoti keleivių duomenis, ir vertindama keleivio duomenų įrašų tvarkymo taisykles bei būdus, kaip supaprastinti informacijos apie keliones jūra tvarkymą. Kelių transporto srityje Komisija įvertins galimybes naudoti **automatinio automobilio registracijos numerio identifikavimo** sistemas platesniu mastu ir padidinti sąveikos su SIS galimybes.

Prognozavimas, inovacijos ir pajėgumais grindžiamas požiūris

Komisija, remdamasi nacionaliniu lygmeniu nustatyta geriausia praktika, parengs **visapusišką vidaus saugumo padėties prognozavimo ES lygmeniu metodą**. Šis metodas padės formuoti politiką ir nukreipti investicijas į atitinkamus ES finansuojamus saugumo srities mokslinius tyrimus ir inovacijas.

Moksliniai tyrimai ir inovacijos atlieka labai svarbų vaidmenį užtikrinant vidaus saugumą, nes vykdant šią veiklą sukuriami sprendimai, kaip kovoti su naujomis grėsmėmis,

[23] DTD yra vienas iš sąveikumo komponentų, nustatytų Reglamentu (ES) 2019/818 ir Reglamentu 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/lt/ip_24_5047
[25] Keleivio duomenų įrašo (PNR) ir išankstinės informacijos apie keleivius (API) sistema, nustatyta Direktyva (ES) 2016/681 (PNR direktyva) ir Reglamentu (ES) 2025/12 bei Reglamentu (ES) 2025/13 (toliau – API reglamentai).

be kita ko, atsirandančiomis dėl netinkamo technologijų naudojimo[26]. ES, pasitelkdama ES finansuojamus saugumo mokslinius tyrimus ir inovacijas[27], turi toliau investuoti į kovai su grėsmėmis saugumui skirtų novatoriškų priemonių ir sprendimų kūrimą, kartu laikantis ES taisyklių ir pagrindinių teisių. Komisija turėtų remti perėjimą nuo mokslinių tyrimų prie diegimo, kad būtų užtikrintas veiksmingas tų šiuolaikinių pajėgumų panaudojimas, pirmenybę teikiant tokioms **šiuolaikinėms technologijoms** kaip dirbtinis intelektas (DI). Šis požiūris turėtų apimti mokymus, kuriais būtų siekiama pagerinti teisėsaugos ir teisminių institucijų naudojimąsi DI sistemomis ir kitais techniniais pajėgumais. Be to, kai aktualu, dvejopo naudojimo technologijų potencialas turėtų būti išnaudojamas abiem kryptimis (nuo naudojimo civilinėms reikmėms iki naudojimo gynybos sektoriuje ir nuo naudojimo gynybos sektoriuje iki naudojimo civilinėms reikmėms)[28].

ES vidaus saugumo inovacijų centras[29] – inovacijų laboratorijų tinklas, teikiantis naujausius inovacijų naujinius ir veiksmingus sprendimus ES ir valstybių narių vidaus saugumo subjektų darbui remti, padėsiantis integruoti mokslinius tyrimus į praktiką ir politiką. Siekiant padidinti Europolo veiksmingumą, reikia stiprinti Europolo priemonių saugyklą (ETR), kad jis galėtų nustatyti, plėtoti, bendrai pirkti ir praktiškai taikyti pažangias technologijas. Be to, Komisija savo Jungtiniame tyrimų centre įsteigs **saugumo mokslinių tyrimų ir inovacijų kompleksą**, subursiantį tyrėjus tam, kad būtų sutrumpintas ciklas nuo mokslinių tyrimų rezultatų iki inovacijų, plėtros ir sėkmingo įgyvendinimo, taip pat sumažintos kūrimo, bandymo ir patvirtinimo išlaidos.

Mūsų **Europos mokslinių tyrimų erdvė** pagal savo pobūdį yra bendradarbiavimu grindžiama erdvė, todėl ji neapsaugota nuo užsienio šalių kišimosi ir dezinformacijos. Priėmus Tarybos rekomendaciją dėl mokslinių tyrimų saugumo didinimo[30], Komisija ir valstybės narės imasi priemonių, kuriomis siekiama suteikti atitinkamiems subjektams galių, *inter alia*, įsteigdamos mokslinių tyrimų saugumo kompetencijos centrą.

Pagrindiniai veiksmai

Komisija priims:

- **pasiūlymą dėl teisėkūros procedūra priimamo akto, kuriuo siekiama pertvarkyti Europolą į gerai veikiančią teisėsaugos agentūrą (2026 m.);**
- **pasiūlymą dėl teisėkūros procedūra priimamo akto dėl Eurojusto stiprinimo (2026 m.);**
- **pasiūlymą dėl teisėkūros procedūra priimamo akto, kuriuo būtų sustiprintas FRONTEX vaidmuo ir užduotys (2026 m.);**
- **pasiūlymą dėl teisėkūros procedūra priimamo akto dėl Europos ypatingos svarbos ryšių sistemos sukūrimo (2026 m.).**

Komisija:

[26] Žr. Komisijos Jungtinio tyrimų centro ataskaitą „Emerging risks and opportunities for EU internal security stemming from new technologies“ („Dėl naujų technologijų atsirandanti rizika ir galimybės ES vidaus saugumui“), https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025 (2025 m. tyrimas „ES finansuojamų saugumo mokslinių tyrimų ir inovacijų stiprinimas. 20 metų ES finansuojami civilinės saugos moksliniai tyrimai ir inovacijos“), https://data.europa.eu/doi/10.2837/0004501.

[28] Kaip nurodyta S. Niinistö pranešime.

[29] ES vidaus saugumo inovacijų centras | Europolas.

[30] OL C/2024/3510, 2024 5 30.

- **2025 m. pateiks veiksmų gaires, kuriose išdėstomi tolesni veiksmai, susiję su teisėta ir veiksminga prieiga prie duomenų teisėsaugos tikslais;**
- **2025 m. parengs poveikio vertinimą, siekdama atitinkamai atnaujinti duomenų saugojimo ES lygmeniu taisykles;**
- **2026 m. pateiks šifravimo technologijų veiksmų gaires, kad būtų nustatyti ir įvertinti technologiniai sprendimai, kuriais teisėsaugos institucijoms būtų suteikta teisėta prieiga prie duomenų;**
- **dirbs siekdama sukurti aukšto lygio grupę operatyviniam teisėsaugos bendradarbiavimui stiprinti;**
- **2026 m. Jungtiniame tyrimų centre įsteigs saugumo mokslinių tyrimų ir inovacijų kompleksą.**

Komisija, bendradarbiaudama su valstybėmis narėmis ir atitinkamomis ES agentūromis:

- **sustiprins EMPACT architektūrą;**
- **dirbs siekdama, kad būtų greitai įdiegta sąveikumo architektūra ir įgyvendintas reglamentas „Priumas II“;**
- **sustiprins kelionių informacijos sistemą.**

Valstybės narės primygtinai raginamos:

- **perkelti į nacionalinę teisę ir visapusiškai įgyvendinti Keitimosi informacija direktyvą.**

4. Atsparumas hibridinėms grėsmėms ir kitiems priešiškiems veiksmams

Didinsime atsparumą hibridinėms grėsmėms gerindami ypatingos svarbos infrastruktūros apsaugą, stiprindami kibernetinį saugumą, apsaugodami transporto mazgus ir uostus ir kovodami su internetinėmis grėsmėmis.

Padažnėjo priešiškų veiksmų, kuriais kenkiama ES saugumui, ir jie tapo sudėtingesni, piktavaliams subjektams smarkiai plečiant savo arsenalą. Suintensyvėjo prieš ES, jos valstybes nares ir partnerius nukreiptos hibridinės kampanijos, apimančios prieš ypatingos svarbos infrastruktūrą nukreiptus sabotažo veiksmus, padegimus, kibernetinius išpuolius, kišimąsi į rinkimus, užsienio vykdomą kišimąsi ir manipuliavimą informacija (FIMI), įskaitant dezinformaciją, ir naudojimąsi migracija kaip ginklu. Dėl savo politinio ir operatyvinio vaidmens ir tvarkomos informacijos pobūdžio Sąjungos institucijos, įstaigos, organai ir agentūros (toliau – Sąjungos subjektai) taip pat tampa jų taikiniu.

ES turi **didinti savo atsparumą**, veiksmingai naudoti dabartines priemones ir ieškoti naujų būdų kovoti su šiomis kintančiomis grėsmėmis, kylančiomis dėl valstybinių ir nevalstybinių subjektų, tiek dabar, tiek ateityje.

Ypatingos svarbos infrastruktūra

Didžiausią susirūpinimą kelia grėsmės **ypatingos svarbos infrastruktūrai**, įskaitant hibridines grėsmes, pavyzdžiui, sabotažą ir kibernetinę kenkimo veiklą, visų pirma infrastruktūrai, jungiančiai valstybes nares, nesvarbu, ar tai būtų energijos jungiamosios linijos, ar tarpvalstybiniai ryšių kabeliai, ir transporto srityje. Nuo Rusijos agresijos karo prieš Ukrainą pradžios, ypač 2024 m., padaugėjo prieš ypatingos svarbos infrastruktūros objektus nukreiptų sabotažo veiksmų, kurie daro poveikį daugeliui valstybių narių. Teisėsaugos, saugumo ir kibernetinio saugumo tarnybų, karinės ir civilinės saugos tarnybų ir privačių veiklos vykdytojų

bendradarbiavimas yra labai svarbus siekiant veiksmingai numatyti tokius veiksmus, juos nustatyti, užkirsti jiems kelią ir į juos reaguoti.

Siekiant užtikrinti nepertraukiamą ekonomikai ir visuomenei gyvybiškai svarbių paslaugų teikimą, būtina mažinti ypatingos svarbos subjektų pažeidžiamumą ir didinti jų atsparumą. Todėl šiuo atžvilgiu labai svarbu, kad visos valstybės narės laiku perkeltų į nacionalinę teisę ir tinkamai įgyvendintų **Direktyvą dėl ypatingos svarbos subjektų atsparumo**[31] ir **Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS2)**[32].

Siekdama užtikrinti sparčią pažangą, Komisija, bendradarbiaudama su **Ypatingos svarbos subjektų atsparumo klausimų grupe ir TIS bendradarbiavimo grupe**, padės valstybėms narėms nustatyti ypatingos svarbos subjektus[33] ir keistis gerąja patirtimi, susijusia su nacionaline strategija ir rizikos vertinimais esminių paslaugų srityje. Jei ypatingos svarbos infrastruktūros sutrikimai darys didelį tarpvalstybinį poveikį, pagal **ES ypatingos svarbos infrastruktūros planą** bus koordinuojami ES lygmens atsakomieji veiksmai. Komisija ragina Tarybą skubiai priimti **ES kibernetinio saugumo planą** ir pagal šį planą bus toliau stiprinamas su krizių valdymu susijęs koordinavimas, sudarant palankesnes sąlygas glaudesniam valdžios institucijų bendradarbiavimui fizinio ir skaitmeninio atsparumo srityje. Po 2023 m. sėkmingai atlikto energetikos sektoriaus testavimo nepalankiausiomis sąlygomis Komisija skatins **savanoriškai atlikti** kitų pagrindinių vidaus saugumo sektorių **testavimą nepalankiausiomis sąlygomis**. Be to, Komisija pateiks **Sąjungos lygmens tarpvalstybinės ir tarpsektorinės rizikos** esminėms paslaugoms **apžvalgą**, kad padėtų valstybėms narėms atlikti rizikos vertinimus ir pateiktų išsamiam ES lygmens rizikos vertinimui atlikti reikalingos informacijos. Laikydamasi ES pasirengimo krizėms strategijos, Komisija bendradarbiaus su valstybėmis narėmis, kad nustatytų kitus sektorius ir paslaugas, neįtrauktus į dabartinių teisės aktų taikymo sritį, dėl kurių gali prireikti imtis veiksmų.

ES ir NATO ypatingos svarbos infrastruktūros atsparumo didinimo darbo grupė skatino puikų bendradarbiavimą dalijantis geriausios praktikos pavyzdžiais ir didinant atsparumą energetikos, transporto, skaitmeninės infrastruktūros ir kosmoso sektoriuose. Šis darbas bus tęsiamas vykdant **ES ir NATO struktūrinį dialogą atsparumo klausimais**. **ES hibridinių priemonių rinkiniu** valstybėms narėms ir partneriams siūloma tvirta parama rengiantis hibridinėms grėsmėms ir su jomis kovojant. Valstybių narių, įvairių ES misijų ir partnerių prašymu **greitojo reagavimo į hibridines grėsmes grupės**[34] teikia pritaikytą trumpalaikę pagalbą. Be to, Komisija tęs ES bendradarbiavimą kovos su sabotažu srityje pasitelkdama ekspertų veiklą[35], įskaitant **specialią bendrą** ekspertų **darbo programą**, kuria siekiama supaprastinti keitimąsi informacija ir nustatyti atsakomąsias priemones.

Incidentai, per kuriuos pažeidžiami **jūriniai kabeliai** Europoje, rodo, kad reikia griežtesnių priemonių ir aiškesnių atsakomųjų veiksmų. Kaip nurodyta **ES veiksmų plane dėl kabelių**

[31] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2557 dėl ypatingos svarbos subjektų atsparumo, kuria panaikinama Tarybos direktyva 2008/114/EB.

[32] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148, (TIS 2 direktyva).

[33] Į direktyvos taikymo sritį įtraukti energetikos, transporto, bankininkystės, finansų rinkos infrastruktūros, sveikatos, geriamojo vandens, nuotekų, skaitmeninės infrastruktūros, viešojo administravimo, kosmoso, maisto gamybos, perdirbimo ir paskirstymo sektoriai.

[34] 2022 m. ES saugumo ir gynybos strateginis kelrodis, p. 22.

[35] ES patarėjus saugumo klausimais, Europos sprogmenų atsargų nukenksminimo tinklą (EEODN), tinklą „Atlas“, ES didelės rizikos viešųjų erdvių saugumo tinklą, ChBRB saugumo klausimų patariamąją grupę, Ypatingos svarbos subjektų atsparumo klausimų grupę.

saugumo[36], Komisija kartu su vyriausiuoju įgaliotiniu bendradarbiaus su valstybėmis narėmis, ES agentūromis ir partneriais, pavyzdžiui, NATO, kad užkirstų kelią grėsmėms povandeniniams kabeliams, jas nustatytų, į jas reaguotų ir jas pašalintų. Siekdama sukurti integruotą grėsmių padėties vaizdo sistemą, Komisija bendradarbiaus su valstybėmis narėmis, kad būtų sukurtas ir savanoriškai įdiegtas integruotas jūrinių kabelių stebėjimo kiekviename jūros baseine mechanizmas, pradedant Šiaurės ir Baltijos šalių regioniniu centru.

Kibernetinis saugumas

Dėl to, kad **kibernetinė kenkimo veikla**, kuri dažnai yra įvairesnių daugialypių ir hibridinių grėsmių dalis, yra nuolatinio pobūdžio, reikia nuolatinio dėmesio ir veiksmų Europos lygmeniu. Pastaraisiais metais Sąjunga priėmė įvairius kibernetinio saugumo teisės aktus, kuriais stiprinamas ES ypatingos svarbos sektoriuose veikiančių TIS 2 subjektų ir Sąjungos subjektų kibernetinis atsparumas[37], didinamas skaitmeninių produktų saugumas (Kibernetinio atsparumo aktas) ir nustatoma pasirengimo ir reagavimo į incidentus paramos sistema (Kibernetinio solidarumo aktas). 2025 m. sausio mėn. Komisija priėmė **Europos ligoninių ir sveikatos priežiūros paslaugų teikėjų kibernetinio saugumo veiksmų planą**[38], kuriuo siekiama pagerinti grėsmių nustatymą, pasirengimą joms ir reagavimą į jas. Labai svarbu, kad jis būtų visiškai įgyvendintas. Tuo pat metu, siekdami reaguoti į naujas grėsmes ir pokyčius, turime imtis aktyvesnių veiksmų, visų pirma keitimosi informacija, tiekimo grandinės saugumo, išpirkos reikalavimo programinės įrangos ir kibernetinių išpuolių bei technologinio suverenumo srityse.

Be to, norint jį įgyvendinti, reikia panaikinti dabartinį 299 000 kibernetinio saugumo srities kvalifikuotų darbuotojų trūkumą. Komisija bendradarbiaus su valstybėmis narėmis pagal įgūdžių sąjungos kūrimo iniciatyvą[39], kad būtų išplėsta kibernetinio saugumo darbo jėga, visų pirma pasitelkiant naująją Kibernetinio saugumo įgūdžių akademiją. Strateginis gamtos mokslų, technologijų, inžinerijos ir matematikos mokymo planas[40] padeda gerinti talentų bazę ir Europos atsaką į kibernetinio saugumo darbo rinkos poreikius.

ES ne tik didins savo atsparumą, bet ir toliau visapusiškai naudosis Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistema **(Kibernetinio saugumo diplomatijos priemonių rinkiniu)**, kad užkirstų kelią valstybinių ir nevalstybinių subjektų keliamoms kibernetinėms grėsmėms, jas pašalintų ir į jas reaguotų.

IRT tiekimo grandinių saugumas

5G kibernetinio saugumo priemonių rinkiniu sukuriama tinkama 5G tinklų apsaugos sistema, tačiau šiuo metu jis nėra pakankamu mastu įgyvendintas valstybėse narėse. Tebėra nepriimtinos saugumo rizikos, visų pirma susijusios su didelės rizikos paslaugų teikėjų pakeitimu. Suderintas požiūris į IRT tiekimo grandinės saugumą gali padėti pašalinti dabartinį skirtingų nacionalinio lygmens požiūrių sukurtą vidaus rinkos susiskaidymą, išvengti kritinės priklausomybės ir sumažinti mūsų IRT tiekimo grandinių riziką, kylančią dėl didelės rizikos tiekėjų, taip apsaugant mūsų ypatingos svarbos infrastruktūrą.

[36] JOIN(2025) 9 *final*.
[37] 2023 m. gruodžio 13 d. Europos Parlamento ir Tarybos reglamentas (ES, Euratomas) 2023/2841, kuriuo nustatomos priemonės aukštam bendram kibernetinio saugumo lygiui Sąjungos institucijose, įstaigose, organuose ir agentūrose užtikrinti, OL L, 2023/2841, 2023 12 18.
[38] https://digital-strategy.ec.europa.eu/lt/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers
[39] COM(2025) 90 *final*.
[40] COM(2025) 89 *final*.

Laikydamasi šio požiūrio, per būsimą **Kibernetinio saugumo akto** peržiūrą Komisija plačiau nagrinės IRT tiekimo grandinių ir infrastruktūros saugumo ir atsparumo klausimus. Be to, Komisija siūlys patobulinti **Europos kibernetinio saugumo sertifikavimo sistemą**, siekdama užtikrinti, kad būsimos sertifikavimo schemos galėtų būti priimtos laiku ir atitiktų politikos poreikius.

Remdamasi esamais arba šiuo metu atliekamais sektorių vertinimais[41], Komisija kartu su valstybėmis narėmis parengs **strateginio suderintų kibernetinio saugumo rizikos vertinimų planavimo sistemą**.

Debesijos ir telekomunikacijų paslaugos tapo įprastiniu ypatingos svarbos infrastruktūros objektų, įmonių ir valdžios institucijų tiekimo grandinių elementu. Komisija imsis veiksmų, kad paskatintų ypatingos svarbos subjektus rinktis **debesijos ir telekomunikacijų paslaugas, kuriomis užtikrinamas tinkamas kibernetinio saugumo lygis**, atsižvelgiant ne tik į techninę riziką, bet ir į strateginę riziką ir priklausomybę.

Išpirkos reikalavimo programinė įranga ir kibernetiniai išpuoliai

Viena iš nuolatinių didelių problemų ES ir visame pasaulyje yra **išpirkos reikalavimo programinė įranga**, dėl kurios, kaip apskaičiuota vienoje ataskaitoje, iki 2031 m. pasaulinės metinės išlaidos sudarys daugiau kaip 250 mlrd. EUR[42]. Tiek **TIS 2 direktyva**, tiek **Kibernetinio atsparumo aktu** bus gerokai pagerinta subjektų saugumo padėtis, todėl išpirkos reikalavimo programinę įrangą naudojantiems tinklams bus brangiau vykdyti savo išpuolius. Be to, Komisija glaudžiai bendradarbiaus su valstybėmis narėmis siekdama užtikrinti, kad teisėsaugos institucijoms būtų dažniau pranešama apie išpuolius, vykdomus naudojant išpirkos reikalavimo programinę įrangą, visų pirma apie dideles nuolatines grėsmes ir išpirkos mokėjimus, ir taip būtų palengvinami tyrimai.

Siekdama užkirsti kelią kibernetiniams išpuoliams ir juos sustabdyti, ES turi stiprinti teisėsaugos institucijų, kibernetinio saugumo institucijų ir subjektų bei privačių subjektų tarpusavio keitimąsi informacija vadovaujant Europolui ir ES kibernetinio saugumo agentūrai (ENISA).

Europolo ir Eurojusto agentūros turėtų toliau remtis laimėjimais, kurių pasiekė nutraukdamos išpirkos reikalavimo programinės įrangos operacijas ir taip remdamos teisėsaugos bendradarbiavimą. Šiuo tikslu teisėsaugos institucijos turėtų kuo labiau išnaudoti bendradarbiavimo mechanizmus, įskaitant **Europolo tarptautinį reagavimo į išpirkos reikalavimo programinę įrangą modelį** ir **Tarptautinę kovos su išpirkos reikalavimo programine įranga iniciatyvą**[43], o ENISA ir Europolas turėtų bendradarbiauti, kad būtų išplėsta išpirkos reikalavimo programinės įrangos atmainų iššifravimo priemonių saugykla[44].

Technologinis suverenumas

Kibernetinis saugumas ir technologinis suverenumas yra glaudžiai tarpusavyje susiję, tad pirmiausiai reikia spręsti technologinės priklausomybės klausimą. Sąjunga turi **vadovauti naujų technologijų kūrimui ir diegimui**, o Komisija turi **stiprinti** tokių **strateginių technologijų** kaip dirbtinis intelektas, kvantinės technologijos, pažangusis junglumas, debesija,

[41] Pavyzdžiui, 5G tinklų, telekomunikacijų, elektros energijos, atsinaujinančiųjų išteklių energijos ir susietųjų transporto priemonių srityse.

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[43] https://counter-ransomware.org/

[44] Galima rasti projektui „No More Ransom“ skirtoje svetainėje https://www.nomoreransom.org/lt/index.html.

tinklo paribio technologijos ir daiktų internetas[45] **srities pajėgumus**, įgyvendindama būsimas iniciatyvas, pavyzdžiui, Žemyno dirbtinio intelekto veiksmų planą, Kvantinių technologijų strategiją ir kitas iniciatyvas[46]. Komisija toliau teiks paramą, kuria siekiama, kad būtų laiku įdiegti naujausi turimi tarptautiniu mastu sutarti **interneto protokolai**, kurie yra labai svarbūs siekiant išlaikyti lengvai prieinamą ir našų internetą, užtikrinantį didesnį kibernetinį saugumą. Taip pat reikia imtis tolesnių veiksmų, kad būtų sprendžiamos **su radijo spektru susijusios problemos**, tokios kaip GNSS signalo klastojimas, trukdžiai, tiekimo grandinės rizika ir priklausomybė: pavyzdžiui, naudoti kvantinio matavimo technologijas ir nagrinėti galimybę išplėtoti radijo dažnio stebėsenos pajėgumus.

Siekiant apsaugoti perduodamą neskelbtiną informaciją, saugomus duomenis ir skaitmeninę tapatybę naujame kvantiniame amžiuje bus labai svarbu įdiegti **postkvantinės kriptografijos** sprendimus. Remdamasi 2024 m. Rekomendacija dėl Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių[47], Komisija bendradarbiauja su valstybėmis narėmis, kad paskatintų tą perėjimą. Šiuo atžvilgiu valstybės narės turėtų kuo greičiau ir ne vėliau kaip iki 2030 m. pabaigos nustatyti ypatingos svarbos subjektų taikomos didelės rizikos atvejus ir užtikrinti šiais didelės rizikos atvejais taikytiną kvantiniams kompiuteriams atsparų šifravimą. Komisija taip pat bendradarbiauja su valstybėmis narėmis ir Europos kosmoso agentūra (EKA), kad sukurtų ir įdiegtų kvantinių raktų paskirstymu grindžiamą **Europos kvantinio ryšio infrastruktūrą**[48], kuri yra ES saugaus junglumo programos **IRIS²** dalis. Abiem iniciatyvomis galiausiai bus sudarytos sąlygos subjektams saugiai perduoti duomenis ir saugoti informaciją.

Kvantinės technologijos taip pat atliks svarbų vaidmenį saugumo prietaikų srityje: bus parengtos **kvantinio matavimo saugumo prietaikų srities veiksmų gairės** kaip **Kvantinių technologijų strategijos** dalis. Komisija taip pat siekia, kad jos organizacijos saugumo požiūriu itin svarbios sistemos, įskaitant įslaptintas IT sistemas, būtų atsparios kvantiniams kompiuteriams.

Verslui palanki kibernetinio saugumo sistema

Būsima Kibernetinio saugumo akto peržiūra suteikia galimybę **supaprastinti ES kibernetinio saugumo teisės aktus**, laikantis Konkurencingumo kelrodžio. Komisija glaudžiai bendradarbiaus su valstybėmis narėmis, kad užtikrintų greitą, nuoseklų ir verslui palankų TIS 2 direktyvoje, Kibernetinio atsparumo akte ir Kibernetinio solidarumo akte nustatytos horizontaliosios kibernetinio saugumo sistemos įgyvendinimą, skatindama paprastumą ir nuoseklumą ir vengdama kibernetinio saugumo taisyklių susiskaidymo ar dubliavimo ES ir nacionalinės teisės aktuose.

Kad būtų užtikrinta saugi prieiga prie internetinių paslaugų ir sustiprintas skaitmeninis saugumas visoje ES, pagal **Europos skaitmeninės tapatybės sistemą** visiems ES piliečiams ir gyventojams iki 2026 m. pabaigos bus pasiūlytos patikimos skaitmeninės tapatybės dėklės. Įdiegus būsimą **Europos verslo dėklę** bus sudarytos palankesnės sąlygos saugiai tarpvalstybinei įmonių ir viešojo administravimo institucijų sąveikai. Abi šios priemonės yra būtinos saugiam ir veiksmingesniam duomenimis grindžiamos bendrosios rinkos veikimui, naudojant tokias priemones kaip bendrieji skaitmeniniai vartai, elektroninės sąskaitos faktūros, elektroninis viešasis pirkimas ir skaitmeninis gaminio pasas.

[45] https://strategic-technologies.europa.eu/about_en?prefLang=lt&etrans=lt

[46] Pvz., „EuropHPC“ bendrosios įmonės iniciatyvą, https://eurohpc-ju.europa.eu/index_en, Pavyzdinę kvantinių technologijų iniciatyvą, *Homepage of Quantum Flagship* | Quantum Flagship, 3C tinklų iniciatyvą (COM(2024) 81 *final*) ir ES veiksmų planą dėl kabelių saugumo (JOIN(2025) 9 *final*).

[47] Rekomendacija dėl Koordinuotų perėjimo prie postkvantinės kriptografijos veiksmų gairių | *Shaping Europe's digital future*.

[48] https://digital-strategy.ec.europa.eu/lt/policies/european-quantum-communication-infrastructure-euroqci

Internetinis saugumas

Kai kurios didžiausios hibridinės grėsmės, keliančios pavojų žmonių saugumui ir saugai Europoje ir nukreiptos prieš ES demokratinę erdvę, kyla internete. Šios grėsmės apima neteisėtą veiklą ir neteisėtą turinį internete, manipuliavimą informacija, susijusį su dirbtiniu sureikšminimu, klaidinančia informacija ir užsienio vykdomu manipuliavimu informacija ir kišimusi (FIMI).

Griežtas **Skaitmeninių paslaugų akto (SPA)** vykdymo užtikrinimas yra labai svarbus siekiant užtikrinti saugią ir prieinamą interneto aplinką su atskaitingais subjektais, kuri taip pat būtų atspari hibridinėms grėsmėms. Skaitmeninių paslaugų aktu labai didelių interneto platformų ir labai didelių interneto paieškos sistemų paslaugų teikėjai įpareigojami atlikti rizikos vertinimus ir įdiegti dėl jų paslaugų kūrimo, veikimo ar naudojimo kylančios sisteminės rizikos mažinimo priemones. Tokia rizika gali būti neigiamas poveikis pilietiniam diskursui ir rinkimų procesams, taip pat visuomenės saugumui, kaip antai plataus masto piktavališkų užsienio valstybių subjektų kišimasis, pavyzdžiui, į rinkimų procesus. Svarbu mokyti valstybių narių kompetentingas institucijas, kaip naudotis teisinėmis priemonėmis siekiant greitai pašalinti neteisėtą turinį internete, visų pirma susijusį su kibernetiniu smurtu dėl lyties. SPA numatytas reagavimo į krizes mechanizmas, kurį galima aktyvuoti, kai dėl ypatingų aplinkybių Sąjungoje arba didelėje jos dalyje kyla didelė grėsmė visuomenės saugumui ar visuomenės sveikatai. Siekdamos papildyti šį mechanizmą, Komisija ir nacionalinės kompetentingos institucijos, paskirtos skaitmeninių paslaugų koordinatoriais, taip pat sukūrė **SPA savanorišką reagavimo į incidentus sistemą**. Skaitmeninių paslaugų koordinatoriai taip pat ėmėsi veiksmų, kad padėtų apsaugoti rinkimų integralumą, pavyzdžiui, rengdami rinkimų apskritojo stalo diskusijas ir testavimą nepalankiausiomis sąlygomis[49]. Skaitmeninių paslaugų akte, kaip ir Reglamente dėl politinės reklamos[50], numatyta viena iš kelių krypčių, susijusių su demokratijos ir demokratinių procesų, kurie yra pažeidžiami dėl priešiškų subjektų išpuolių, be kita ko, vykdomų naudojant skaitmenines priemones ir socialiniuose tinkluose, integralumo apsauga.

FIMI priemonių rinkinio įgyvendinimas yra dar vienas svarbus komponentas, teikiantis svarbią paramą ES lygmeniu. Dedant šias pastangas taip pat labai svarbu remti skaitmeninio raštingumo, gebėjimo naudotis žiniasklaidos priemonėmis ir kritinio mąstymo ugdymą[51].

Kova su naudojimusi migracija kaip ginklu

Rusija, padedant ir ryžtingai remiant Baltarusijai, sąmoningai naudojosi migracija kaip ginklu ir neteisėtai skatino migracijos srautus prie ES išorės sienų, siekdama destabilizuoti mūsų visuomenę ir pakenkti Europos Sąjungos vienybei. Tai kelia pavojų ne tik valstybių narių nacionaliniam saugumui ir suverenumui, bet ir Šengeno erdvės saugumui ir vientisumui bei visos Sąjungos saugumui. 2024 m. spalio mėn. išvadose Europos Vadovų Taryba pabrėžė, kad Rusijai ir Baltarusijai ar bet kuriai kitai šaliai negali būti leidžiama piktnaudžiauti mūsų vertybėmis, įskaitant teisę į prieglobstį, ir kenkti mūsų demokratijai.

Kaip nurodyta 2024 m. Komisijos komunikate dėl naudojimosi migracija kaip ginklu, Sąjunga, siekdama veiksmingai kovoti su šiomis grėsmėmis, ne tik teikė tvirtą politinę paramą, bet ir ėmėsi finansinių, operatyvinių ir diplomatinių priemonių, įskaitant bendradarbiavimą su kilmės ir tranzito šalimis[52]. Šis atsakas, be kita ko, yra Tarybos sukurtos naujos sistemos naudojimas

[49] Skaitmeninių paslaugų akto rinkimams skirtas priemonių rinkinys skaitmeninių paslaugų koordinatoriams, 2025 m., https://digital-strategy.ec.europa.eu/lt/library/dsa-elections-toolkit-digital-services-coordinators.
[50] 2024 m. kovo 13 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/900 dėl politinės reklamos skaidrumo ir atrankiojo adresavimo, OL L, 2024/900, 2024 3 20.
[51] 2021–2027 m. skaitmeninio švietimo veiksmų planas – Europos švietimo erdvė.
[52] COM(2024) 570 *final*.

siekiant taikyti sankcijas asmenims ir organizacijoms, dalyvaujantiems vykdant tokius veiksmus ir politiką kaip, pavyzdžiui, Rusijos naudojimasis migracija kaip ginklu, įšaldant jų turtą arba draudžiant jiems keliauti[53]. Prireikus ES toliau naudosis šia sistema ir padės valstybėms narėms kovoti su šia grėsme.

Transporto saugumas

Jūrų uostai, oro uostai ir sausumos infrastruktūra yra labai svarbūs atvykimo ir išvykimo punktai. Jie atlieka itin reikšmingą vaidmenį ES ekonomikoje ir visuomenėje ir yra labai svarbūs kariniam mobilumui. Vis dėlto šie transporto mazgai ir priemonės taip pat yra pagrindiniai išorės grėsmių ir nusikalstamos veiklos taikiniai. Pastarojo meto incidentai, įskaitant krovinių gabenimo oro transportu saugumo reikalavimų pažeidimus ir išpuolius prieš geležinkelių infrastruktūrą, rodo, kad yra didelė rizika. **Vežėjai** gali būti ir piktavališkų subjektų taikiniai, ir priemonės. Galiojančios ES teisinės priemonės padėjo padidinti aviacijos saugumą[54], tačiau dėl didelės grėsmės civilinei aviacijai reikia priemonių incidentams numatyti ir greitai konsultuotis su atitinkamomis valstybėmis narėmis. Komisija bendradarbiaus su valstybėmis narėmis, kad iš dalies pakeistų galiojančius aviacijos saugumo srities įgyvendinimo teisės aktus, susijusius su dalijimusi įslaptinta informacija apie **aviacijos saugumo įvykius**. Be to, Komisija apsvarstys galimybę nustatyti **reguliavimo priemones**, skirtas kovai su naujomis grėsmėmis, pavyzdžiui, **krovinių vežimo oro transportu incidentais**, ir sugriežtinti aviacijos saugumo standartus. Tam taip pat reikės stiprinti **aviacijos saugumo teisės aktus**, kad būtų galima imtis neatidėliotinų reagavimo priemonių, kartu išlaikant vienkartinio patikrinimo zoną ES oro uostuose.

Rengdama būsimą **ES uostų strategiją**, remdamasi **ES uostų aljansu**, Komisija išnagrinės būdus, kaip toliau stiprinti jūrų saugumo teisės aktus, kad būtų veiksmingai kovojama su naujomis grėsmėmis, apsaugoti uostai ir padidintas ES tiekimo grandinės saugumas. Šiuo tikslu Komisija užtikrins patikimą jos įgyvendinimą ir dirbs, kad suderintų nacionalinę praktiką ir sugriežtintų asmenų patikrinimus uostuose. Nustačiusi oro transportu gabenamų krovinių saugumo protokolus, Komisija bendradarbiaus su valstybėmis narėmis ir privačiuoju sektoriumi, kad šie protokolai būtų išplėsti siekiant apsaugoti jūrų transporto grandines.

Siūloma, kad ES muitinė analizuotų ir vertintų riziką, remdamasi **muitinės informacija**, susijusia su į ES įvežamomis, iš jos išvežamomis ir per ją tranzitu gabenamomis prekėmis, ir taip padėtų valstybėms narėms užkirsti kelią piktavališkų subjektų naudojimuisi tarptautinėmis tiekimo grandinėmis. Pagal ES jūrų saugumo strategiją[55] būsimas **Europos vandenynų paktas** atliks svarbų vaidmenį didinant jūrų saugumą jūrų baseinuose aplink ES ir už jos ribų, be kita ko, skatinant plėsti daugiatiksles jūrų operacijas ir pratybas.

Tiekimo grandinių atsparumas

Europa turi mažiau naudoti trečiųjų šalių technologijas, nes tai gali lemti priklausomybę ir saugumo riziką. Komisija siekia sumažinti priklausomybę nuo vienintelių užsienio tiekėjų, sumažinti mūsų tiekimo grandinių riziką, kurią kelia didelės rizikos tiekėjai, taip pat apsaugoti ypatingos svarbos infrastruktūrą ir pramonės pajėgumus ES teritorijoje, kaip nurodyta **Konkurencingumo kelrodyje[56]** ir **Švarios pramonės kurso komunikate[57]**. Komisija skatins

[53] 2024 m. spalio 8 d. Tarybos reglamentas (ES) 2024/2642 dėl ribojamųjų priemonių atsižvelgiant į Rusijos destabilizuojančią veiklą, ST/8744/2024/INIT, OL L, 2024/2642, 2024 10 9.
[54] 2008 m. kovo 11 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 300/2008 dėl civilinės aviacijos saugumo bendrųjų taisyklių, OL L 97, 2008 4 9, p. 72–84.
[55] JOIN(2023) 8 *final*.
[56] COM(2025) 30 *final*.
[57] COM(2025) 85 *final*.

vidaus saugumo pramonės politiką bendradarbiaudama su pagrindiniais ES pramonės sektoriais (pvz., transporto mazgais, ypatingos svarbos infrastruktūros objektais), kad būtų parengti saugumo sprendimai, pavyzdžiui, aptikimo įranga, biometrinės technologijos ir bepiločiai orlaiviai, kuriuose integruoti pritaikytojo saugumo elementai. **Peržiūrėdama ES viešųjų pirkimų taisykles**, Komisija įvertins, ar 2009 m. Viešųjų pirkimų gynybos ir saugumo srityje direktyvoje[58] nustatytų saugumo aspektų pakanka teisėsaugos ir ypatingos svarbos subjektų atsparumo poreikiams patenkinti.

Komisija padės valstybėms narėms **tikrinti tiesiogines užsienio investicijas (TUI)** ir logistikos centrams skirtos įrangos viešuosius pirkimus, užtikrindama, kad ypatingos svarbos infrastruktūra ir technologijos išliktų saugios.

Pradėjus taikyti **Vidaus rinkos veikimo užtikrinimo ekstremaliomis sąlygomis ir atsparumo didinimo aktą (IMERA)**, jis padės ES valdyti krizes, dėl kurių sutrikdomos ypatingos svarbos tiekimo grandinės ir laisvas prekių, paslaugų ir žmonių judėjimas. Juo bus sudarytos sąlygos greitai koordinuoti krizes, nustatyti kilus krizei svarbias prekes ir paslaugas, ir suteikta priemonių, kuriomis užtikrinamas jų prieinamumas. Be to, glaudžiai bendradarbiaudama su valstybėmis narėmis, Komisija pasiūlys sukurti **tarpžinybinį įspėjimo apie transporto ir tiekimo grandinės saugumą mechanizmą**, kad būtų tinkamu laiku užtikrintas saugus keitimasis svarbia informacija, būtina grėsmėms numatyti ir su jomis kovoti.

Be to, įgyvendinus Ypatingos svarbos žaliavų aktą ir Poveikio klimatui neutralizavimo pramonės aktą, dažnesnis tvarumo, atsparumo ir pirmenybės teikimo Europai kriterijų taikymas ES viešuosiuose pirkimuose paskatins eksperimentinių rinkų plėtrą. Glaudesni prekybos ryšiai, pavyzdžiui, įgyvendinant partnerystės žaliavų srityje susitarimus ir švarios prekybos ir investicijų partnerystės susitarimus, padės įvairinti tiekimo grandines.

Atsparumas cheminėms, biologinėms, radiologinėms ir branduolinėms grėsmėms ir pasirengimas joms

Dėl Rusijos agresijos karo prieš Ukrainą **padidėjo cheminių, biologinių, radiologinių ir branduolinių (ChBRB) grėsmių rizika**. Siekdama spręsti galimo ChBRB medžiagų įsigijimo ir naudojimosi jomis kaip ginklu klausimą, Komisija rems valstybes nares ir šalis partneres rengdama specialius mokymus ir pratybas. Komisija taip pat didins pasirengimo ChBRB grėsmėms ir reagavimo į jas pajėgumus nustatydama grėsmių prioritetus, teikdama novatorišką finansavimą atsakomosioms priemonėms, „rescEU“ atsargoms ir kaupdama medicinines atsako priemones pagal naują **Pasirengimo ChBRB grėsmėms ir reagavimo į jas veiksmų planą**. Be to, **ES medicininių atsako priemonių strategija** bus remiamas medicininių atsako priemonių kūrimas nuo mokslinių tyrimų iki gamybos ir platinimo, siekiant apsaugoti ES nuo pandemijų ir ChBRB grėsmių.

Remdamasi per COVID-19 pandemiją įgyta patirtimi, ES sustiprino sveikatos saugumo sistemą[59]. Komisija skiria ES etalonines visuomenės sveikatos laboratorijas siekdama sustiprinti ES ir nacionalinius priežiūros ir greito aptikimo pajėgumus. 2025 m. bus paskelbtas Sąjungos parengties, prevencijos ir atsako veiksmų sveikatos saugumo srityje planas.

Pagrindiniai veiksmai

Komisija:

- **2025 m. peržiūrės ir atnaujins Kibernetinio saugumo aktą;**

[58] Direktyva 2009/81/EB dėl darbų, prekių ir paslaugų pirkimo tam tikrų sutarčių, kurias sudaro perkančiosios organizacijos ar subjektai gynybos ir saugumo srityse, sudarymo tvarkos derinimo, OL L 216, 2009 8 20.
[59] Visų pirma Reglamentu (ES) 2022/2371 dėl didelių tarpvalstybinio pobūdžio grėsmių sveikatai.

- **parengs priemones, kuriomis būtų užtikrintas saugus kibernetinis debesijos paslaugų naudojimas;**
- **2025 m. pasiūlys ES uostų strategiją;**
- **2026 m. peržiūrės ES gynybos ir saugumo srities viešųjų pirkimų taisykles;**
- **2026 m. pateiks naują Pasirengimo ChBRB grėsmėms ir reagavimo į jas veiksmų planą.**

Komisija, bendradarbiaudama su valstybėmis narėmis:

- **sukurs ir įdiegs Europos kvantinę ryšių infrastruktūrą (iniciatyva „EuroQCI“);**
- **užtikrins veiksmingą Skaitmeninių paslaugų akto vykdymą;**
- **vykdys darbą, kuriuo siekiama kovoti su naudojimusi migracija kaip ginklu;**
- **sukurs aviacijos saugumo įvykių sistemą;**
- **dirbs siekdama sukurti tarpžinybinį įspėjimo apie transporto ir tiekimo grandinės saugumą mechanizmą.**

Taryba primygtinai raginama:

- **priimti Tarybos rekomendaciją dėl ES kibernetinio saugumo plano.**

Valstybės narės primygtinai raginamos:

- **perkelti į nacionalinę teisę ir visapusiškai įgyvendinti Direktyvą dėl ypatingos svarbos subjektų atsparumo ir TIS 2 direktyvą.**

5. Kovos su sunkių formų ir organizuotu nusikalstamumu tinklo griežtinimas

Padėsime panaikinti organizuotą nusikalstamumą pasiūlydami griežtesnes kovos su organizuotais nusikaltėlių tinklais taisykles, be kita ko, susijusias su tyrimais, sumažinti ES jaunimo pažeidžiamumą dėl verbavimo vykdyti nusikalstamą veiką ir aktyviau taikyti priemones, kuriomis būtų atimta galimybė naudotis nusikaltimo įrankiais ir nusikalstamu būdu įgytu turtu.

Organizuota nusikalstama veikla vykdoma išnaudojant kintančią aplinką ir labai sparčiai plinta. Ją vykdant naudojamasi pažangiosiomis technologijomis, veikiama keliose jurisdikcijose ir palaikomi tvirti ryšiai už ES ribų. Atsižvelgiant į šias sudėtingas tarpvalstybines grėsmes, labai svarbu užtikrinti ES lygmens koordinavimą ir paramą.

Nusikalstamumo prevencija

Jaunimo verbavimas dalyvauti organizuotoje nusikalstamoje veikloje kelia vis didesnį susirūpinimą ES. Kovojant su organizuotu nusikalstamumu reikia šalinti **pagrindines jo priežastis** siūlant švietimo galimybes ir nusikalstamumo alternatyvas, laikantis visos visuomenės įtraukimo požiūrio. Komisija rems saugumo aspektų integravimą į ES švietimo, socialinę, užimtumo ir regioninę politiką. ES **skatins įrodymais grindžiamą nusikalstamumo prevencijos politiką**[60], pritaikytą prie vietos aplinkybių.

Siekiant apsaugoti internetinių paslaugų gavėjus, visų pirma nepilnamečius, nuo, *inter alia*, seksualinės prievartos prieš vaikus, prekiautojų žmonėmis ir verbavimo nusikalstamos veikos ar smurtinio ekstremizmo tikslais, pagal **Skaitmeninių paslaugų akte** nustatytas priemones reikalaujama, kad nepilnamečiams prieinamų interneto platformų paslaugų teikėjai valdytų riziką ir imtųsi veiksmų dėl neteisėto turinio, įskaitant neapykantą kurstančią kalbą. Komisija planuoja paskelbti **nepilnamečių apsaugos gaires**, kad padėtų interneto platformų paslaugų teikėjams užtikrinti aukštą nepilnamečių privatumo, saugos ir saugumo lygį internete. Gairėse

[60] https://www.eucpn.org/

bus pateiktos rekomendacijos dėl visų Sąjungoje veikiančių skaitmeninių paslaugų, kad būtų užtikrinta didesnė nepilnamečių apsauga internete. 2025 m. Komisija taip pat planuoja sudaryti palankesnes sąlygas tam, kad būtų parengtas ES **amžiaus patikros, atliekamos apsaugant privatumą**, sprendimas, užpildysiantis spragą iki tol, kol 2026 m. pabaigoje bus pasiūlyta Europos skaitmeninės tapatybės reglamente nustatyta dėklė. Komisija taip pat pateiks kovos su patyčiomis kibernetinėje erdvėje veiksmų planą.

Be to, Komisija toliau rems savanorišką įvairių suinteresuotųjų subjektų bendradarbiavimą su interneto platformomis ir kitais atitinkamais subjektais, be kita ko, pasitelkdama ES interneto forumą ir tikslinius elgesio kodeksus pagal Skaitmeninių paslaugų aktą, pavyzdžiui, 2025 m. Kovos su neapykantos kurstymu internete elgesio kodeksą. Tuo siekiama didinti informuotumą, kartu reaguoti į esamas ir atsirandančias grėsmes ir parengti gerąją grėsmių mažinimo priemonių taikymo praktiką bei ja dalytis.

Iš to, kokį poveikį organizuotas nusikalstamumas daro vietos lygmeniu, akivaizdžiai matyti, kad reikia regioninių sprendimų, kuriais būtų mažinamas pažeidžiamumas ir neteisėtos veiklos patrauklumas. Įgyvendinant ES miestų darbotvarkę bus sprendžiamos saugumo problemos miestuose, remiantis iniciatyva „ES miestai prieš radikalizaciją“. Komisija rems valstybių narių pastangas didinti miestų ir regionų saugumą pasitelkdama Europos regioninės plėtros fondą.

Tvirtesni išsilavinimo pagrindai ir įgūdžiai yra atsparios ir darnios visuomenės pagrindas. Įgyvendindama **įgūdžių sąjungą** ir **Integracijos ir įtraukties veiksmų planą**, Sąjunga sieks padėti žmonėms tapti atsparesniems klaidingai informacijai ir dezinformacijai, radikalizacijai ir verbavimui vykdyti nusikalstamą veiką.

Vaikų apsauga nuo visų formų smurto, įskaitant nusikalstamą veiką, fizinį ar psichinį smurtą internete ir realiame gyvenime, yra vienas iš pagrindinių ES tikslų. Siekdama patenkinti konkrečius ypač pažeidžiamų grupių, pavyzdžiui, vaikų, kurie vis dažniau susiduria su verbavimu ir radikalizacija, viliojimu ir seksualine prievarta prieš vaikus, patyčiomis kibernetinėje erdvėje, dezinformacija ir kitomis grėsmėmis, poreikius, ES parengs **Vaikų apsaugos nuo nusikaltimų veiksmų planą**, apimantį interneto ir neinternetinius aspektus. Jame bus nustatytas nuoseklus ir koordinuotas požiūris, grindžiamas esamomis sistemomis ir priemonėmis, įskaitant būsimą ES seksualinės prievartos prieš vaikus prevencijos ir kovos su ja centrą ir kitas ES įstaigas bei agentūras, ir bus pasiūlyti tolesni veiksmai tose srityse, kuriose likę spragų.

Nusikaltėlių tinklų ir juos įgalinančių subjektų veiklos išardymas

Būtina aktyviau kovoti su didelės rizikos nusikaltėlių tinklais, organizuoto nusikalstamumo lyderiais ir įgalinančiais subjektais. Nors pastarojo laikotarpio laimėjimai yra svarūs[61], pasenusios taisyklės ir nenuoseklios nusikaltėlių tinklų apibrėžtys trukdo veiksmingai reaguoti baudžiamosios teisenos priemonėmis ir bendradarbiauti tarpvalstybiniu mastu. Komisija peržiūrės pasenusius šios srities teisės aktus ir pasiūlys atnaujintą **kovos su organizuotu nusikalstamumu teisinę sistemą**, kad būtų sugriežtintas atsakas.

Kaip matyti iš Europos prokuratūros ir Europos kovos su sukčiavimu tarnybos (OLAF) veiklos kovojant su **tarpvalstybiniu sukčiavimu ir ES finansiniams interesams kenkiančiais nusikaltimais**, administracinis vykdymo užtikrinimas gali padėti užtikrinti greitesnius rezultatus. Sukčiautojai subsidijų srityje teikia prioritetą tokiems sektoriams kaip atsinaujinančiųjų išteklių energija, mokslinių tyrimų programos ir žemės ūkio sektorius[62]. Komisija išnagrinės būdus, kaip koordinuoti baudžiamųjų ir administracinių priemonių

[61] Įskaitant pastarojo laikotarpio EMPACT bylas.
[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

naudojimą, stiprinant bendradarbiavimą su Europolu, Eurojustu ir Europos prokuratūra. Komisija taip pat toliau rems platesnį **administracinio požiūrio** taikymą, kad vietos ir kitos administracinės institucijos galėtų sužlugdyti nusikaltėlių įsiskverbimą[63].

ES siekia stiprinti savo kovos su **korupcija** teisinę sistemą[64]. Europos Parlamentas ir Taryba turėtų skubiai užbaigti derybas dėl Komisijos pasiūlytos atnaujintos kovos su korupcija sistemos. Komisija pateiks ES kovos su korupcija strategiją, kad būtų skatinamas sąžiningumas ir stiprinamas visų atitinkamų institucijų ir suinteresuotųjų subjektų veiklos koordinavimas šioje srityje.

Šaunamieji ginklai yra vienas iš pagrindinių veiksnių, įgalinančių vis didėjantį organizuotų nusikalstamų grupių vykdomą smurtą. Komisija pasiūlys bendrus baudžiamosios teisės standartus, susijusius su neteisėta prekyba šaunamaisiais ginklais. Nauju **ES kovos su neteisėta prekyba šaunamaisiais ginklais veiksmų planu** bus siekiama apsaugoti teisėtą rinką, apriboti nusikalstamą veiklą, remiantis geresne informacijos rinkimo veikla, ir stiprinti tarptautinį bendradarbiavimą, ypatingą dėmesį skiriant Ukrainai ir Vakarų Balkanams.

Reikia priemonių neteisėtai parduodamų pirotechnikos priemonių naudojimo vykdant nusikaltimus prevencijai ir atsekamumui gerinti. Šiuo metu Komisija vertina Pirotechnikos direktyvą ir apsvarstys galimybę taikyti **baudžiamąsias sankcijas už neteisėtą prekybą pirotechnikos priemonėmis**.

Pinigų sekimas

Sekti pinigus labai svarbu kovojant su organizuotu nusikalstamumu ir terorizmu, tačiau tai daryti tebėra labai sudėtinga. Organizuotas nusikalstamumas ir pinigų srautai yra tarpusavyje susiję, todėl reikia stiprių bendrų pastangų, siekiant nutraukti nusikaltėlių tinklų prieigą prie finansavimo šaltinių ir geriau apsaugoti žmones, įmones ir valstybės biudžetus.

ES sustiprino savo pastangas priimdama naujas kovos su pinigų plovimu taisykles ir įsteigdama **ES kovos su pinigų plovimu instituciją (AMLA)**[65]. AMLA, OLAF, Europos prokuratūros, Eurojusto ir Europolo bendradarbiavimas yra labai svarbus siekiant atlikti veiksmingus finansinius tyrimus. Komisija rems **partnerystės susitarimų –** tiek tų, kuriais palengvinamas tarpžinybinis bendradarbiavimas, tiek ir tų, kuriuos įgyvendinant dalyvauja privatusis sektorius, – sudarymą.

Siekiant pašalinti organizuoto nusikalstamumo finansinius motyvus, labai svarbu areštuoti turtą ir konfiskuoti nusikalstamu būdu įgytas pajamas. Valstybės narės turėtų nedelsdamos perkelti į nacionalinę teisę neseniai priimtas griežtesnes **turto susigrąžinimo ir konfiskavimo** taisykles[66] ir jas taikyti išnaudodamos visą jų potencialą. Kovojant su lygiagrečiomis finansų sistemomis, kuriomis apeinama ES kovos su pinigų plovimu sistema, įskaitant kriptografija grindžiamas sistemas, taip pat reikia imtis novatoriškų veiksmų, valstybės narės turi dalytis geriausios praktikos pavyzdžiais ir būtina didesnė Europolo ir Eurojusto parama. Komisija išnagrinės galimybes sukurti naują ES masto sistemą, skirtą organizuoto nusikalstamumo pelnui ir teroristų finansavimui sekti, ir skatins laiku vykdomus išplėstinės informacijos srautus

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf

[64] Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl kovos su korupcija, kuria pakeičiamas Tarybos pamatinis sprendimas 2003/568/TVR ir Konvencija dėl kovos su korupcija, susijusia su Europos Bendrijų pareigūnais ar Europos Sąjungos valstybių narių pareigūnais, ir iš dalies keičiama Europos Parlamento ir Tarybos direktyva (ES) 2017/1371, COM(2023) 234 *final*, Briuselis, 2023 5 3.

[65] ttps://www.amla.europa.eu/index_en?prefLang=lt

[66] 2024 m. balandžio 24 d. Europos Parlamento ir Tarybos direktyva (ES) 2024/1260 dėl turto susigrąžinimo ir konfiskavimo, OL L, 2024/1260, 2024 5 2.

iš **finansinės žvalgybos padalinių** į teisėsaugos institucijas. Komisija ieškos būdų, kaip pašalinti spragas, padės valstybėms narėms stiprinti gebėjimus ir toliau sieks stiprinti bendradarbiavimą su trečiosiomis šalimis, kuriomis nusikaltėliai piktnaudžiauja vykdydami pogrindinės bankininkystės operacijas.

Kova su sunkiais nusikaltimais

Kovojant su sunkiais nusikaltimais reikia ne tik išardyti nusikaltėlių tinklus, bet ir telkti tikslingas pastangas. Siekdama sustiprinti mūsų gebėjimą kovoti su **sukčiavimu internete**, darančiu labai didelę finansinę žalą[67], Komisija rems prevencines priemones ir veiksmingesnius teisėsaugos veiksmus ir bendradarbiaus su valstybėmis narėmis ir suinteresuotaisiais subjektais, siekdama, kad būtų užtikrinta parama aukoms ir jų apsauga, be kita ko, padedant aukoms susigrąžinti savo lėšas. Šios pastangos bus oficialiai įtvirtintos **Kovos su sukčiavimu internete veiksmų plane**.

Remdamasi 2020–2025 m. ES kovos su **seksualine prievarta prieš vaikus** strategija[68], Komisija padės teisėkūros institucijoms užbaigti rengti du pasiūlymus dėl teisėkūros procedūra priimamų aktų[69], kuriais siekiama užkirsti kelią seksualinei prievartai prieš vaikus internete ir su ja kovoti bei užtikrinti, kad teisėsaugos veiksmai kovojant su seksualine prievarta prieš vaikus ir jų išnaudojimu būtų veiksmingesni. Kadangi laikinosios taisyklės galioja iki 2026 m. balandžio mėn., labai svarbu sukurti nuolatinę teisinę sistemą, tad Komisija ragina teisėkūros institucijas pradėti derybas dėl reglamento, kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės, projekto. Teisėkūros institucijų taip pat prašoma daryti pažangą derantis dėl Direktyvos dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir seksualinės prievartos prieš vaikus medžiaga – šia direktyva bus nustatytos būtiniausios taisyklės dėl nusikalstamų veikų apibrėžties ir sankcijų kovos su seksualiniu vaikų išnaudojimu srityje.

Pusė pavojingiausių ES nusikaltėlių tinklų dalyvauja smurtinėje **prekyboje narkotikais**. Nors ES neseniai sustiprino kovą su šia nusikalstama veika[70], visų pirma išplėsdama **ES narkotikų agentūros** įgaliojimus, būtina imtis tolesnių veiksmų. Komisija glaudžiai bendradarbiaus su valstybėmis narėmis, kad pasiūlytų naują **ES kovos su narkotikais strategiją**. Ji taip pat peržiūrės **narkotinių ir psichotropinių medžiagų pirmtakų (prekursorių) teisinę sistemą** ir pasiūlys **ES kovos su prekyba narkotikais veiksmų planą**, kad būtų suardyti maršrutai ir verslo modeliai. **ES uostų aljanso viešojo ir privačiojo sektorių** sustiprintos uostų apsaugos **partnerystė** bus išplėsta siekiant įtraukti mažesnius ir vidaus vandenų uostus ir užtikrinti, kad būtų laikomasi jūrų saugumo taisyklių. Pripažindama didelį prekybos narkotikais poveikį vietos lygmeniu, Komisija toliau rems subalansuotą, įrodymais pagrįstą ir daugiadalykę kovos su narkotikais politiką, kad būtume pasirengę reaguoti į staigų narkotikų, ypač sintetinių opioidų, antplūdį.

Siekdama kovoti su žmonių išnaudojimu, ES patvirtino naujas taisykles[71] ir priims **atnaujintą** 2026–2030 m. **ES kovos su prekyba žmonėmis strategiją**, apimsiančią visus etapus nuo prevencijos iki baudžiamojo persekiojimo, daugiausia dėmesio skirdama paramai aukoms tiek ES, tiek tarptautiniu lygmeniu.

[67] Global Anti-Scam Report 2024 (2024 m. Pasaulinė kovos su sukčiavimu ataskaita).
[68] COM (2020) 607 *final*.
[69] COM(2022) 209 *final* ir COM(2024) 60 *final*.
[70] COM(2023) 641 *final*.
[71] 2024 m. birželio 13 d. Direktyva (ES) 2024/1712, kuria iš dalies keičiama Direktyva 2011/36/ES dėl prekybos žmonėmis prevencijos, kovos su ja ir aukų apsaugos, OL L, 2024/1712, 2024 6 24.

Komisija kartu su pagrindiniais partneriais vadovaus kovai su **neteisėtu migrantų gabenimu** per naująjį Pasaulinį kovos su neteisėtu migrantų gabenimu aljansą, bendradarbiaudama su Europolu, Eurojustu ir FRONTEX, įskaitant ir interneto aspektą. Komisijos pasiūlymai dėl kovos su neteisėtu migrantų gabenimu[72] turėtų būti nedelsiant priimti ir įgyvendinti. Be to, priėmus **vežėjams skirtą priemonių rinkinį**[73], Komisija aktyviau bendravo su užsienio institucijomis ir veiklos vykdytojais, taip pat ji toliau bendradarbiaus su aviacijos pramone ir civilinės aviacijos organizacijomis[74] siekdama didinti informuotumą apie neteisėtą migrantų gabenimą oro transportu[75].

Nusikaltimai aplinkai ilguoju laikotarpiu kelia grėsmę aplinkai, visuomenės sveikatai ir ekonomikai. Komisija padės valstybėms narėms įgyvendinti Direktyvą dėl nusikaltimų aplinkai[76] ir rems šios srities operatyvinius tinklus ir veiksmus[77]. Labai svarbu griežtai užtikrinti jų vykdymą. Be to, neseniai priimta Europos Tarybos konvencija dėl aplinkos apsaugos pagal baudžiamąją teisę[78] padės užtikrinti tvirtas ir panašias pastangas kovoti su nusikaltimais aplinkai tiek Europoje, tiek už jos ribų.

Atsakas baudžiamosios teisenos srityje

Nusikalstamumas ir terorizmas gali daryti poveikį visiems, todėl būtina remti ir apsaugoti **aukų** teises, kad būtų sumažinta žala ir padidintas bendras saugumas bei pasitikėjimas institucijomis. Remdamasi Nusikaltimų aukų teisių direktyva, Komisija pateiks naują **ES strategiją dėl nusikaltimų aukų teisių**.

ES baudžiamosios teisenos sistemoms reikia veiksmingų priemonių kylančioms grėsmėms šalinti. Siekdama šio tikslo, Komisija įsteigė **Aukšto lygio forumą ES baudžiamosios teisenos ateities klausimais**. Šiame forume dalyvauja valstybės narės, Europos Parlamentas, ES agentūros ir įstaigos bei kiti atitinkami suinteresuotieji subjektai. Jo tikslas – aptarti būdus, kaip užtikrinti, kad mūsų baudžiamosios teisenos sistemos išliktų veiksmingos, teisingos ir atsparios kintant iššūkiams, kartu stiprinant teisminį bendradarbiavimą ir tarpusavio pasitikėjimą, be kita ko, pasitelkiant skaitmenizaciją[79].

Pagrindiniai veiksmai

Komisija:

- **2026 m. pateiks pasiūlymą dėl teisėkūros procedūra priimamo akto dėl modernizuotų kovos su organizuotu nusikalstamumu taisyklių;**
- **2025 m. pateiks pasiūlymą dėl teisėkūros procedūra priimamo akto dėl narkotinių ir psichotropinių medžiagų pirmtakų (prekursorių) teisinės sistemos peržiūros;**

[72] COM(2023) 755 *final* ir COM(2023) 754 *final*.
[73] Priemonių rinkinys, susijęs su komercinių transporto priemonių naudojimu siekiant palengvinti neteisėtą migraciją į ES.
[74] Įskaitant Tarptautinę civilinės aviacijos organizaciją (ICAO).
[75] Komisija taip pat padės užbaigti rengti Reglamentą dėl priemonių, taikomų vežėjams, padedantiems prekiauti žmonėmis ar neteisėtai gabenti migrantus arba užsiimantiems tokia veikla, COM(2021) 753 *final*.
[76] 2024 m. balandžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2024/1203 dėl aplinkos apsaugos baudžiamosios teisės priemonėmis, OL L, 2024/1203, 2024 4 30.
[77] ES aplinkos apsaugos teisės aktų įgyvendinimo ir vykdymo užtikrinimo tinklą (IMPEL tinklas), Europos aplinkos prokurorų tinklą (ENPE), „EnviCrimeNet“ tinklą ir ES aplinkos teisėjų forumą.
[78] *Committee of experts on the protection of the environment through Criminal Law (PC-ENV) - European Committee on Crime Problems* (Aplinkos apsaugos pagal baudžiamąją teisę ekspertų komitetas – Europos nusikalstamumo problemų komitetas).
[79] Visų pirma sukuriant Ryšių palaikymo e. teisingumo srityje keičiantis duomenimis internetu sistemą (eCODEX) ir Centralizuotą valstybių narių, turinčių informacijos apie priimtus trečiųjų šalių piliečių arba asmenų be pilietybės apkaltinamuosius nuosprendžius, nustatymo sistemą (ECRIS-TCN).

- **2025 m. pateiks pasiūlymą dėl teisėkūros procedūra priimamo akto dėl bendrų baudžiamosios teisės standartų, susijusių su neteisėta prekyba šaunamaisiais ginklais;**
- **įvertins poreikį peržiūrėti direktyvas dėl pirotechnikos ir civiliniam naudojimui skirtų sprogmenų;**
- **įvertins poreikį dar labiau sustiprinti Europos tyrimo orderį ir Europos arešto orderį;**
- **2026 m. pateiks naują ES kovos su prekyba žmonėmis strategiją;**
- **2026 m. pateiks naują ES strategiją dėl nusikaltimų aukų teisių;**
- **iki 2027 m. pateiks ES vaikų apsaugos nuo nusikaltimų veiksmų planą;**
- **2025 m. pateiks ES kovos su prekyba narkotikais veiksmų planą;**
- **2026 m. pateiks ES kovos su neteisėta prekyba šaunamaisiais ginklais veiksmų planą;**
- **nuo 2025 m. nuosekliai plės ES uostų aljansą;**
- **2026 m. priims Skaitmeninių paslaugų akto gaires dėl nepilnamečių apsaugos;**
- **2026 m. pateiks ES kovos su patyčiomis kibernetinėje erdvėje veiksmų planą.**

Valstybės narės primygtinai raginamos:

- **iki 2026 m. pabaigos visiškai perkelti į nacionalinę teisę naujas turto susigrąžinimo ir konfiskavimo taisykles ir pradėti jas taikyti išnaudojant visą jų potencialą;**
- **įgyvendinti administracinį požiūrį kovojant su nusikaltėlių įsiskverbimu;**
- **sudaryti viešojo ir privačiojo sektorių kovos su pinigų plovimu partnerystės susitarimus;**
- **perkelti į nacionalinę teisę ir visapusiškai įgyvendinti Direktyvą dėl smurto prieš moteris ir smurto artimoje aplinkoje prevencijos ir kovos su juo.**

Europos Parlamentas ir Taryba primygtinai raginami:

- **daryti pažangą derybose dėl Reglamento, kuriuo nustatomos seksualinės prievartos prieš vaikus prevencijos ir kovos su ja taisyklės, ir Direktyvos dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir seksualinės prievartos prieš vaikus medžiaga;**
- **užbaigti derybas dėl Direktyvos dėl kovos su korupcija.**

6. Kova su terorizmu ir smurtiniu ekstremizmu

Nustatysime išsamią kovos su terorizmu darbotvarkę, kad būtų užkirstas kelias radikalizacijai, užtikrintas internetinės ir viešųjų erdvių saugumas, užkirsta prieiga prie finansavimo kanalų ir reaguojama į išpuolius, kai tik jie įvyksta.

Terorizmo grėsmės lygis ES tebėra aukštas. Jis yra glaudžiai susijęs su šalutiniu geopolitinių įvykių, naujų technologijų ir naujų teroristų finansavimo priemonių poveikiu. Turime užtikrinti, kad ES būtų gerai pasirengusi numatyti grėsmes, užkirsti kelią radikalizacijai (tiek realiame gyvenime, tiek internete), apsaugoti piliečius ir viešąsias erdves nuo išpuolių ir veiksmingai reaguoti į išpuolius, kai tik jie įvyksta. 2025 m. bus pateikta nauja **ES terorizmo ir smurtinio ekstremizmo prevencijos ir kovos su jais darbotvarkė**, kurioje turi būti išdėstyti būsimi ES veiksmai. Pagal naująją darbotvarkę ES ir Vakarų Balkanai 2025 m. pasirašys naują terorizmo ir smurtinio ekstremizmo prevencijos ir kovos su jais **bendrą veiksmų planą**.

Radikalizacijos prevencija ir žmonių apsauga internete

Panašiai kaip kova su organizuotu nusikalstamumu, kova su terorizmu ir smurtiniu ekstremizmu prasideda nuo **pagrindinių jo priežasčių šalinimo**. **ES radikalizacijos prevencijos žinių centras** padidins savo paramą specialistams ir politikos formuotojams, pateikdamas jiems naują **išsamų prevencijos priemonių rinkinį**, kad būtų galima anksti nustatyti radikalizacijos pastangas, didžiausią dėmesį skiriant pažeidžiamiausiems asmenims, visų pirma nepilnamečiams, ir imtis intervencinių veiksmų. Radikalizacija dažnai vyksta kalėjimuose, tad siekdama padėti valstybėms narėms spręsti šį klausimą, Komisija pateiks naujų rekomendacijų.

Teroristai ir smurtiniai ekstremistai naudojasi interneto platformomis, kad skleistų teroristinį ir žalingą turinį, rinktų lėšas ir verbuotų. Pažeidžiami naudotojai, visų pirma nepilnamečiai, radikalizuojami internete nerimą keliančiu tempu. **Reglamentas dėl teroristinio turinio internete** padėjo kovoti su teroristinio turinio sklaida internete ir sudarė sąlygas greitai šalinti žiauriausią ir pavojingiausią medžiagą[80]. Šiuo metu Komisija atlieka jo veikimo vertinimą ir nustatys, kaip geriausiai būtų galima šią sistemą sustiprinti.

ES krizių protokolas, pagal kurį teisėsaugos institucijos ir technologijų pramonė gali bendrai ir greitai reaguoti į teroristinius išpuolius, bus iš dalies pakeistas, siekiant užtikrinti išplečiamumą ir lankstumą, kad būtų galima reaguoti į didėjantį teroristinių išpuolių internetinį aspektą. ES interneto forumas ir toliau bus pagrindinis būdas savanoriškai bendradarbiauti su technologijų pramone kovojant su teroristiniu ir žalingu turiniu internete. Be to, Komisija dalyvauja tarptautinėse iniciatyvose, pavyzdžiui, Kraistčerčo raginimo fondo veikloje ir Pasauliniame kovos su terorizmu interneto forume.

Kova su terorizmo finansavimu

Teroristai finansuoja savo veiklą rengdami sutelktinio finansavimo kampanijas ir naudodami kriptoturtą ir neobankus arba internetines mokėjimo platformas. Teisėsaugos institucijos turi nustatyti ir ištirti šiuos finansinius srautus. Tam reikia išteklių, priemonių ir ekspertinių žinių. **Kovos su terorizmu finansinių tyrėjų tinklas** atlieka labai svarbų vaidmenį. Komisija išnagrinės galimybę sukurti **naują ES masto teroristų finansavimo sekimo sistemą**, kuri apimtų ES vidaus ir SEPA operacijas, kriptoturto pervedimus, internetinius ir elektroninius mokėjimus ir papildytų ES ir JAV susitarimą dėl Terorizmo finansavimo sekimo programos (TFSP).

ES biudžetas turi būti **apsaugotas nuo netinkamo naudojimo siekiant skatinti radikalias ir (arba) ekstremistines pažiūras** valstybėse narėse. Į persvarstytą **Finansinį reglamentą** dabar įtraukti apkaltinamieji nuosprendžiai dėl diskriminacijos, neapykantos ar smurto kurstymo kaip pagrindas neskirti ES finansavimo. Komisija toliau ieškos geriausių būdų visapusiškai pasinaudoti priemonių rinkiniu, be kita ko, atrinkdama galimus paramos gavėjus. ES biudžeto apsauga taip pat grindžiama tvirtu bendradarbiavimu ir dalijimusi informacija su nacionalinėmis valdžios institucijomis, ES agentūromis ir įstaigomis.

Apsauga nuo išpuolių

Svarbus piliečių apsaugos elementas yra ne tik investicijos į radikalizacijos prevenciją, bet ir teroristų bei nusikaltėlių galimybių vykdyti išpuolius ribojimas. Reikia imtis veiksmų tiek dėl teroristų naudojamų priemonių, tiek siekiant apsaugoti taikinius, kuriems gresia išpuolis.

[80] Iki 2024 m. gruodžio 31 d. buvo išduoti 1 426 nurodymai pašalinti teroristinį turinį arba blokuoti prieigą prie jo, kurių didžioji dauguma nukreipta ne tik prieš džihadistų teroristinį turinį, bet ir prieš dešiniųjų pažiūrų teroristinį turinį.

Komisija ne tik imsis veiksmų, susijusių su šaunamaisiais ginklais, bet ir **peržiūrės taisykles** dėl **sprogstamųjų medžiagų pirmtakų**, kad jos būtų taikomos ir labai pavojingoms cheminėms medžiagoms. **Viešosios erdvės** tebėra dažniausi teroristinių išpuolių taikiniai, ypač pavieniui veikiantiems teroristams. Siekiant apsaugoti piliečius nuo žalos, bus sustiprinta **ES patarėjų saugumo klausimais programa**, pagal kurią valstybių narių prašymu būtų galima atlikti viešųjų erdvių, ypatingos svarbos infrastruktūros objektų ir didelės rizikos renginių pažeidžiamumo vertinimus, ir ji bus finansuojama Vidaus saugumo fondui asignuotomis ES biudžeto lėšomis. ES sieks padidinti turimą viešųjų erdvių apsaugos finansavimą. Komisija teikia paramą valstybių narių institucijoms ir privatiems veiklos vykdytojams, pasitelkdama specialias gaires ir priemones, pavyzdžiui, **Viešųjų erdvių apsaugos žinių centrą**[81], ir nuo 2020 m. viešųjų erdvių apsaugai remti jau skyrė 70 mln. EUR.

Komisija, bendradarbiaudama su vietos valdžios institucijomis ir privačiais partneriais, taip pat išnagrinės galimybę nustatyti reikalavimus organizacijoms apsvarstyti galimybę taikyti arba taikyti saugumo priemones viešai prieinamose vietose.

Atsižvelgiant į akivaizdų pažeidžiamumą, Komisijos veiksmai žydų bendruomenės apsaugos srityje ir toliau bus grindžiami **2021–2030 m. ES kovos su antisemitizmu ir žydų gyvenimo puoselėjimo strategija**. Komisija taip pat užtikrins, kad būtų įdiegtos tinkamos priemonės, skirtos padėti valstybėms narėms **kovoti su neapykanta musulmonams**.

Bepiločių orlaivių naudojimas šnipinėjimo ir išpuolių vykdymo tikslais tampa vis didesniu saugumo iššūkiu. Komisija parengs **suderintą kovos su bepiločiais orlaiviais sistemų bandymo metodiką**, įsteigs **kovos su bepiločiais orlaiviais kompetencijos centrą** ir įvertins poreikį suderinti valstybių narių įstatymus ir procedūras[82].

Užsienio teroristai kovotojai

Kad būtų galima nustatyti grįžtančius arba atvykstančius prie ES išorės sienų užsienio teroristus kovotojus, reikia duomenų apie terorizmo grėsmę keliančius asmenis. Šiuo tikslu Komisija kartu su Europolu stiprins savo **bendradarbiavimą su pagrindinėmis trečiosiomis šalimis, kad gautų biografinius ir biometrinius duomenis apie asmenis, galinčius kelti terorizmo grėsmę**, įskaitant užsienio teroristus kovotojus, kurie vėliau gali būti įtraukti į Šengeno informacinę sistemą, visapusiškai laikantis taikytinų ES ir nacionalinių teisinių sistemų. Todėl labai svarbu, kad valstybės narės naudotųsi visomis esamomis priemonėmis. Tai apima visos svarbios informacijos įtraukimą į **SIS**, biometrinių patikrų tobulinimą ir privalomus sistemingus visų asmenų patikrinimus prie ES išorės sienų[83]. Be to, FRONTEX parengti **bendri rizikos rodikliai** ir toliau padės valstybių narių sienų kontrolės institucijoms nustatyti ir įvertinti galimų užsienio teroristų kovotojų įtartinų kelionių riziką.

Be to, siekdama užtikrinti, kad valstybės narės ir toliau turėtų prieigą prie **kovos lauko įrodymų**, kuriuos surinko JT tyrimų grupė atsakomybei už „Da'esh“ / ISIL įvykdytus nusikaltimus skatinti (UNITAD) užsienio teroristų kovotojų baudžiamojo persekiojimo tikslais, Komisija kartu su Eurojustu įvertins galimybę saugoti šiuos įrodymus Eurojusto sunkiausių tarptautinių nusikaltimų įrodymų duomenų bazėje. Be to, naujasis Europos **teisminis kovos su terorizmu registras** ir toliau padės valstybių narių teisminėms institucijoms greitai nustatyti tarpvalstybines sąsajas terorizmo bylose.

Pagrindiniai veiksmai

[81] Viešųjų erdvių apsaugos žinių centras.
[82] Atsižvelgiant į 2023 m. Komunikate dėl kovos su bepiločiais orlaiviais (COM(2023) 659 *final*) nustatytus pagrindinius veiksmus, COM(2023) 659 *final*.
[83] Visapusiškai laikantis Šengeno sienų kodekso ir Tikrinimo reglamento.

Komisija:

- **2025 m. priims naują ES terorizmo ir smurtinio ekstremizmo prevencijos ir kovos su jais darbotvarkę;**
- **2025 m. su Vakarų Balkanais pasirašys naują terorizmo ir smurtinio ekstremizmo prevencijos ir kovos su jais bendrą veiksmų planą;**
- **kartu su ES žinių centru parengs naują išsamų prevencijos priemonių rinkinį;**
- **2026 m. įvertins Reglamento dėl teroristinio turinio internete taikymą;**
- **2025 m. iš dalies pakeis ES krizių protokolą;**
- **2026 m. pateiks pasiūlymą dėl teisėkūros procedūra priimamo akto dėl Reglamento dėl prekybos sprogstamųjų medžiagų pirmtakais ir jų naudojimo peržiūros;**
- **išnagrinės galimybę sukurti naują ES masto teroristų finansavimo sekimo sistemą.**

Valstybės narės primygtinai raginamos:

- **patobulinti biometrines patikras ir vykdyti privalomus sistemingus patikrinimus prie ES išorės sienų;**
- **visapusiškai naudotis Europos teisminiu kovos su terorizmu registru.**

7. ES – stipri pasaulinė veikėja saugumo srityje

Siekdami sustiprinti ES saugumą, didinsime operatyvinį bendradarbiavimą plėtodami partnerystės ryšius su pagrindiniais regionais, pavyzdžiui, plėtros ir kaimynystės partneriais, Lotynų Amerika ir Vidužemio jūros regionu. Vykdant tarptautinį bendradarbiavimą bus atsižvelgiama į ES saugumo interesus, be kita ko, pasinaudojant ES priemonėmis.

Pastaraisiais metais paaiškėjo, kad ES išorės ir vidaus saugumas yra glaudžiai susijęs. Rusijos agresijos karas prieš Ukrainą, konfliktas Gazoje, padėtis Sirijoje ir visame pasaulyje kylantys konfliktai padarė didelį šalutinį poveikį ES vidaus saugumui. Kad galėtų kovoti su pasaulinio nestabilumo poveikiu vidaus saugumui, **ES turi aktyviai ginti savo saugumo interesus** šalindama išorės grėsmes, suardydama neteisėtos prekybos maršrutus ir užtikrindama strateginės svarbos koridorių, pavyzdžiui, prekybos maršrutų, apsaugą. Be to, ES toliau bus tvirta šalių partnerių sąjungininkė, siekdama su jomis išvien didinti pasaulinį saugumą ir abipusį atsparumą grėsmėms.

Pastaraisiais metais ES ėmėsi svarbių veiksmų, kad sustiprintų bendradarbiavimą saugumo srityje. ES yra sudariusi operatyvinius teisėsaugos ir teisminio bendradarbiavimo susitarimus, taip pat kitų rūšių susitarimus su šalimis partnerėmis. ES aktyviai siekia sudaryti papildomus tarptautinius susitarimus, atitinkančius Tarybos derybinius nurodymus, ir imtis gebėjimų stiprinimo iniciatyvų, įgyvendinamų padedant ES agentūroms ir įstaigoms. KVTBP „Globali Europa“ taip pat yra labai svarbi stiprinant saugumą su šalimis partnerėmis.

Taisyklėmis grindžiama tarptautinė tvarka yra pasaulinio saugumo stiprinimo pagrindas. Dialogai saugumo klausimais, įskaitant teminius dialogus, yra labai svarbūs stiprinant šias pastangas. **Saugumo ir gynybos strateginio kelrodžio** įgyvendinimas kartu su dvišalio ir daugiašalio bendradarbiavimo sistemomis, pavyzdžiui, stabilizacijos ir asociacijos susitarimais ir asociacijos susitarimais, ir bendradarbiavimas su tokiomis organizacijomis kaip JT ir NATO yra labai svarbūs ieškant veiksmingų saugumo sprendimų. ES toliau atliks savo vaidmenį

tarptautiniuose forumuose[84] ir stiprins bendradarbiavimą su atitinkamomis tarptautinėmis ir regioninėmis organizacijomis bei struktūromis, įskaitant NATO, Jungtines Tautas, Europos Tarybą, Interpolą, G7, ESBO ir pilietinę visuomenę.

Regioninis bendradarbiavimas

Prioritetine tvarka toliau teikti tvirtą ES paramą **Ukrainai** ir stiprinti **ES plėtros šalių** saugumą ir atsparumą yra politinė ir geostrateginė būtinybė. Remiant ES saugumą kartu turėtų būti **spartinama šalių kandidačių integracija** į **ES saugumo architektūrą** ir stiprinamas jų regioninis bendradarbiavimas. Komisija pasitelks ES plėtros politiką, kad paremtų ES šalių kandidačių ir potencialių šalių kandidačių pajėgumus reaguoti į grėsmes, stiprintų operatyvinį bendradarbiavimą ir keitimąsi informacija ir užtikrintų suderinamumą su ES principais, teisės aktais ir priemonėmis. Pasirengimo narystei paramos priemonė (PNPP III), taip pat Ukrainos, Moldovos ir Vakarų Balkanų priemonės yra labai svarbios stiprinant saugumą tiek šalyse kandidatėse, tiek potencialiose kandidatėse.

ES taip pat toliau integruos **kaimynines šalis partneres** į ES saugumo architektūrą. Įgyvendindama naują **Vidužemio jūros regiono paktą** ir būsimą **strateginį požiūrį į Juodąją jūrą**, Sąjunga sieks toliau plėtoti regioninį bendradarbiavimą ir dvišalės visapusiškos strateginės partnerystės ryšius, apimančius saugumo aspektą, kai tai aktualu, reguliariai rengdama aukšto lygio dialogus saugumo klausimais. Bus sustiprintas operatyvinis bendradarbiavimas su Šiaurės Afrika, **Artimaisiais Rytais ir Persijos įlanka**, visų pirma kovos su terorizmu, pinigų plovimu, neteisėta prekyba šaunamaisiais ginklais ir narkotikų, visų pirma kaptagono, gamyba ir neteisėta prekyba srityse.

Siekdama kovoti su plintančia teroristine ir nusikalstama veikla ir jos galimu poveikiu **Užsachario Afrikoje, visų pirma Sahelyje, Somalio pusiasalyje ir Vakarų Afrikoje**, ES stiprins paramą Afrikos Sąjungai, regioninėms ekonominėms bendrijoms (REB) ir regiono šalims. Vadovaudamasi ES jūrų saugumo strategija[85], ES stiprins bendradarbiavimą **Gvinėjos įlankoje, Raudonojoje jūroje ir Indijos vandenyne**, kad būtų kovojama su neteisėta prekyba ir piratavimu, remdama Afrikos vidaus ir regioninį bendradarbiavimą, įgyvendindama ES koordinuoto buvimo jūroje (CMP) koncepciją ir pasitelkdama Jūrų analizės ir operacijų centrą kovai su prekyba narkotikais (MAOC-N).

ES stiprins operatyvinį bendradarbiavimą su **Lotynų Amerika ir Karibų jūros regionu**, kad būtų išardyti didelės rizikos nusikaltėlių tinklai ir nusikaltėliai būtų patraukti baudžiamojon atsakomybėn, sužlugdyta neteisėta veikla ir išardyti neteisėtos prekybos maršrutai, stiprindama bendradarbiavimo sistemas, pavyzdžiui, ES ir CLASI (Lotynų Amerikos vidaus saugumo komitetas) ir ES ir CELAC koordinavimo ir bendradarbiavimo kovos su narkotikais srityje mechanizmą. Tarp prioritetų bus logistikos centrų atsparumo didinimas, partnerystės ryšių užmezgimas ir pinigų stebėjimo metodai. ES toliau rems Šiaurės ir Pietų Amerikos policijos bendruomenės (AMERIPOL) plėtrą, kad ji taptų Europolo regioniniu ekvivalentu, ir stiprins valstybių narių ir regiono teisminį bendradarbiavimą. ES taip pat bendradarbiaus su **Pietų ir Vidurine Azija** sprendžiant bendras saugumo problemas, susijusias su terorizmu, prekyba neteisėtomis prekėmis, įskaitant narkotikus, prekyba žmonėmis ir neteisėtu migrantų gabenimu.

Be to, ES rems regioninio bendradarbiavimo sistemas trečiosiose šalyse, siekdama toliau padėti joms stabdyti neteisėtą prekybą jos atsiradimo vietoje, laikantis bendros atsakomybės už visą

[84] Pasauliniame kovos su terorizmu forume, Pasaulinėje kovos su „Da'esh“ koalicijoje, Pasauliniame kovos su terorizmu interneto forume, Kraistčerčo raginimo fonde, Pasaulinėje koalicijoje su sintetiniais narkotikais susijusioms grėsmėms šalinti.
[85] JOIN(2023) 8 *final*.

nusikalstamą tiekimo grandinę principo. ES taip pat padės stiprinti logistikos centrų saugumą užsienyje, koordinuodama **bendrus patikrinimus trečiųjų šalių uostuose**.

Operatyvinis bendradarbiavimas

Strategija „Global Gateway“ bus remiami tvarūs ir aukštos kokybės infrastruktūros projektai skaitmeniniame, klimato ir energetikos, transporto, sveikatos, švietimo ir mokslinių tyrimų sektoriuose. Nuo šiol Komisija, kai aktualu, į būsimas investicijas pagal strategiją „Global Gateway“ įtrauks saugumo aspektus. Tai, be kita ko, bus iniciatyvos, kurios yra itin svarbios ES ir jos šalių partnerių strateginiam savarankiškumui, pavyzdžiui, infrastruktūros projektai, apimantys saugumo vertinimus ir rizikos mažinimo priemones.

Komisija sieks tolesnių **ES ir trečiųjų šalių susitarimų dėl bendradarbiavimo su Europolu ir Eurojustu**, visų pirma su Lotynų Amerikos šalimis.

Be to, aktyvus ES nepriklausančių šalių dalyvavimas **EMPACT** yra viena iš veiksmingiausių operatyvinio bendradarbiavimo stiprinimo priemonių. ES toliau skatins trečiųjų šalių, visų pirma Vakarų Balkanų, rytinių kaimyninių šalių, Užsacharo Afrikos, Šiaurės Afrikos, Artimųjų Rytų, Lotynų Amerikos ir Karibų jūros regiono šalių, dalyvavimą šioje sistemoje. Dar viena bendradarbiavimo su trečiosiomis šalimis kovos su nusikalstamumu srityje stiprinimo priemonė yra Europolo koordinuojamos valstybių narių operatyvinės darbo grupės, kurių veikloje gali dalyvauti trečiosios šalys. Komisija taip pat siekia užbaigti derybas dėl **ES ir Interpolo** tarptautinio susitarimo[86], užtikrindama vienodesnį požiūrį į pasaulines grėsmes saugumui ir kovą su tarpvalstybiniais nusikaltimais.

Sąjunga turi imtis veiksmų vietoje, laikydamasi Europos komandos požiūrio. Sąjungos ir valstybių narių specialistai atlieka labai svarbų vaidmenį užtikrinant, kad Sąjungos išorės veiksmai būtų tinkamai pagrįsti, koordinuojami ir operatyvūs. Siekdama šį požiūrį perkelti į kitą lygmenį, Komisija, padedama vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai, stiprins **ryšių palaikymo tinklus** ir palengvins regioninių **Europolo ir Eurojusto ryšių palaikymo pareigūnų** dislokavimą, atsižvelgdama į valstybių narių operatyvinius poreikius.

ES sieks glaudesnio operatyvinio teisėsaugos ir teisminio bendradarbiavimo, skatins keistis informacija tikruoju laiku ir rengti bendras operacijas per **jungtines tyrimo grupes** trečiosiose šalyse, padedant Europolui ir Eurojustui. Komisija taip pat padės valstybėms narėms steigti **bendrus analizės ir informavimo centrus**, kuriuose dalyvautų ekspertai ir vietos teisėsaugos institucijos strateginėse trečiosiose šalyse.

Bendros užsienio ir saugumo politikos (BUSP) priemonės

Bendros saugumo ir gynybos politikos (BSGP) misijos taip pat bus visapusiškai išnaudojamos siekiant geriau nustatyti išorės grėsmes ES vidaus saugumui ir su jomis kovoti, laikantis Tarybos nustatytų jų įgaliojimų. Kad būtų stiprinami trečiųjų šalių pajėgumai, vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai ir Komisija rems BSGP veiksmus specialiomis finansavimo priemonėmis ir išnagrinės visus tinkamus finansavimo būdus.

ES ribojamosios priemonės yra patikima BUSP priemonė, taip pat naudojama kovojant su terorizmu. Remdamasi vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai, valstybių narių arba Komisijos pasiūlymais, Taryba galėtų įvertinti, kaip būtų galima pasiekti, kad ES autonominės ribojamosios priemonės (ES teroristų sąrašas) taptų veiksmingesnės,

[86] 2021 m. liepos 19 d. Tarybos sprendimas (ES) 2021/1312 ir 2021 m. liepos 19 d. Tarybos sprendimas (ES) 2021/1313.

operatyvesnės ir lankstesnės. Be to, jie galėtų apsvarstyti galimybę išnagrinėti papildomas ribojamąsias priemones, nukreiptas prieš nusikaltėlių tinklus, atsižvelgiant į BUSP tikslus.

Vizų politika ir keitimasis informacija

ES vizų politika yra labai svarbi priemonė, skirta bendradarbiauti su trečiosiomis šalimis ir mūsų sienoms apsaugoti, kontroliuojant atvykimą į ES ir nustatant jo sąlygas. Komisija visapusiškai integruos **saugumo aspektus į ES vizų politiką** įgyvendindama būsimą ES vizų politikos strategiją. Komisija bendradarbiaus su teisėkūros institucijomis, kad būtų priimtas pasiūlymas peržiūrėti ir supaprastinti bevizio režimo sustabdymo mechanizmą, visų pirma konkrečiais piktnaudžiavimo beviziu režimu atvejais[87]. Trečiosios šalys bus skatinamos dalytis informacija apie asmenis, galinčius kelti grėsmę saugumui, ir ši informacija bus įvedama į ES informacines sistemas ir duomenų bazes.

Siekdama užtikrinti politikos koordinavimą ir pradinės grandies veiksmus, kuriais skatinamas veiksmingesnis, greitesnis ir sklandesnis bendradarbiavimas, Komisija atliks darbą, kad būtų nustatyta **duomenų srauto tvarka**, ir ieškos būdų, kaip teisėsaugos ir sienų valdymo tikslais **stiprinti keitimąsi informacija** su patikimomis trečiosiomis šalimis, laikantis pagrindinių teisių ir duomenų apsaugos taisyklių.

Pagrindiniai veiksmai

Komisija:

- **sudarys ES ir prioritetinių trečiųjų šalių tarptautinius susitarimus dėl bendradarbiavimo su Europolu ir Eurojustu;**
- **skatins šalis partneres dalyvauti EMPACT kovojant su organizuotu nusikalstamumu ir terorizmu;**
- **padės ES agentūroms ir įstaigoms sudaryti ir stiprinti darbo susitarimus su šalimis partnerėmis;**
- **toliau atsižvelgs į saugumo aspektus ES vizų politikoje įgyvendindama būsimą vizų strategiją;**
- **stiprins keitimąsi informacija su patikimomis trečiosiomis šalimis teisėsaugos ir sienų valdymo tikslais.**

Komisija, bendradarbiaudama su vyriausiuoju įgaliotiniu užsienio reikalams:

- **visapusiškai naudosis civilinėmis bendros saugumo ir gynybos politikos (BSGP) misijomis;**
- **iki 2027 m. koordinuos bendrus patikrinimus trečiųjų valstybių uostuose.**

Komisija, bendradarbiaudama su vyriausiuoju įgaliotiniu užsienio reikalams ir saugumo politikai ir valstybėmis narėmis:

- **stiprins ryšių palaikymo tinklus ir bendradarbiavimą, laikydamasi Europos komandos požiūrio;**
- **nuo 2025 m. trečiosiose šalyse steigs bendras operatyvines grupes ir analizės ir informavimo centrus.**

Europos Parlamentas ir Taryba primygtinai raginami:

- **užbaigti derybas dėl bevizio režimo sustabdymo mechanizmo peržiūros.**

[87] COM(2023) 642.

8. Išvada

Pasaulyje vyraujant netikrumui, reikia didinti Sąjungos gebėjimą numatyti grėsmes saugumui, užkirsti joms kelią ir į jas reaguoti.

Nepakanka reaguoti į krizes tik tada, kai jos kyla. Turime didinti savo informuotumą ir susidaryti išsamų vaizdą apie kintančias grėsmes. Taip pat turime užtikrinti, kad mūsų priemonės ir pajėgumai atitiktų šią užduotį.

Šioje strategijoje smulkiai aprašytas išsamus priemonių rinkinys padės sukurti stipresnę Sąjungą pasaulyje: Sąjungą, kuri geba numatyti ir planuoti savo saugumo poreikius ir jais rūpintis, kuri gali veiksmingai reaguoti į grėsmes savo vidaus saugumui ir patraukti kaltininkus atsakomybėn ir kuri saugo savo atvirą, laisvą ir klestinčią visuomenę ir demokratiją.

Tam turime pakeisti savo požiūrį į vidaus saugumą. Sieksime padėti puoselėti naują ES saugumo kultūrą, pagal kurią visuose mūsų teisės aktuose, politikos srityse ir programose – nuo jų priėmimo iki įgyvendinimo – atsižvelgiama į saugumo aspektus, o bendradarbiavimas įvairiose politikos srityse suteikia mums galimybę daryti pažangą.

Tai nėra tik vienos institucijos, vyriausybės ar subjekto užduotis. Tai bendras Europos siekis.