



Europos Sąjungos
Taryba

Briuselis, 2023 m. spalio 18 d.
(OR. en)

14372/23

JAI 1332	COPEN 363
COSI 179	FREMP 292
ENFOPOL 431	JAIEX 66
ENFOCUSTOM 110	CFSP/PESC 1410
IXIM 194	COPS 489
CT 155	HYBRID 73
CRIMORG 137	DISINFO 85
FRONT 327	TELECOM 306
ASIM 92	DIGIT 223
VISA 208	COMPET 1008
CYBER 247	RECH 456
DATAPROTECT 278	CULT 122
CATS 58	COTER 185
DROIPEN 151	CORDROGUE 94

PRIDEDAMAS PRANEŠIMAS

nuo:	Europos Komisijos generalinės sekretorės, kurios vardu pasirašo direktorė Martine DEPREZ
gavimo data:	2023 m. spalio 18 d.
kam:	Europos Sąjungos Tarybos generalinei sekretorei Thérèse BLANCHET
Komisijos dok. Nr.:	COM(2023) 665 final
Dalykas:	KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI dėl šeštosios ES saugumo sąjungos strategijos įgyvendinimo pažangos ataskaitos

Delegacijoms pridedamas dokumentas COM(2023) 665 final.

Pridedama: COM(2023) 665 final



Briuselis, 2023 10 18
COM(2023) 665 final

KOMISIJOS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI
dėl šeštosios ES saugumo sąjungos strategijos įgyvendinimo pažangos ataskaitos

I. Įvadas

Prieš trejus metus Komisija priėmė 2020–2025 m. saugumo sąjungos strategiją¹, kurioje apibrėžti pagrindiniai Sąjungos prioritetai saugumo srityje. Nuo to laiko padarėme didelę pažangą visomis keturiomis strategijos kryptimis, įgyvendindami svarbius teisės aktus – nuo ypatingos svarbos subjektų apsaugos iki kibernetinio atsparumo didinimo. Tačiau grėsmių saugumui padėtis Europoje ir mūsų kaimyninėse šalyse tebekinta. Pastarosiomis dienomis įvykdyti teroristiniai išpuoliai vienoje iš Prancūzijos mokyklų ir Briuselio gatvėse yra aiškus priminimas, kad būtina toliau pritaikyti ir stiprinti mūsų saugumo architektūrą. Kibernetinių išpuolių keliamas pavojus ir toliau auga, o jį didina ir tai, kad piktaivališki subjektai įsitraukia į vykstančius konfliktus. Hibridinių grėsmių, įskaitant dezinformaciją, ir toliau daugėja. Europolas nustatė, kad Rusijos agresijos karas prieš Ukrainą labai sustiprino kibernetinius išpuolius prieš ES taikinius, o didžiausi išpuoliai yra politiškai motyvuoti ir juos koordinuoja prorusiškos įsilaužėlių grupuotės². Tai jaučiama, kai blokuojama interneto prieiga ir trikdomas pagrindinių paslaugų teikimas, pavyzdžiui, energetikos tinklų veikla³.

Saugumo sąjungos strategija buvo parengta taip, kad ES galėtų geriau atlaikyti kintančią grėsmių padėtį. Kadangi susidūrėme su pandemijos ir karo sukeltomis krizėmis, įvykiai parodė strategijoje išdėstyto požiūrio svarbą – mūsų ryžtą galutinai integruoti ES saugumo ekosistemą ir panaikinti atotrūkį tarp kibernetinių ir fizinių saugumo aspektų, be kita ko, kovoje su organizuotu nusikalstamumu, terorizmu ir radikalizacija.

Tačiau norėdami išlikti budrūs, turėtume nuolat tirti, kokių mūsų veiksmų dar trūksta, kad galėtume užtikrinti savo piliečių saugumą. Strategijoje nustatytos prioritetinės sritys, kuriose Sąjunga gali suteikti pridėtinės vertės ir padėti valstybėms narėms didinti visų Europoje gyvenančių žmonių saugumą. Nuo tada, kai ji buvo priimta, imtasi visų nurodytų veiksmų ir įtraukti nauji veiksmai siekiant reaguoti į išliekančius saugumo iššūkius.

Apskritai Komisija pagal Saugumo sąjungos strategiją pateikė 36 teisėkūros iniciatyvas. Dėl daugiau nei pusės šių pasiūlymų tarpinstitucinės derybos jau baigtos – priimti nauji griežti teisės aktai, kaip aprašyta priede pateiktoje lentelėje. Tiesa, Europos Parlamentas ir Taryba toliau derasi dėl kelių pagrindinių Komisijos pasiūlytų iniciatyvų. Kadangi dabartinė Parlamento kadencija baigiasi po 2024 m. birželio mėn. Europos Parlamento rinkimų, būtina skubiai imtis veiksmų, kad būtų apsispręsta dėl likusių dokumentų ir kad piliečiai atitinkamai pajustų saugumo sąjungos teikiamus privalumus. Todėl šioje 6-ojoje saugumo sąjungos pažangos ataskaitoje daugiausia dėmesio skiriama tiems esminiams Komisijos priimtiems saugumo sąjungos teisėkūros ir ne teisėkūros dokumentams, dėl kurių reikia dėti daugiau pastangų, kad jie būtų užbaigti ir veiksmingai įgyvendinti.

ES teisės aktų, dėl kurių jau susitarta, nauda bus juntama tik tada, kai jie bus praktiškai įgyvendinti. Daugiausia dėmesio reikia skirti teisingam ir visiškam jų perkėlimui į nacionalinę teisę, įgyvendinimui ir taikymui valstybėse narėse. 2023 m. Komisija ir toliau užtikrina, kad

¹ COM(2020) 605.

² Paskirstytojo paslaugos trikdymo atakos (DDoS atakos): žr. Europolo „Spotlight“ ataskaitą „Cyber-attacks: the apex of crime-as-a-service“ (liet. „Kibernetiniai išpuoliai: paslauginių nusikaltimų apogėjus“), 2023 m. rugsėjo 13 d.

³ Kenkimo – duomenų naikinimo – programinė įranga per konfliktą Ukrainoje buvo gausiai naudojama siekiant sunaikinti duomenis ir sistemas, pavyzdžiui, trikdant tūkstančių ES abonentų prieigą prie interneto ir iš didelės Vokietijos energetikos įmonės atimant nuotolinės kontrolės prieigą prie daugiau kaip 5 800 vėjo jėgainių. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict (liet. „Kibernetinės veiklos vaidmuo Rusijos kare prieš Ukrainą: jo poveikis ir pasekmės ginkluoto konflikto ateičiai“), Europos Parlamento tyrimas, 2023 m. rugsėjo mėn., PE 702.594.

ES saugumo sąjungos strategija būtų veiksminga, – naudodamasi savo instituciniais įgaliojimais ji pradeda pažeidimo nagrinėjimo procedūras tais atvejais, kai valstybės narės į nacionalinę teisę neperkėlė ES teisės aktų arba juos perkėlė netinkamai.

Šioje ataskaitoje taip pat aptariami atvejai, kai valstybių narių ir (arba) ES agentūrų veiksmai yra itin svarbūs siekiant rezultatų. ES agentūros svariai prisideda prie saugumo sąjungos iniciatyvų įgyvendinimo ir pastaruosius keletą metų buvo plėtojama jų kompetencija. Ataskaitoje nurodomos kai kurios svarbiausios naujos užduotys, kurios agentūroms buvo pavestos, kad jos valstybėms narėms labiau padėtų įgyvendinti pagrindines saugumo sąjungos iniciatyvas.

Be to, geopolitinė padėtis išryškino išorės saugumo svarbą mūsų vidaus saugumui. Tvirtesnė ES vidaus sistema saugumo srityje yra neatsiejama nuo tvirtesnės partnerystės ir bendradarbiavimo su trečiosiomis šalimis. ES turi toliau aktyviai aiškintis, kaip bendradarbiavimas visame pasaulyje galėtų padėti užtikrinti piliečių saugumą namuose.

II. Ateities iššūkiams atspari saugumo aplinka

Ypatingos svarbos infrastruktūros objektų kibernetinis saugumas ir atsparumas

Pagal saugumo sąjungos iniciatyvą Sąjunga yra įsipareigojusi užtikrinti, kad visi Europos piliečiai ir įmonės būtų gerai apsaugoti tiek internete, tiek realiame gyvenime, ir propaguoti atvirą, saugią ir stabilią kibernetinę erdvę. Vis didesni, dažnesni ir paveikesni kibernetiniai incidentai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui ir vidaus rinkai. Rusijos agresijos karas prieš Ukrainą dar labiau sustiprino šią grėsmę, o dabartinę geopolitinę įtampą vis labiau apsunkina daugybės su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų intervenciniai veiksmai. Praėjusį rudenį įvykdytas dujotiekių „Nord Stream“ sabotžas atskleidė, kad tokie svarbūs sektoriai kaip energetika, skaitmeninė infrastruktūra, transportas ir kosmosas priklauso nuo ypatingos svarbos infrastruktūros atsparumo. Pastarojo meto incidentas, susijęs su povandeniniu dujotiekiu ir duomenų kabeliu Estijoje ir Suomijoje, rodo, kad reikia aukšto lygio pasirengimo reaguoti į tokias situacijas. Nors žalos priežastis tebėra neaiški ir tyrimai tebevyksta, valstybių narių ir Komisijos keitimasis informacija įvairiais lygmenimis teikia vilčių. Sutrikimai neturėjo tiesioginio poveikio nei interneto ryšiui, nei dujų tiekimo saugumui Europos ar vietos lygmeniu. Tai rodo pastaraisiais mėnesiais padarytą pažangą ir sustiprintas pasirengimo pastangas.

Todėl, siekiant užtikrinti šių ypatingos svarbos infrastruktūros objektų apsaugą ir atsparumą, būtina aiški ir patikima teisinė sistema. Šiomis aplinkybėmis itin svarbus proveržis buvo pasiektas tuo pačiu metu priimant peržiūrėtą Direktyvą dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (TIS 2)⁴ ir Direktyvą dėl ypatingos svarbos subjektų atsparumo⁵: abi jos įsigaliojo 2023 m. sausio 16 d. Dabar valstybės narės raginamos skubiai, iki galo ir ne vėliau kaip iki 2024 m. spalio 17 d. perkelti šiuos esminius teisės aktus į nacionalinę teisę, kad būtų sukurta patikima Sąjungos ypatingos svarbos infrastruktūros objektų apsaugos nuo fizinių ir kibernetinių grėsmių sistema.

⁴ 2022 m. gruodžio 14 d. Direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti ir Direktyvos (ES) 2018/1972 (TIS 2) direktyva).

⁵ 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.

2023 m. liepos mėn. Komisijos deleguotajame reglamente Komisija nustatė esmines paslaugas 11-oje sektorių, kuriems taikoma Direktyva dėl ypatingos svarbos subjektų atsparumo⁶. Kitas žingsnis – valstybės narės turi atlikti šių paslaugų rizikos vertinimus. Priėmus 2022 m. gruodžio 8 d. Tarybos rekomendaciją⁷, intensyviau imamasi darbo, susijusio su ypatingos svarbos infrastruktūros objektų testavimu nepalankiausiomis sąlygomis, pradedant energetikos sektoriumi, ir stiprinant bendradarbiavimą su NATO ir svarbiausiomis šalimis partnerėmis. Šio darbo procese 2023 m. birželio mėn. ES ir NATO ypatingos svarbos infrastruktūros atsparumo didinimo darbo grupė parengė ataskaitą, kurioje apžvelgiami dabartiniai ypatingos svarbos infrastruktūros objektų saugumo uždaviniai keturiuose pagrindiniuose sektoriuose (energetikos, transporto, skaitmeninės infrastruktūros bei kosmoso) ir pateikiamos atsparumo didinimo rekomendacijos. Rekomendacijas, be kita ko, dėl geresnio koordinavimo, keitimosi informacija ir pratybų, įgyvendina ES ir NATO darbuotojai vykstant struktūriniam dialogui atsparumo klausimais.

Tuo pat metu 2023 m. rugsėjo 6 d. Komisija priėmė pasiūlymą⁸ dėl Tarybos rekomendacijos dėl plano koordinuoti Sąjungos lygmens reagavimą į didelę tarpvalstybinę reikšmę turinčius ypatingos svarbos infrastruktūros sutrikimus. 2023 m. spalio 4 d. buvo surengtos scenarijais grindžiamos diskusijos dėl plano, siekiant išbandyti, kaip jis būtų taikomas praktiškai, ir suteikti informacijos, reikalingos šiuo metu vykstančioms deryboms dėl pasiūlymo Taryboje.

Atsižvelgdami į Tarybos raginimus⁹, Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė atlieka rizikos vertinimus ir rengia rizikos scenarijus kibernetinio saugumo požiūriu. Šiame darbe daugiausia dėmesio skiriama telekomunikacijų ir elektros energijos sektoriams. Dalyvaujant visoms atitinkamoms civilinėms ir karinėms agentūroms ir tinklams, pirmą kartą atliekamas visapusiškas ir įtraukus Sąjungos masto vertinimas. Šis vertinimas taip pat papildys koordinuojamus ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimus, atliekamus pagal TIS 2, ir ypatingos svarbos infrastruktūros objektų rizikos vertinimus bei testavimą nepalankiausiomis sąlygomis energetikos, skaitmeninės infrastruktūros ryšių, transporto ir kosmoso sektoriuose. Siekiant koordinavimo ir suderinamumo, šie įvairūs veiksmai turėtų vienas kitą papildyti, kad būtų lengviau parengti standartinę koncepciją, ir šia koncepcija turėtų būti vadovaujama rengiant būsimas pratybas. Šių veiksmų sėkmė dabar priklausys nuo aktyvaus valstybių narių dalyvavimo.

Ekonomikos ir visuomenės veikimas vis labiau priklauso nuo su kosmosu susijusių paslaugų ir duomenų, ypač saugumo ir gynybos srityje. Kosmosas tampa vis labiau ginčytina strategine sritimi, o jo svarba saugumui padidėjo, ypač po Rusijos invazijos į Ukrainą. Siekiant sustiprinti mūsų strateginę padėtį ir savarankiškumą kosmoso srityje, 2023 m. kovo mėn. priimta ES kosmoso strategija saugumo ir gynybos srityje. Vienas iš pagrindinių su šia strategija susijusių veiksmų – tai, kad Europos Komisija 2024 m. pasiūlys ES kosmoso teisės aktą, kuriuo būtų reglamentuojama su kosmosu susijusios veiklos sauga, tvarumas ir atsparumas / saugumas Europos Sąjungoje.

Kalbant apie išorės aspektą, saugi infrastruktūra yra pasaulinės ekonomikos ir tiekimo grandinių atsparumo pagrindas¹⁰, todėl į ES strategiją „Global Gateway“ įtrauktas stiprus

⁶ C(2023) 4878.

⁷ 2022 m. gruodžio 8 d. Tarybos rekomendacija dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą.

⁸ COM(2023) 526.

⁹ 2022 m. gegužės 23 d. Tarybos išvados dėl Europos Sąjungos kibernetinio saugumo būklės raidos, 2022 m. kovo 9 d. Nevero raginimas stiprinti ES kibernetinio saugumo pajėgumus.

¹⁰ JOIN(2021) 30.

saugumo aspektas. Be to, atsižvelgiant į ES ir šalių partnerių infrastruktūros jungtis, būtinas tolesnis tarptautinis bendradarbiavimas siekiant stiprinti pasaulinį kibernetinį atsparumą ir remti laisvą, atvirą, saugią ir patikimą kibernetinę erdvę.

Kibernetinio atsparumo aktas

Siekiant Europos kibernetinio saugumo itin svarbu užtikrinti, kad vartotojai ir verslo subjektai galėtų pasikliauti saugiais skaitmeniniais produktais. Šį poreikį Komisija siekė patenkinti 2022 m. rugsėjo 15 d. priimtu pasiūlymu dėl Kibernetinio atsparumo akto¹¹. Juo būtų nustatyti privalomi horizontalieji kibernetinio saugumo reikalavimai produktams su skaitmeniniais elementais penkerius metus arba visą jų gyvavimo ciklą (trumpesniu juo iš šių laikotarpių). Taip būtų sudarytos sąlygos projektuoti ir kurti saugius produktus su skaitmeniniais elementais, užtikrinant, kad rinkai pateikiami aparatinės ir programinės įrangos produktai turėtų kuo mažiau pažeidžiamų vietų. Tai būtų svarbus žingsnis keliant Europos kibernetinio saugumo standartus visose srityse ir tikėtina, kad tai taps tarptautiniu atskaitos tašku, kuris suteiks aiškių pranašumų Sąjungos kibernetinio saugumo pramonei pasaulinėse rinkose. 2023 m. liepos mėn. Europos Parlamentas ir Taryba priėmė atitinkamas pozicijas, todėl derybos turėtų būti vykdomos sparčiai.

Kibernetinio saugumo sertifikavimui taip pat tenka itin svarbus vaidmuo didinant pasitikėjimą IRT produktais ir paslaugomis, nes jis sudaro sąlygas vartotojams, verslo subjektams ir valdžios institucijoms priimti informacija pagrįstus sprendimus dėl tinkamo kibernetinio saugumo lygio. Daroma pažanga kibernetinio saugumo sertifikavimo srityje: pagal komiteto procedūrą atliekamas ES bendrais kriterijais grindžiamas kibernetinio saugumo sertifikavimo schemos vertinimas. Europos Sąjungos kibernetinio saugumo agentūra (ENISA) šiuo metu rengia potencialią ES debesijos saugumo sertifikavimo schemą (EUCS), o Europos kibernetinio saugumo sertifikavimo grupė ją svarsto. Intensyviai bendradarbiaujant su įvairių sektorių ekspertais, vartotojais ir paslaugų teikėjais turėtų būti suformuota patikima teisinė ir techninė koncepcija, kuri suteiktų būtinas saugumo garantijas, atitinkančias Sąjungos teisę, tarptautinius įsipareigojimus ir PPO prievoles. Be to, ENISA rengia potencialią programą „EU5G“ ir kuria ES skaitmeninės tapatybės dėklę (EUIDW). Siekiant didinti bendrą IRT produktų, paslaugų ir procesų saugumą labai svarbu, kad visos valstybės narės dėtų suderintas pastangas.

Reglamentai dėl informacijos saugumo ir kibernetinio saugumo ES institucijose, įstaigose ir agentūrose

2022 m. kovo mėn. kartu pasiūlyti reglamentai dėl pačios Sąjungos institucijų kibernetinio saugumo ir informacijos saugumo reglamentavimo buvo svarstomi skirtingu tempu. Praėjusių metų birželio mėn. buvo pasiektas politinis susitarimas dėl kibernetinio saugumo reglamento, kuriuo sudaromos sąlygos sustiprinti visų ES institucijų, įstaigų, organų ir agentūrų kibernetinio saugumo padėtį. Tai rodo, kaip ES svarbu sparčiai įgyvendinti šį pasiūlymą. Tokiomis aplinkybėmis ypač didelį susirūpinimą kelia tai, kad, priešingai nei tikėtasi, lygiagretus pasiūlymas dėl informacijos saugumo, kuris yra būtinas siekiant baigti kurti tvirtą institucijų, įstaigų, organų ir agentūrų teisės aktų sistemą, svarstomas lėtai. Abu pasiūlymai turėtų būti priimti prieš Europos Parlamento rinkimus, kad dabartinėmis geopolitinėmis aplinkybėmis ES administracija taptų patikima ir atspari. Visoms institucijoms, įstaigoms, organams ir agentūroms nustačius būtiniausias informacijos saugumo taisykles ir standartus būtų užtikrintas tikrumas visoms susijusioms šalims, taip pat būtų užtikrinta nuosekli apsauga nuo kintančių grėsmių jų informacijai – tiek ES įslaptintai, tiek neįslaptintai. Visos šios naujos taisyklės suteiktų stabilų pagrindą saugiam keitimuisi informacija tarp institucijų, įstaigų, organų ir agentūrų ir su valstybėmis narėmis, taikant standartizuotą informacijos srautų apsaugos

¹¹ COM(2022) 454.

praktiką ir priemones. Šia prasme minėtomis taisyklėmis reaguojama į ne vieną Tarybos raginimą didinti institucijų, įstaigų, organų ir agentūrų atsparumą ir geriau apsaugoti Sąjungos sprendimų priėmimo procesą nuo piktavališko kišimosi.

Kibernetinio solidarumo aktas

2023 m. balandžio 18 d. Komisijos priimtas pasiūlymas dėl Kibernetinio solidarumo akto¹², pagrįstas jau galiojančia tvirta strategine, politikos ir teisės aktų sistema, turėtų dar labiau pagerinti kibernetinių grėsmių nustatymą, atsparumą ir pasirengimą visais Sąjungos kibernetinio saugumo ekosistemos lygmenimis. Šie tikslai būtų įgyvendinami trimis pagrindiniais veiksmais:

- (1) diegiant ***ES kibernetinio saugumo skydą***, kad būtų sukurti ir stiprinami bendri aptikimo ir informuotumo apie padėtį pajėgumai. Skydą sudarytų visi nacionaliniai saugumo operacijų centrai (toliau – nacionaliniai SOC) ir tarpvalstybiniai saugumo operacijų centrai (toliau – tarpvalstybiniai SOC);
- (2) sukuriant ***reagavimo į kibernetinio saugumo krizes mechanizmą***, kuris padėtų valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą. Reaguoti į incidentus padėtų ES kibernetinio saugumo rezervas, kuriuo taip pat galėtų naudotis Europos institucijos, įstaigos, organai ir agentūros ir Skaitmeninės Europos programos asocijuotosios trečiosios šalys, jei tai numatyta jų asociacijos susitarime dėl Skaitmeninės Europos programos;
- (3) sukuriant ***Europos kibernetinio saugumo incidentų peržiūros mechanizmą*** reikšmingiems arba didelio masto incidentams peržiūrėti ir įvertinti. Peržiūros po incidento ataskaitą koordinuotų ir parengtų ENISA.

Taryboje ir Europos Parlamente prasidėjo diskusijos. Užbaigus derybas iki dabartinės Europos Parlamento kadencijos pabaigos atsirasti didelis postūmis aktyviau saugoti piliečius ir verslo subjektus visoje Sąjungoje.

Kibernetinio saugumo įgūdžių akademija

Kibernetinės grėsmės didėja, ir ES skubiai reikia specialistų, turinčių įgūdžių ir kompetencijų, kad būtų užkirstas kelias kibernetiniams išpuoliams prieš ES, jie būtų aptikti, nuo jų būtų atgrasoma ir ginama. Šiuo metu apskaičiuota, kad kibernetinio saugumo darbo jėgos poreikis yra 883 000 specialistų, o 2022 m. neužimtų darbo vietų skaičius svyravo nuo 260 000 iki 500 000. Visos visuomenės grupės turėtų būti skatinamos padėti užpildyti šią spragą, tačiau visų pirma pažymėtina, kad 2022 m. moterys sudarė tik 20 proc. kibernetinio saugumo srities absolventų ir 19 proc. informacinių ir ryšių technologijų specialistų. 2023 m. – Europos įgūdžių metais – Komisija 2023 m. balandžio 18 d.¹³ priėmė valstybių narių palankiai vertinamą iniciatyvą¹⁴ įsteigti Kibernetinio saugumo įgūdžių akademiją, kad būtų panaikintas kibernetinio saugumo talentų trūkumas. Kibernetinio saugumo įgūdžių akademija telktų esamas kibernetinio saugumo įgūdžių iniciatyvas ir pagerintų koordinavimą. Komisija ragina valstybes nares, regionines ir vietos valdžios institucijas, taip pat Europos viešuosius subjektus priimti specialias strategijas ar iniciatyvas dėl kibernetinio saugumo įgūdžių arba integruoti kibernetinio saugumo įgūdžius į atitinkamas platesnio masto strategijas ar iniciatyvas (pvz., kibernetinio saugumo, skaitmeninių įgūdžių, užimtumo ir kt.). Siekiant sumažinti kibernetinio saugumo įgūdžių

¹² COM(2023) 209.

¹³ COM(2023) 207.

¹⁴ 2023 m. gegužės 22 d. Tarybos išvados dėl ES kibernetinės gynybos politikos.

trūkumą ir susijusį darbo jėgos trūkumą Europoje labai svarbus ir privačių suinteresuotųjų subjektų dalyvavimas.

Bepiločiai orlaiviai

Kita didėjanti grėsmė viešosioms erdvėms ir ypatingos svarbos infrastruktūros objektams yra piktavališkas bepiločių orlaivių naudojimas. Su bepiločiais orlaiviais susiję incidentai Sąjungoje ir už jos ribų tapo dažnesni, o kovos su bepiločiais orlaiviais sprendimai – viena iš pagrindinių priemonių, skirtų Sąjungos teisėsaugos ir kitoms valdžios institucijoms, taip pat privatiems ypatingos svarbos infrastruktūros operatoriams. Be to, teisėtas bepiločių orlaivių naudojimas labai prisideda prie dvejopos žaliosios ir skaitmeninės pertvarkos¹⁵. Kaip paskelbta 2022 m. lapkričio mėn. priimtoje Dronų strategijoje 2.0, šiandien Komisija priima komunikatą, kaip kovoti su bepiločių orlaivių galimai keliamomis grėsmėmis. Jį papildė du žinynai su praktinėmis pagrindinių techninių aspektų rekomendacijomis¹⁶. Siekiama, kad pagal šią iniciatyvą atsirastų visapusiška ir suderinta politikos sistema ir vienodai suprantamos taisyklės, taikytinos kovojant su bepiločių orlaivių galimai keliamomis grėsmėmis, prireikus prisitaikant prie sparčios technologijų raidos. Valstybės narės ir atitinkami privatūs veiklos vykdytojai raginami glaudžiai bendradarbiauti su Komisija, kad būtų užtikrintas visapusiškas sistemos įgyvendinimas.

Jūrų ir aviacijos saugumas

Neteisėta veikla, pavyzdžiui, piratavimas, ginkluoti plėšimai jūroje, neteisėtas migrantų gabenimas ir prekyba žmonėmis, ginklais ir narkotikais, taip pat terorizmas, tebekelia jūrų saugumo iššūkių ir problemą gilina naujai besiformuojančios grėsmės, be kita ko, hibridiniai ir kibernetiniai išpuoliai. 2023 m. kovo 10 d. Komisija ir vyriausiasis įgaliojimas priėmė bendrą komunikatą dėl ES jūrų saugumo strategijos atnaujinimo¹⁷. Ji dabar turėtų būti įgyvendinama pagal atnaujintą veiksmų planą.

Aviacijos saugumo srityje 2023 m. vasario 2 d. Komisija priėmė Komisijos tarnybų darbinį dokumentą „Tobulesnės ir atsparesnės aviacijos saugumo politikos kūrimas“¹⁸, jame pateikta plataus užmojo programa, kuria siekiama 1) modernizuoti aviacijos saugumo reglamentavimo struktūrą, 2) skatinti kurti ir diegti novatoriškesnius sprendimus ir 3) atnaujinti aviacijos saugumo bazinį lygį, kad Sąjungos oro uostai galėtų visapusiškai naudotis naujomis pažangiausiomis technologijomis ir atitinkamai galėtų įveikti didžiausio prioriteto grėsmes. Per dvejus metus turi būti įgyvendinta keturiolika pavyzdinių veiksmų.

Komisija ragina Europos Parlamentą ir Tarybą skubiai, ne vėliau kaip iki dabartinės sudėties Europos Parlamento kadencijos pabaigos, užbaigti derybas dėl šių dokumentų:

- pasiūlymo dėl Kibernetinio atsparumo akto;
- pasiūlymo dėl Kibernetinio solidarumo akto;
- pasiūlymo dėl Reglamento dėl informacijos saugumo ES institucijose, įstaigose, organuose ir agentūrose.

Komisija ragina valstybes nares:

¹⁵ COM(2022) 652.

¹⁶ COM(2023) 659.

¹⁷ JOIN(2023) 8.

¹⁸ SWD(2023) 37.

- pirmenybės tvarka tęsti Ypatingos svarbos subjektų atsparumo direktyvos perkėlimą į nacionalinę teisę, taip pat ypatingos svarbos infrastruktūros objektų testavimą nepalankiausiomis sąlygomis energetikos sektoriuje;
- priimti Tarybos rekomendaciją dėl koordinuojamo reagavimo į didelę tarpvalstybinę reikšmę turinčios ypatingos svarbos infrastruktūros sutrikimus plano;
- visapusiškai ir skubiai perkelti TIS 2 direktyvą į nacionalinę teisę, kad būtų padidintas esminių ir svarbių subjektų kibernetinis saugumas;
- aktyviai dalyvauti atliekant kibernetinio saugumo rizikos vertinimus ir rengiant ypatingos svarbos infrastruktūros objektų ir tiekimo grandinių rizikos scenarijus;
- imtis tolesnių veiksmų, susijusių su Kibernetinio saugumo įgūdžių akademija, aktyviai dalyvaujant Europos lygmeniu, rengiant specialias nacionalines kibernetinio saugumo įgūdžių strategijas ar iniciatyvas ir į tai įtraukiant pagrindinius suinteresuotuosius subjektus, įskaitant regionų ir vietos valdžios institucijas;
- bendradarbiauti su atitinkamais privačiais veiklos vykdytojais ir Komisija siekiant užtikrinti visų Komunikate dėl kovos su bepiločių orlaivių galimai keliamomis grėsmėmis išvardytų veiksmų įgyvendinimą;
- įgyvendinti ES jūrų saugumo strategijos veiksmų planą ir reguliariai teikti ataskaitas apie pasiektus rezultatus;
- įgyvendinti aviacijos saugumui didinti numatytų 14 pavyzdinių veiksmų.

III. Kova su naujai besiformuojančiomis grėsmėmis

Nauja geopolitinė įtampa aiškiai rodo, kad saugumo iššūkis ES ne tik didėja, bet ir tampa vis nepastovesnis ir stiprėja dėl hibridinio daugelio grėsmių pobūdžio. Saugumas taip pat turi atitikti visuomenės ir technologijų pokyčius. COVID-19 pandemija padidino kibernetinių nusikaltėlių galimybes ir visų pirma padidino seksualinės prievartos prieš vaikus medžiagos internete grėsmę. Nusikaltėliai ir piktavališki subjektai visada pasirengę pasinaudoti technologine plėtra. Tvyrant tokioms dažnai sudėtingoms ir daugialypėms grėsmėms, reikia imtis ryžtingų ir nuoseklių ES veiksmų.

Reglamentas dėl kovos su seksualine prievarta prieš vaikus internete

Europolo organizuoto nusikalstamumo internete grėsmės vertinimas parodė, kad 2022 m. seksualinis vaikų išnaudojimas ir prievarta prieš vaikus ir toliau dažnėjo ir sunkėjo, nes nusikaltėliai ir toliau naudojami techninėmis galimybėmis užmaskuoti savo veiksmus ir tapatybę¹⁹. Dabartinė sistema, grindžiama tuo, kad įmonės grėsmes nustato ir apie jas praneša savo noru, pasirodė esanti nepakankama vaikams apsaugoti. Laikinasis reglamentas įmonėms leidžia savanoriškai nustatyti tapatybę ir teikti pranešimus, jei tai teisėta pagal Bendrąjį duomenų apsaugos reglamentą (BDAR). Šis reglamentas baigs galioti 2024 m. rugpjūčio mėn. 2022 m. gegužės mėn. Komisija pasiūlė reglamentą²⁰, kuriuo siekiama kovoti su piktnaudžiavimu internetinėmis paslaugomis seksualinės prievartos prieš vaikus tikslais. Siūlomoje sistemoje daug dėmesio skiriama prevencijai. Įmonės būtų įpareigosotos savo sistemose įvertinti seksualinės prievartos prieš vaikus riziką ir imtis prevencinių priemonių. Kraštutiniu, tik didelės rizikos atveju nacionaliniai teismai arba nepriklausomos

¹⁹ Europol (2023), Internet Organised Crime Threat Assessment (IOCTA) 2023.

²⁰ COM(2022) 209.

administracinės institucijos paslaugų teikėjams galėtų duoti tikslinius nurodymus aptikti turinį. Naujas nepriklausomas ES centras palengvintų paslaugų teikėjų darbą, veikdamas kaip ekspertinių žinių centras, kuri teikia patikimą informaciją apie aptiktą medžiagą, gauna ir analizuoja paslaugų teikėjų pranešimus apie seksualinę prievartą prieš vaikus internete, kad būtų galima nustatyti klaidingus pranešimus ir teikti paramą nukentėjusiesiems. Labai svarbu, kad naujosios taisyklės būtų priimtose ir įgyvendintos kuo greičiau, siekiant apsaugoti vaikus nuo tolesnės prievartos, užkirsti kelią pakartotiniam medžiagos atsiradimui internete ir patraukti nusikaltėlius baudžiamojon atsakomybėn. Taryboje ir Parlamente vyksta derybos siekiant susitarti dėl šio dokumento iki Parlamento kadencijos pabaigos.

Direktyva dėl kovos su smurtu prieš moteris ir smurtu šeimoje

Kaip naujo smurto prieš moteris forma, atsirado kibernetinis smurtas prieš moteris (be kita ko, smurto šeimoje kontekste), kuris internetu bei IT priemonėmis peržengia atskirų valstybių narių ribas. 2022 m. kovo mėn. Komisija pasiūlė direktyvą, kuria siekiama kovoti su smurtu prieš moteris ir smurtu šeimoje, įskaitant konkrečias taisykles dėl kibernetinio smurto ir priemonės apsaugos, teisės kreiptis į teismą ir prevencijos spragoms užpildyti. Ankstyvas priėmimas ir įgyvendinimas suteiktų valstybėms narėms papildomų priemonių kovoti su šios formos nusikalstamumu. Teisėkūros institucijos tarpinstitucines derybas pradėjo 2023 m. liepos mėn. ir siekia užbaigti derybas iki dabartinės Europos Parlamento kadencijos pabaigos.

5G kibernetinis saugumas

5G tinklų saugumas yra vienas iš svarbiausių Komisijos prioritetų ir vienas esminių jos saugumo sąjungos strategijos elementų. 5G tinklai yra labai svarbi infrastruktūra, suteikianti pagrindą įvairioms paslaugoms, kurios yra būtinos vidaus rinkos veikimui ir gyvybiškai svarbioms visuomenės ir ekonominėms funkcijoms atlikti. 2023 m. birželio 15 d. TIS bendradarbiavimo grupėje atstovaujamos ES valstybių narių valdžios institucijos, talkinamos Komisijos ir ENISA, paskelbė antrąją ES 5G kibernetinio saugumo priemonių rinkinio įgyvendinimo pažangos ataskaitą. Ataskaitoje teigiama, kad 24 valstybės narės priėmė arba rengia teisėkūros priemones, kuriomis nacionalinėms valdžios institucijoms suteikiami įgaliojimai atlikti tiekėjų vertinimą ir nustatyti apribojimus, o 10 valstybių narių tokius apribojimus nustatė. Tačiau reikia imtis tolesnių veiksmų, kad būtų išvengta visos Sąjungos pažeidžiamumo, kuris gali turėti didelį neigiamą poveikį atskirų naudotojų ir įmonių saugumui visoje Sąjungoje ir Sąjungos ypatingos svarbos infrastruktūros objektų saugumui. Visos valstybės narės turi nedelsdamos įgyvendinti priemonių rinkinį. Tą pačią dieną Komisija priėmė Komunikatą dėl priemonių rinkinio įgyvendinimo valstybėse narėse ir dėl pačios Komisijos, kaip organizacijos, ryšių bei Sąjungos finansavimo veiklos. Tai parodė, kad esama didelio susirūpinimo dėl pavojaus ES saugumui, kurį kelia mobiliojo ryšio tinklo įrangos „Huawei“ ir „ZTE“ tiekėjai. Atsižvelgdama į tai, Komisija imasi priemonių, kad išvengtų tiekėjų „Huawei“ ir „ZTE“ naudojančių mobiliojo ryšio tinklų poveikio savo, kaip organizacijos, ryšiams. Nebus leidžiama pirkti naujų ryšio paslaugų, grindžiamų tų tiekėjų įranga, o Komisija bendradarbiaudama su valstybėmis narėmis ir telekomunikacijų operatoriais sieks užtikrinti, kad palaipsniui būtų atsisakyta tų tiekėjų Komisijos patalpose teikiamų ryšio paslaugų. Komisija taip pat aiškinasi, kaip atsižvelgti į šį sprendimą atitinkamose Sąjungos finansavimo programose ir priemonėse, visapusiškai laikantis Sąjungos teisės.

Prieiga prie duomenų siekiant užtikrinti veiksmingą teisėsaugą

Šiandienos skaitmeninėje epochoje beveik kiekvienas nusikaltimas turi skaitmeninį komponentą. Technologijos ir priemonės taip pat naudojamos nusikalstamais tikslais, įskaitant tas, kurios būtinos siekiant užtikrinti mūsų visuomenės kibernetinio saugumo, duomenų apsaugos ir privatumo poreikį. Dėl to tampa vis sunkiau užtikrinti veiksmingą teisėsaugą visoje

ES, kuri pasirūpintų visuomenės saugumu ir užkirstų kelią nusikaltimams, juos nustatytų, tirtų ir patrauktų už juos baudžiamojon atsakomybėn, ir nors Sąjungos ir nacionaliniu lygmenimis įdėta daug pastangų, be kita ko, priimant teisės aktus, stiprinant gebėjimus ir taikant novatoriškas iniciatyvas, tebėra teisinių ir techninių problemų. Komisija, jungdamasi prie Tarybai pirmininkaujančios valstybės narės, įsteigė Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio ekspertų grupę, kad įvairūs suinteresuotieji subjektai ir ekspertai turėtų bendradarbiavimo platformą, kurioje būtų galima nagrinėti problemas, su kuriomis susiduria baudžiamosios teisės specialistai (pvz., šifravimas, duomenų saugojimas, 5G ir standartizavimas). Komisija tikisi, kad aukšto lygio grupė iki 2024 m. birželio mėn. parengs subalansuotas, patikimas ir įgyvendinamas rekomendacijas, atspindinčias šių klausimų sudėtingumą, be kita ko, kibernetinio saugumo ir duomenų apsaugos aspektu. Todėl valstybės narės ir dalyvaujantys ekspertai raginami aktyviai įsitraukti į šį procesą ir siekti veiksmingų, teisėtų ir visuotinai priimtinių sprendimų.

Hibridinės grėsmės

Geopolitinėmis aplinkybėmis, kai hibridinės grėsmės tampa vis sudėtingesnės ir komplikuočiau, ES saugumo ir gynybos strateginiame kelrodyje²¹ (Strateginis kelrodys) pateiktas bendras grėsmių ir iššūkių, su kuriais susiduria Sąjunga, vertinimas ir strateginis veiksmų planas. Dažnėjantis valstybių ir nevalstybinių subjektų piktavališkas elgesys kibernetinėje erdvėje, be kita ko, karo prieš Ukrainą kontekste, dar labiau išryškino kibernetinę erdvę kaip užsienio ir saugumo politikos sritį. Dėl galimos piktavališkų veiksmų ir dezinformacijos rizikos rinkimų laikotarpiais, be kita ko, rengiantis 2024 m. Europos Parlamento rinkimams, būtinas ypatingas budrumas.

Atsižvelgdama į didelę šalutinio poveikio riziką, ES toliau plėtojo kibernetinių pajėgumų stiprinimo veiklą ir puoselėjo partnerystes su trečiosiomis šalimis, be kita ko, vesdama specialius dialogus kibernetinės erdvės klausimais, kad aktyviai prisidėtų prie jos bendro atsparumo. Siekiant sustiprinti Sąjungos gebėjimą veiksmingai kovoti su hibridinėmis grėsmėmis, buvo parengtos, peržiūrėtos ir sustiprintos tam tikros priemonės, kaip aprašyta 2023 m. rugsėjo 14 d. paskelbtoje 7-ojoje pažangos ataskaitoje dėl hibridinių grėsmių²². Tai:

- ES hibridinių priemonių rinkinys, kuriuo siekiama užtikrinti koordinuoto ir gerai informacija pagrįsto atsako į hibridines grėsmes ir kampanijas sistemą;
- vykdomas darbas siekiant sukurti ESES greitojo reagavimo į hibridines grėsmes grupes, kurios teiktų trumpalaikę pritaikytą paramą valstybėms narėms, šalims partnerėms ir bendros saugumo ir gynybos politikos (BSGP) misijoms ir operacijoms;
- peržiūrėtas ES operatyvinių veiksmų protokolai dėl kovos su hibridinėmis grėsmėmis (toliau – ES hibridinių grėsmių vadovas)²³, kuriame aprašomi Sąjungos procesai ir struktūros, kovojančios su hibridinėmis grėsmėmis ir kampanijomis;
- peržiūrėtas Bendro ES diplomatinio atsako į kibernetinę kenkimo veiklą sistemos²⁴ (Kibernetinio saugumo diplomatijos priemonių rinkinio) įgyvendinimo gairės, sudarančios sąlygas parengti tvarias, pritaikytas, suderintas ir koordinuojamas kovos su nuolatinėmis kibernetinėmis grėsmėmis keliančiais subjektais strategijas;
- Kovos su užsienio vykdomu manipuliavimu informacija ir kišimusi (FIMI) priemonių rinkinys, kuriuo siekiama sustiprinti esamas Sąjungos priemones, skirtas užkirsti kelią FIMI, atgrasyti nuo jo ir į jį reaguoti;

²¹ Tarybos dokumentas 7371/22.

²² SWD(2023) 315.

²³ SWD(2023) 116.

²⁴ 10289/23, 2023 m. birželio 8 d.

- ES kibernetinės gynybos politika²⁵, kuria siekiama stiprinti ES kibernetinės gynybos pajėgumus, didinti informuotumą apie padėtį ir vykdyti koordinavimą įvairių gynybos variantų klausimais, siekiant didinti atsparumą, reaguoti į kibernetinius išpuolius ir užtikrinti solidarumą bei savitarpio pagalbą.

Todėl valstybės narės raginamos tęsti ir stiprinti bendradarbiavimą šioje srityje, užtikrinant veiksmingą minėtų priemonių rinkinių įgyvendinimą, be kita ko, reguliariomis pratybomis, ir susitariant dėl greitojo reagavimo į hibridines grėsmes grupių koncepcijos, kuria bus galima vadovautis tolesniame šių grupių kūrimo darbe.

Dirbtinis intelektas teisėsaugos srityje

Dirbtinis intelektas (DI) greitai tapo įprasta kasdienio gyvenimo dalimi. Dirbtinio intelekto naudojimo poveikis kibernetiniams nusikaltimams ir kibernetiniam saugumui dar nėra visiškai žinomas, tačiau akivaizdu, kad jis kels naujų iššūkių. Nors DI gali būti naudingas, kai naudojamas saugiai ir kontroliuojamai, piktavalių subjektų rankose jis gali būti pavojingas, t. y. gali, be kita ko, padėti nusikaltėliams nuslėpti savo tapatybę darant tokius nusikaltimus kaip terorizmas ir seksualinė prievarta prieš vaikus. Todėl itin svarbu, kad valdžios institucijos, siekdamos užkirsti kelią piktnaudžiavimui ir reaguoti į netinkamą naudojimą, neatsilikytų nuo pokyčių²⁶. Derybose dėl siūlomo Dirbtinio intelekto akto siekiama spręsti šiuos klausimus ir prasidėjo itin svarbus jų etapas, o teisėkūros institucijos dabar aptaria techninius ir politinius klausimus, nulemsiančius sąveiką su šia technologija daugelį ateinančių metų. Labai svarbu rasti subalansuotus sprendimus, ypač dėl didelės rizikos taikomųjų programų, be kita ko, teisėsaugos srityje.

Komisija ragina Europos Parlamentą ir Tarybą skubiai, bet kuriuo atveju iki šios Europos Parlamento kadencijos pabaigos, užbaigti tarpinstitucines derybas dėl šių dar nepriimtų dokumentų:

- pasiūlymo dėl Reglamento dėl kovos su seksualine prievarta prieš vaikus internete;
- pasiūlymo dėl direktyvos dėl kovos su smurtu prieš moteris ir smurtu šeimoje;
- pasiūlymo dėl reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (DI aktas).

Komisija ragina valstybes nares:

- nedelsiant visapusiškai įgyvendinti ES 5G kibernetinio saugumo priemonių rinkinį;
- remti Prieigos prie duomenų veiksmingai teisėsaugai užtikrinti aukšto lygio ekspertų darbą, kad būtų parengtos aiškios, patikimos ir įgyvendinamos rekomendacijos, kaip proporcingai spręsti dabartines ir numatomas problemas;
- bendradarbiaujant su vyriausiuoju įgaliotiniu imtis veiksmų siekiant užtikrinti veiksmingą ES hibridinių priemonių rinkinio, peržiūrėto Kibernetinio saugumo diplomatijos priemonių rinkinio ir Kovos su užsienio vykdomu manipuliavimu informacija ir kišimusi priemonių rinkinio įgyvendinimą, be kita ko, vykdant reguliarias pratybas ir atsižvelgiant į pasaulinę dinamiką;
- pasiekti susitarimą dėl greitojo reagavimo į hibridines grėsmes grupių koncepcijos.

²⁵ JOIN(2022) 49.

²⁶ Žr., pavyzdžiui, 2023 m. balandžio 17 d. paskelbtą Europolo ataskaitą *ChatGPT - the impact of Large Language Models on Law Enforcement* („ChatGPT – didelių kalbų modelių poveikis teisėsaugai“).

IV. ES piliečių apsauga nuo terorizmo ir organizuoto nusikalstamumo

Visą laiką esama pavojaus, kad dėl pasaulinių ar vietos įvykių gali kilti naujų terorizmo protrūkių. Lygiagrečiai viena didžiausių grėsmių ES saugumui yra organizuotas nusikalstamumas ir prekyba narkotikais. Siekiant sustiprinti bendras Sąjungos kovos su šiomis grėsmėmis pastangas, kolektyviai įgyvendinama ES kovos su organizuotu nusikalstamumu strategija²⁷, ES kovos su prekyba žmonėmis strategija²⁸, ES kovos su narkotikais darbotvarkė ir veiksmų planas²⁹ bei ES kovos su terorizmu darbotvarkė³⁰. Tačiau, siekiant reaguoti į nerimą keliančią dėl organizuoto nusikalstamumo ir prekybos narkotikais blogėjančią padėtį, reikia toliau intensyvinti valstybių narių ir ES darbą, kad sustiprėtų mūsų kolektyvinis atkirtis nusikaltėlių tinklams, o nusikaltimų aukos būtų geriau apsaugotos. Kartu su šia ataskaita skelbiamos ES kovos su prekyba narkotikais ir organizuotu nusikalstamumu gairės³¹.

Kovos su terorizmu srityje ES taip pat stiprina savo išorės priemonių rinkinį³², aktyviai pasitelkdama aukšto lygio dialogu kovos su terorizmu klausimais ir ES delegacijų kovos su terorizmu ir saugumo ekspertų tinklą, taip pat veikdama daugiašaliuose forumuose, be kita ko, kaip viena iš Pasaulinio kovos su terorizmu forumo (GCTF) pirmininkių.

Neteisėta prekyba narkotikais

Europos narkotikų ir narkomanijos stebėsenos centrui suteikus naujus įgaliojimus, kurie bus taikomi nuo 2024 m. liepos mėn., ES bus geriau pasirengusi spręsti sudėtingą saugumo ir sveikatos problemą, su kuria susiduria milijonai žmonių ES ir visame pasaulyje. Komisija taip pat peržiūri³³ reglamentus dėl narkotinių ir psichotropinių medžiagų pirmtakų (prekursorių)³⁴, siekdama spręsti pagrindines problemas, nustatytas 2020 m. vertinime³⁵: jame pabrėžta, kad norint mažinti neteisėtų narkotikų pasiūlą reikia spręsti propirmtakių³⁶ keliamas problemas.

Tačiau, atsižvelgiant į precedento neturintį neteisėtų narkotikų gausėjimą Europoje, kova su prekyba narkotikais turi suintensyvėti bendradarbiaujant su tarptautiniais partneriais. Valstybės narės ir ES turi imtis papildomų veiksmų siekdamas išardyti nusikaltėlių tinklus ir geriau apsaugoti nusikaltimų aukas. Šiandien Komisija pristato ES kovos su prekyba narkotikais ir organizuotu nusikalstamumu gaires. Jose nustatyta 17 veiksmų keturiose prioritetinėse srityse: stiprinti logistikos centrų atsparumą su Europos uostų aljansu, ardyti nusikaltėlių tinklus, didinti prevencijos pastangas ir stiprinti bendradarbiavimą su tarptautiniais partneriais. Šie veiksmai turi būti įgyvendinti 2024 ir 2025 m.

²⁷ COM(2021) 170.

²⁸ COM(2021) 171.

²⁹ COM(2020) 606.

³⁰ COM(2020) 795.

³¹ COM(2023) 641.

³² Kaip raginama Strateginiame kelrodyje ir 2022 m. birželio mėn. priimtose Tarybos išvadose dėl klausimų, susijusių su nuolat kintančios terorizmo ar smurtinio ekstremizmo grėsmės išorės aspektu, sprendimo.

³³ Narkotinių ir psichotropinių medžiagų pirmtakai (prekursoriai). ES teisės aktai (peržiūrėtos taisyklės) (europa.eu).

³⁴ Reglamentas (EB) Nr. 273/2004 dėl narkotinių ir psichotropinių medžiagų pirmtakų (prekursorių) ir Tarybos reglamentas (EB) Nr. 111/2005, nustatantis prekybos narkotinių ir psichotropinių medžiagų pirmtakais (prekursoriais) tarp Bendrijos ir trečiųjų šalių stebėsenos taisyklės.

³⁵ COM(2020) 768.

³⁶ Kovos su narkotikais veiksmų plano, COM(2020) 606, 23 veiksmas.

Šaunamieji ginklai

Neteisėta prekyba šaunamaisiais ginklais skatina organizuotą nusikalstamumą ES viduje ir kaimyninėse šalyse. Manoma, kad ES civiliai gyventojai turi net 35 mln. neteisėtų šaunamųjų ginklų, o Šengeno informacinėje sistemoje yra užregistruota apie 630 000 pavogtų arba dingusių šaunamųjų ginklų. Vystantis greitam siuntų pristatymui ir naujoms technologijoms, pvz., 3D spausdinimui, neteisėta prekyba šaunamaisiais ginklais įgyja naujų formų, kuriomis siekiama išvengti kontrolės. Rusijos agresijos karas prieš Ukrainą taip pat padidino šaunamųjų ginklų platinimo riziką. 2022 m. spalio mėn. Komisija priėmė pasiūlymą atnaujinti galiojančius teisės aktus dėl civilinių šaunamųjų ginklų importo, eksporto ir tranzito, kad būtų panaikintos galiojančių taisyklių spragos, dėl kurių gali padidėti į ES neteisėtai įvežamų ir nukreipiamų šaunamųjų ginklų skaičius³⁷. Vidutiniu laikotarpiu šios naujos taisyklės padės sumažinti riziką, kad eksportuojant civiliniam naudojimui skirtus šaunamuosius ginklus bus apeinamas embargas, ir padidinti šio tipo šaunamųjų ginklų importo iš ES nepriklausančių šalių kontrolę. Abi teisėkūros institucijos vis dar turi priimti savo pozicijas dėl šio dokumento, kad susitarimas dėl minėto dokumento būtų pasiektas iki šios Parlamento kadencijos pabaigos.

Prekyba žmonėmis

Prekyba žmonėmis yra itin sunkus organizuotas nusikaltimas ir šiurkštus pagrindinių teisių pažeidimas. Nukentėjusiais prekiaujama ES viduje, daugiausia seksualinio išnaudojimo ir išnaudojimo darbe tikslais, taip pat dėl priverstinio elgetavimo, priverstinio nusikalstamumo ir išnaudojimo kitomis formomis. 2022 m. gruodžio mėn. Komisija pasiūlė iš dalies pakeisti Kovos su prekyba žmonėmis direktyvą³⁸ su atnaujintomis taisyklėmis, kad būtų pašalinti dabartinės teisinės sistemos trūkumai. Visų pirma, priėmus peržiūrėtą direktyvą, į direktyvos taikymo sritį būtų įtrauktos priverstinės santuokos ir neteisėtas įvaikinimas, taip pat būtų įtraukta aiški nuoroda į prekybos žmonėmis internetinį aspektą. Į direktyvos taikymo sritį taip pat būtų įtrauktas privalomas sankcijų nusikaltėliams režimas ir formalizuotas nacionalinių nukreipimo mechanizmų sukūrimas, siekiant pagerinti ankstyvą tapatybės nustatymą ir tarpvalstybinį nukreipimą dėl pagalbos ir paramos nukentėjusiesiems. Sąmoningas naudojimas prekybos žmonėmis aukų teikiamomis paslaugomis taptų nusikalstama veika ir taptų privaloma kasmet rinkti duomenis apie prekybą žmonėmis, kuriuos skelbtų Eurostatas. 2023 m. birželio mėn. Taryba priėmė bendrą požiūrį, o Europos Parlamentas dar turi priimti savo poziciją. Reikės imtis skubių veiksmų, kad susitarimas būtų pasiektas iki šios Parlamento kadencijos pabaigos.

Nusikaltimai aplinkai

Nusikaltimai aplinkai tapo pasauline grėsme, jų kasmet daugėja apytikriai 5–7 proc. Didelis pelnas, kurį galima gauti, teisinės spragos tarp valstybių narių ir maža rizika, kad nusikaltimai bus nustatyti, pritraukia organizuotą nusikalstamumą. Europolo teigimu, yra požymių, kad iš šios veiklos gautos pajamos naudojamos terorizmui finansuoti. 2021 m. gruodžio mėn. Komisija priėmė pasiūlymą pakeisti 2008 m. Direktyvą dėl aplinkos apsaugos pagal baudžiamąją teisę. Pasiūlyme daugiausia dėmesio skiriama nusikaltimų aplinkai kategorijų apibrėžčių tobulinimui ir atnaujinimui bei veiksmingų, atgrasančių ir proporcingų sankcijų fiziniams ir juridiniams asmenims rūšių ir dydžių nustatymui. Nauji nusikaltimai apima nusikaltimus, susijusius su neteisėtu miškų naikinimu, ES cheminių medžiagų teisės aktų pažeidimais, neteisėta paviršinio ar požeminio vandens gavyba ir neteisėtu laivų perdirbimu. Pasiūlymu siekiama gerokai sustiprinti teisėsaugos grandinę ir tarpvalstybinį valstybių narių valdžios institucijų ir ES agentūrų bei įstaigų bendradarbiavimą. Europos Parlamentas ir Taryba

³⁷ COM(2022) 480.

³⁸ COM(2022) 732.

priėmė atitinkamas pozicijas dėl pasiūlymo ir šiuo metu tarp jų tuo klausimu vyksta derybos, kurias jie veikiausiai galės užbaigti iki metų pabaigos. Siekiant toliau stiprinti prevenciją ir vykdymo užtikrinimą, reikia įgyvendinti persvarstytą Kovos su neteisėta prekyba laukiniais augalais ir gyvūnais veiksmų planą³⁹.

Nusikalstamo turto susigrąžinimas ir konfiskavimas

Siekiant sužlugdyti organizuotą nusikalstamumą, labai svarbu atimti iš nusikaltėlių neteisėtas pajamas. Todėl be pasiūlymo, kuriuo teisėsaugos institucijoms suteikiama prieiga prie banko sąskaitų informacijos visoje ES⁴⁰ (dėl kurio politinis susitarimas pasiektas 2023 m. birželio mėn.), 2022 m. gegužės mėn. Komisija pateikė pasiūlymą dėl turto susigrąžinimo ir konfiskavimo⁴¹, siekdama sustiprinti turto atsekimo, nustatymo, įšaldymo, konfiskavimo ir valdymo pajėgumus. Pagrindinės pasiūlymo nuostatos yra susijusios su finansinių tyrimų reikalavimais ir papildomais turto susigrąžinimo tarnybų įgaliojimais bei priemonėmis, taip pat platesniam nusikaltimų ratui taikomomis veiksmingesnėmis įšaldymo ir konfiskavimo priemonėmis. Viena iš naujų nusikalstamų veikų, dėl kurių šios priemonės būtų taikomos, yra Sąjungos ribojamųjų priemonių pažeidimas. 2022 m. gruodžio mėn. Komisija priėmė atskirą pasiūlymą dėl Sąjungos ribojamųjų priemonių pažeidimų apibrėžčių ir sankcijų už juos suderinimo. Veiksmingas Sąjungos ribojamųjų priemonių įgyvendinimas ir vykdymo užtikrinimas tebėra vienas iš svarbiausių Komisijos prioritetų. Čia padeda Turto įšaldymo ir areštavimo darbo grupė, kurią Komisija įsteigė reaguodama į Rusijos agresijos karą prieš Ukrainą, darbu. Dėl abiejų pasiūlymų Europos Parlamentas ir Taryba priėmė savo pozicijas, kad iki šių metų pabaigos būtų pasiektas susitarimas.

Kovos su pinigų plovimu dokumentų rinkinys

Pinigų plovimas yra susijęs su beveik visa nusikalstama veikla, iš kurios Europos Sąjungoje nusikalstamu būdu gaunamos pajamos⁴², todėl jis yra vienas pagrindinių kovos su nusikalstamumu ES svertų. 2021 m. liepos mėn. Komisija pateikė plataus užmojo pasiūlymą, kaip sustiprinti ES pinigų plovimo ir terorizmo finansavimo prevencijos priemones⁴³, – keturis pasiūlymus dėl teisėkūros procedūra priimamų aktų, kuriais siekiama tobulinti nusikaltėlių bandymų plauti neteisėtas pajamas arba finansuoti teroristinę veiklą per finansų sistemą prevenciją ir nustatymą. Vieną iš keturių rinkinio iniciatyvų, kuriomis siekiama užtikrinti kriptoturto pervedimų atsekamumą, teisėkūros institucijos priėmė 2023 m. gegužės mėn.⁴⁴ Šis reglamentas bus pradėtas taikyti 2024 m. gruodžio 30 d.: nuo šios datos visi kriptoturto paslaugų teikėjai turės rinkti ir saugoti informaciją apie kriptoturto pervedimo iniciatorių ir gavėją. Likusiais trimis pasiūlymais siekiama i) įsteigti naują ES kovos su pinigų plovimu instituciją, kuri, remdama ir koordinuodama finansinės žvalgybos padalinių darbą, užtikrintų nuoseklią aukštos kokybės priežiūrą visoje vidaus rinkoje, įskaitant rizikingiausių tarpvalstybinių subjektų priežiūrą, ii) nustatyti suderintas taisykles privačiam sektoriui, be kita ko, nustatyti ES masto 10 000 EUR ribą stambiems mokėjimams grynaisiais pinigais už paslaugas ir prekes, ir iii) sustiprinti kompetentingų institucijų įgaliojimus ir bendradarbiavimo priemones. Tikimasi, kad šis dokumentų rinkinys labai sustiprins ES pajėgumą kovoti su pinigų

³⁹ COM(2022) 581.

⁴⁰ COM(2021) 429.

⁴¹ COM(2022) 245.

⁴² Europol, *Enterprising criminals – Europe's fight against the global networks of financial and economic crime* (liet. „Verslūs nusikaltėliai. Europos kova su pasauliniais finansinių ir ekonominių nusikaltimų tinklais“), 2020 m.

⁴³ COM(2021) 420.

⁴⁴ 2023 m. gegužės 31 d. Reglamentas (ES) 2023/1113 dėl informacijos, teikiamos pervedant lėšas ir tam tikrą kriptoturta, kuriuo iš dalies keičiama Direktyva (ES) 2015/849.

plovimu ir apsaugoti ES piliečius nuo terorizmo ir organizuoto nusikalstamumo. Šiuo metu teisėkūros institucijos derasi dėl trijų dar nepriimtų pasiūlymų, siekdamos iki dabartinės sudėties Parlamento kadencijos pabaigos pasiekti susitarimą dėl šio dokumentų rinkinio.

Komisija ragina Europos Parlamentą ir Tarybą kuo skubiau, bet kuriuo atveju iki dabartinės sudėties Europos Parlamento kadencijos pabaigos, užbaigti tarpinstitucines derybas dėl šių dar nebaigtų nagrinėti dokumentų:

- pasiūlymo dėl Direktyvos dėl turto susigrąžinimo ir konfiskavimo;
- pasiūlymo dėl direktyvos, kuria siekiama suderinti Sąjungos ribojamųjų priemonių pažeidimų apibrėžtis ir sankcijas už juos;
- pasiūlymo dėl Kovos su prekyba žmonėmis direktyvos;
- pasiūlymo dėl direktyvos, kuria gerinama aplinkos apsauga baudžiamosios teisės priemonėmis;
- pasiūlymo dėl kovos su pinigų plovimu dokumentų rinkinio;
- pasiūlymo atnaujinti galiojančius teisės aktus dėl civilinių šaunamųjų ginklų importo, eksporto ir tranzito.

Komisija ragina valstybes nares, ES agentūras ir įstaigas:

- kartu dirbti siekiant 2023 ir 2024 m. įgyvendinti 17 ES kovos su prekyba narkotikais ir organizuotu nusikalstamumu gairių veiksmų.

V. Stipri Europos saugumo ekosistema

Per pastaruosius keletą metų grėsmės saugumui tampa vis labiau tarpvalstybinio pobūdžio, todėl reikia tolesnės sąveikos ir glaudesnio bendradarbiavimo visais lygmenimis. Nuo tada, kai buvo priimta Saugumo sąjungos strategija, imtasi svarbių iniciatyvų siekiant kuo labiau suaktyvinti tarpvalstybinį bendradarbiavimą, racionalizuoti ir atnaujinti turimas priemones ir procedūras tiek prie išorės sienų, tiek Šengeno erdvėje, taip pat gerinti teisėsaugos ir teisminių institucijų keitimasi informacija, kad būtų geriau kovojama su organizuotu nusikalstamumu. Šiomis aplinkybėmis veiksmingas keitimosi duomenimis sąveikumo sistemos įgyvendinimas yra svarbus veiksnys siekiant stiprinti saugumą ir veiksmingą Europos atsaką į tarpvalstybines grėsmes, kuris kartu užtikrina laisvą judėjimą ES viduje.

Aktyvesnis keitimasis informacija Šengeno erdvėje: Išankstinė informacija apie keleivius (API), keleivio duomenų įrašai (PNR) ir Priumas II

2022 m. gruodžio mėn. Komisijos priimti du API pasiūlymai⁴⁵ turėtų padidinti Sąjungos vidaus saugumą, nes valstybių narių teisėsaugos institucijoms būtų suteiktos papildomos kovos su sunkiais nusikaltimais ir terorizmu priemonės. Visų pirma, kartu su oro transportu keliaujančių asmenų PNR naudojama išankstinė informacija apie ES vidaus skrydžių keleivius sudarytų sąlygas valstybių narių teisėsaugos institucijoms gerokai padidinti savo tyrimų veiksmingumą ir imtis tikslingesnių intervencinių veiksmų. Svarbu, kad siūlomos taisyklės būtų priimtose kuo greičiau: tai ne tik padėtų kovoti su organizuotu nusikalstamumu ir terorizmu, bet ir gerokai sumažintų poreikį sistemingai tikrinti visus keliautojus, kai laikinai atnaujinami patikrinimai kertant vidaus sienas, taigi palengvėtų kelionės oro transportu ir padaugėtų judėjimo laisvės.

⁴⁵ COM(2022) 729, COM(2022) 73.

2023 m. rugsėjo 6 d. Europos Komisija rekomendavo Tarybai leisti vesti derybas su Šveicarija, Islandija ir Norvegija dėl susitarimų dėl PNR duomenų perdavimo. Priėmus šias tris rekomendacijas ES išorės politika PNR klausimu taptų nuoseklesnė ir veiksmingesnė.

Keitimuisi duomenimis skirtos Priumo taisyklės yra kasdien naudojamos policijos kovos su organizuotu nusikalstamumu, narkotikais, terorizmu, seksualiniu išnaudojimu ir prekyba žmonėmis reikmėms. Pasiūlymu dėl reglamento dėl automatinio keitimosi duomenimis policijos bendradarbiavimo srityje („Priumas II“)⁴⁶ peržiūrima esama Priumo sistema, siekiant panaikinti informacijos spragas ir sustiprinti nusikalstamų veikų prevenciją, atskleidimą ir tyrimą ES. Peržiūrėtos automatinio keitimosi duomenimis policijos bendradarbiavimo srityje taisyklės kartu su jau priimta Tarybos rekomendacija dėl operatyvinio tarpvalstybinio bendradarbiavimo stiprinimo ir Direktyva dėl teisėsaugos institucijų keitimosi informacija, yra paskutiniai šios kadencijos pasiūlymai dėl policijos bendradarbiavimo. Greitas šių susijusių priemonių priėmimas ir įgyvendinimas pagerintų, palengvintų ir paspartintų keitimąsi duomenimis tarp teisėsaugos institucijų ir padėtų nustatyti nusikaltėlius.

Visiškai sąveiki sienų valdymo sistema saugios, stiprios, skaitmeninės ir vieningos Šengeno erdvės labui

Gerai veikianti Šengeno erdvė be vidaus sienų priklauso nuo valstybių narių tarpusavio pasitikėjimo. Jis savo ruožtu grindžiamas veiksminga kontrole prie Sąjungos išorės sienų arba alternatyviomis priemonėmis valstybių narių teritorijoje. Komisijos siūlomą Šengeno sienų kodekso pakeitimu⁴⁷ nustatoma, kaip valstybėms narėms geriau pasinaudoti vidaus sienų kontrolės alternatyvomis, galinčiomis užtikrinti aukštą saugumo lygį. Šengeno sienų kodekso pakeitimą svarbu priimti ir įgyvendinti iki galo, kad būtų užtikrintas aukštas ir proporcingas saugumo lygis Šengeno erdvėje. Siekiant geriau remti nacionalinių valdžios institucijų darbą, kuriuo užtikrinamas saugumas ir sienų valdymas, taip pat toliau plėtojama nauja ES informacinių sistemų struktūra. Ją sudaro atnaujinta Šengeno informacinė sistema, Europos kelionių informacijos ir leidimų sistema, atvykimo ir išvykimo sistema, atnaujinta Vizų informacinė sistema ir visiškai saugiai sistemas susiejanti sąveikumo sistema. Iki galo sukūrus šią naują struktūrą, nacionalinės valdžios institucijos gaus visapusiškesnę ir patikimesnę saugumo informaciją. Visi sąveikumo sistemos komponentai yra labai svarbūs, o tai reiškia, kad delsimas dėl vieno aspekto arba vienoje valstybėje narėje lemia diegimo vėlavimą visiems. Atvykimo ir išvykimo sistemos techninio plėtojimo vėlavimai turėtų būti kuo labiau sumažinti, kad ji galėtų pradėti veikti kuo greičiau ir būtų galima įdiegti visus pagrindinius sąveikumo sistemos elementus.

Pasiūlymas dėl tikrinimo⁴⁸ padidintų saugumą Šengeno erdvėje, nes būtų suvienodintos trečiųjų šalių piliečių, kurie neatitinka Šengeno sienų kodekse nurodytų atvykimo sąlygų, tapatybės nustatymo ir jų sveikatos ir saugumo patikrinimų prie išorės sienų taisyklės. Šių tikslų padėtų siekti siūloma sistema EURODAC: joje po patikrinimo būtų rodoma, kad asmuo gali kelti grėsmę vidaus saugumui. Tai savo ruožtu palengvintų siūlomo Prieglobsčio ir migracijos valdymo reglamento įgyvendinimą. Komisija ragina teisėkūros institucijas greitai, iki šio teisėkūros laikotarpio pabaigos, užbaigti derybas dėl šių dokumentų.

Kova su korupcija

⁴⁶ COM(2021) 784.

⁴⁷ COM(2021) 891.

⁴⁸ COM(2020) 612.

Korupcija daro didelę žalą mūsų demokratijai, ekonomikai ir mūsų saugumui, nes ji sudaro sąlygas organizuotam nusikalstamumui ir priešiškam užsienio kišimuisi. Sėkminga korupcijos prevencija ir kova su ja yra labai svarbios tiek siekiant apsaugoti ES vertybes ir ES politikos veiksmingumą, tiek siekiant puoselėti teisinę valstybę ir pasitikėjimą tais, kurie vykdo valdžios funkcijas, bei viešojo sektoriaus institucijomis. Kaip 2022 m. pranešime apie Sąjungos padėtį buvo iš anksto paskelbusi Pirmininkė U. von der Leyen, 2023 m. gegužės 3 d. Komisija priėmė kovos su korupcija priemonių rinkinį⁴⁹. Komisijos pasiūlyme dėl direktyvos dėl kovos su korupcija numatytos griežtesnės taisyklės, pagal kurias visoje ES kriminalizuojami korupcijos nusikaltimai ir suderinamos bausmės. Pasiūlymu taip pat sudaromos sąlygos veiksmingai vykdyti tyrimus ir baudžiamąjį persekiojimą ir daug dėmesio skiriama prevencijai ir sąžiningumo kultūros, kurioje korupcija netoleruojama, kūrimui. Europos Parlamente ir Taryboje pradėtos diskusijos dėl šio pasiūlymo. Be to, valstybių narių prašoma įgyvendinti rekomendacijas, susijusias su 2023 m. liepos 5 d. priimtos 2023 m. teisinės valstybės principo taikymo ataskaitos kovos su korupcija skyriumi. Vyriausiojo įgaliojimo pasiūlyme, kuriam pritaria Komisija, taip pat siūloma nustatyti specialų bendros užsienio ir saugumo politikos (BUSP) sankcijų režimą, skirtą kovai su sunkiais korupcijos nusikaltimais visame pasaulyje.

Nukentėjusiųjų teisių stiprinimas

2023 m. liepos 12 d. Komisija pasiūlė Nusikaltimų aukų teisių direktyvos pakeitimus, kuriais siekiama padidinti nukentėjusiųjų galimybes gauti informaciją, paramą ir apsaugą, dalyvauti baudžiamajame procese ir pasinaudoti teise gauti kompensaciją. Vienas iš bendrų peržiūros tikslų – prisidėti prie aukšto saugumo lygio sukūrimo saugesnę aplinką nukentėjusiesiems, kad būtų paskata pranešti apie nusikaltimus ir mažėtų represijų baimė.

Komisija ragina Europos Parlamentą ir Tarybą skubiai, bet kuriuo atveju iki šios Europos Parlamento kadencijos pabaigos, užbaigti tarpinstitucines derybas dėl šių dar nepriimtų dokumentų:

- pasiūlymo dėl Priemo II reglamento;
- pasiūlymų dėl išankstinės informacijos apie keleivius (API);
- pasiūlymų dėl kovos su korupcija, visų pirma dėl specialaus bendros užsienio ir saugumo politikos (BUSP) sankcijų režimo sukūrimo;
- pasiūlymo iš dalies pakeisti Šengeno sienų kodekso reglamentą;
- pasiūlymo dėl Nusikaltimų aukų teisių direktyvos;
- pasiūlymo dėl tikrinimo.

Komisija ragina valstybes nares:

- užtikrinti, kad atvykimo ir išvykimo sistema įsigaliojūt kuo greičiau – kad būtų užbaigtas ES keitimosi informacija struktūros įgyvendinimas.

VI. Įgyvendinimas

Visos Europos saugumo užtikrinimas yra bendra atsakomybė, kai kiekvienas subjektas turi atlikti savo vaidmenį: Komisija ir teisėkūros institucijos priima naujas, griežtas, išsamias, praktiškas taisykles, valstybės narės laiku perkelia, įgyvendina ir taiko tokias taisykles, o įvairios institucijos, organizacijos ir suinteresuotieji subjektai vykdo operatyvinę veiklą vietoje.

⁴⁹ COM(2023) 234.

Svarbų vaidmenį atlieka ir ES agentūros, veikiančios teisingumo, vidaus reikalų ir kibernetinio saugumo srityse, ir šis vaidmuo dar labiau padidėjo neseniai išplėtus jų kompetenciją.

Sustiprinta ES finansavimo gavėjų patikra

Vykdydama ES biudžetą, Komisija privalo užtikrinti, kad ES finansavimo gavėjai gerbtų ES vertybes. Mechanizmai ir kontrolės sistemos, pagal kuriuos nustatoma, kas gali gauti ES finansavimą, jau yra patikimi, o vykstančiose derybose dėl naujos redakcijos Finansinio reglamento taip pat siekiama suteikti Komisijai daugiau teisinių priemonių prireikus imtis veiksmų. Be to, Komisija šiuo metu ieško būdų, kaip dar labiau sugriežtinti dabartinių ir galimų būsimų ES finansavimo gavėjų tikrinimą, ir tobulina pareigos gerbti ES vertybes gaires ir gaires dėl pasekmių, kurios būtų pažeidus ES vertybes. Taip bus aiškiau apibrėžta tiek paramos gavėjų, tiek ES lygmens kontrolę vykdančių subjektų atsakomybė ir parodytas galima pavyzdys nacionalinio lygmens veiksams. Pažeidus finansavimo sąlygas, Komisija nedvejodama sustabdo bendradarbiavimą su atitinkamo projekto paramos gavėjais ir prireikus susigrąžins lėšas. Svarbu, kad valstybės narės aktyviai dalytųsi informacija su Komisija, kai jos žino apie galimą riziką, susijusią su skirti ES finansavimą prašančiomis organizacijomis.

Pažeidimai

Saugumo srityje Komisija yra atlikusi daug pažeidimo nagrinėjimo procedūrų. Pavyzdžiui, 2023 m. buvo inicijuota daug pažeidimo bylų dėl 2021 m. Reglamente dėl teroristinio turinio sklaidos internete⁵⁰ nustatytų įpareigojimų nevykdymo (16 valstybių narių), o 2022 ir 2023 m. 20 valstybių narių gavo papildomus oficialius pranešimus dėl netinkamo 2011 m. Direktyvos dėl kovos su seksualine prievarta prieš vaikus⁵¹ įgyvendinimo. Vis dar nagrinėjama daug pažeidimo bylų dėl nacionalinės teisės aktų neatitikties 2017 m. Direktyvai dėl kovos su terorizmu⁵² ir dėl to, kad į nacionalinę teisę neperkeltos taisyklės, kuriomis palengvinamas finansinės ir kitos informacijos naudojimas tam tikrų nusikalstamų veikų prevencijos, nustatymo, tyrimo ar baudžiamojo persekiojimo už jas tikslais⁵³. Kitos sritys, kuriose vyksta pažeidimo nagrinėjimo procedūros yra, be kita ko, šaunamųjų ginklų reglamentavimo teisės aktai; taisyklės dėl psichoaktyviųjų medžiagų, naudojamų narkotikuose, kova su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu, kova su pinigų plovimu, keitimasis informacija apie teistumą tarp ES valstybių narių ir Nusikaltimų aukų teisių direktyva. Valstybėms narėms, įgyvendinančioms sutartas iniciatyvas ir veiksmus, skirta parama (techninė ir finansinė), o Komisija ir toliau gali padėti valstybėms narėms optimizuoti įgyvendinimą.

Stebėseną atliekant Šengeno vertinimus ir taikant naują valdymo sistemą

Šengeno *acquis* taikymo vertinimo ir stebėjimo mechanizmas ir toliau padeda veiksmingai įgyvendinti Šengeno taisykles, kuriomis siekiama didinti saugumą erdvėje be vidaus kontrolės. 2023 m. buvo atlikti pirmieji vertinimai pagal sustiprintą Šengeno *acquis* taikymo vertinimo ir stebėjimo mechanizmą, kad būtų galima laiku nustatyti ir pašalinti strateginį pažeidžiamumą, kuris daro tarpvalstybinį poveikį saugumui ir saugai Europos Sąjungoje. Be to, 2023 m. Komisija pradėjo teminį su didelio masto prekyba narkotikais susijusį Šengeno sistemos

⁵⁰ Reglamentas (ES) 2021/784 dėl teroristinio turinio sklaidos internete klausimo sprendimo.

⁵¹ Direktyva (ES) 2011/93 dėl kovos su seksualine prievarta prieš vaikus.

⁵² 2017 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva (ES) 2017/541 dėl kovos su terorizmu, pakeičianti Tarybos pamatinį sprendimą 2002/475/TVR ir iš dalies keičianti Tarybos sprendimą 2005/671/TVR.

⁵³ 2019 m. birželio 20 d. Europos Parlamento ir Tarybos direktyva (ES) 2019/1153, kuria nustatomos taisyklės dėl paprastesnio finansinės ir kitos informacijos naudojimo tam tikrų nusikalstamų veikų prevencijos, nustatymo, tyrimo ir baudžiamojo persekiojimo už jas tikslais ir kuria panaikinamas Tarybos sprendimas 2000/642/TVR.

vertinimą, kad įvertintų valstybių narių, kurios kovoje su neteisėtu narkotikų gabenimu į ES susiduria su panašiomis problemomis, praktika. Atliekant šiuos vertinimus atidžiau ir visapusiškiau nagrinėjami Šengeno sistemos saugumo elementai. Remdamasi periodinių, teminių ir neanonsuotų Šengeno sistemos vertinimų rezultatais, 2023 m. birželio mėn. Taryba nustatė 2023–2024 m. Šengeno ciklo prioritetus. Taryba išdėstė prioritėtines sritis, kurioms reikia papildomo postūmio saugesnei ir tvirtesnei Šengeno erdvei užtikrinti. Veiksmingas ir greitas šių prioritetų įgyvendinimas ir geresnis Šengeno tarybos politikos koordinavimas dar labiau sustiprins kovą su organizuotu nusikalstamumu ir maksimaliai padidins tarpvalstybinį operatyvinį bendradarbiavimą.

ES agentūrų ir įstaigų vaidmuo

Partnerystė labai padeda įgyvendinti saugumo sąjungos iniciatyvas, nes siekiant konkrečių rezultatų reikalingas įvairių nacionalinių ir ES valdžios institucijų ir įstaigų darbas. Pavyzdžiui, EMPACT (Europos kovos su nusikalstamumu grėsmėmis daugiadalykė platforma) sudaro sąlygas valstybių narių struktūriniam daugiadalykiam bendradarbiavimui, kurį remia visos ES institucijos, įstaigos ir agentūros (tokios kaip Europolas, FRONTEX, Eurojustas, CEPOL, OLAF, eu-LISA). EMPACT vykdomomis operacijomis, be kita ko, pasitelkiant specialias operatyvines darbo grupes, yra koordinuojamos valstybių narių ir operatyvinių partnerių pastangos kovoti su nusikaltėlių tinklais ir sunkiais nusikaltimais. Dalyvaujant EMPACT vien 2022 m. atlikti 9 922 areštai, konfiskuota daugiau kaip 180 mln. EUR turto ir pinigų, inicijuoti 9 263 tyrimai, nustatyta 4 019 nukentėjusiųjų, konfiskuota daugiau kaip 62 tonos narkotikų, nustatytas 51 ir suimta 12 didelės vertės taikinių, vykdytos operacijos agresijos karo prieš Ukrainą kontekste, visų pirma siekiant kovoti su prekyba žmonėmis ir šalinti su šaunamaisiais ginklais susijusias grėsmes⁵⁴.

FRONTEX, Europos jūrų saugumo agentūra (EMSA) ir Europos žuvininkystės kontrolės agentūra (EŽKA) toliau stiprina bendradarbiavimą pakrančių apsaugos funkcijų srityje, kad padėtų nacionalinėms institucijoms didinti saugą ir saugumą jūroje. Šios agentūros daugiau negu kitos prisidės prie ES jūrų saugumo strategijos įgyvendinimo.

Pagal keletą saugumo sąjungos iniciatyvų atitinkamoms agentūroms buvo skirta naujų pareigų ir užduočių, kartais susijusių su žmogiškaisiais ištekliais.

Europos Sąjungos kibernetinio saugumo agentūra (ENISA)

Kalbant apie pasirengimą incidentams ir reagavimą į juos kibernetinio saugumo didinimo priemonėmis, Komisija ėmėsi trumpalaikio valstybių narių rėmimo veiksmo ir Skaitmeninės Europos programos finansavimą perkelia **Europos Sąjungos kibernetinio saugumo agentūrai (ENISA)**, kad būtų stiprinamas pasirengimas ir padidinti pajėgumai reaguoti į didelius kibernetinius incidentus. Šiais veiksmais grindžiamas 2023 m. balandžio mėn. priimtas pasiūlymas dėl Kibernetinio solidarumo akto ir, kai jį priims teisėkūros institucijos, ENISA gali būti pavesta papildomų užduočių, pavyzdžiui, užtikrinti būsimo Sąjungos kibernetinio saugumo rezervo veikimą, jį administruoti arba rengti incidentų apžvalgos ataskaitą įvykus didelio masto kibernetinio saugumo incidentams. Pagal siūlomą Kibernetinio atsparumo aktą ENISA būtų pavesta gauti pranešimus iš gamintojų apie produktų su skaitmeniniais elementais pažeidžiamumą ir incidentus, darančius poveikį tų produktų saugumui, o šiuos pranešimus ENISA turėtų persiųsti atitinkamoms reagavimo į kompiuterių saugumo incidentus tarnyboms

⁵⁴ EMPACT 2022 m. rezultatų suvestinė – https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

(CSIRT) arba į atitinkamus valstybių narių kontaktinius punktus. Taip pat tikimasi, kad ENISA kas dvejus metus parengs kibernetinio saugumo rizikos produktuose su skaitmeniniais elementais naujų tendencijų techninę ataskaitą ir pateiks ją TIS bendradarbiavimo grupei.

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras

Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centras (ECCC) kartu su Nacionalinių koordinavimo centrų tinklu yra nauja Sąjungos įstaiga, remianti inovacijas ir pramonės politiką kibernetinio saugumo srityje. Ši ekosistema sustiprins kibernetinio saugumo technologijų bendruomenės pajėgumus, išlaikys kompetenciją mokslinių tyrimų srityje ir padidins Sąjungos pramonės konkurencingumą šioje srityje. ECCC ir Nacionalinių koordinavimo centrų tinklas priims sprendimus dėl strateginių investicijų ir telks Sąjungos, jos valstybių narių ir netiesiogiai pramonės išteklius, kad būtų gerinami ir stiprinami technologiniai ir pramoniniai kibernetinio saugumo pajėgumai. Todėl ECCC tenka svarbus vaidmuo siekiant Skaitmeninės Europos programos ir programos „Europos horizontas“ kibernetinio saugumo plataus užmojo tikslų.

ECCC jau įdarbino daugiau kaip pusę reikalingų darbuotojų ir netrukus įdarbins vykdomąjį direktorių. Jau vykdomas darbas apima programos DIGITAL kibernetinio saugumo dalį ir naują strateginę technologijų kūrimo ir diegimo darbotvarkę⁵⁵. Joje nustatomi prioritetingi veiksmai, kuriais siekiama padėti MVĮ kurti ir naudoti strategines kibernetinio saugumo technologijas, paslaugas ir procesus; remti ir auginti profesionalią darbo jėgą; stiprinti mokslinių tyrimų, plėtros ir inovacijų ekspertines žinias platesnėje Europos kibernetinio saugumo ekosistemoje.

Europolas

Įgijęs visiškai naujus įgaliojimus, **Europolas** bus geriau pasirengęs padėti valstybėms narėms kovoti su organizuotu nusikalstamumu. Vienas iš pagrindinių prioritetų yra kova su prekyba narkotikais, nes prekybos narkotikais problema tampa vis aktualesnė ir vis labiau kenkia ES piliečių saugumui. 2023 m. gegužės 15 d. gavusi Europos Sąjungos Tarybos leidimą, Komisija aktyviai stengiasi sudaryti tarptautinius susitarimus su Bolivija, Brazilija, Ekvadoru, Meksika ir Peru dėl keitimosi asmens duomenimis su Europolu siekiant užkirsti kelią sunkiems nusikaltimams bei terorizmui ir su jais kovoti.

Eurojustas

Eurojustas, kuris daugiau kaip 20 metų teikia teisminę paramą nacionalinėms institucijoms, kovojančiomis su įvairiais sunkiais ir sudėtingais tarpvalstybiniais nusikaltimais patirtį, užima solidžią vietą ES laisvės, saugumo ir teisingumo erdvėje. Siekdama stiprinti visų suinteresuotųjų subjektų bendradarbiavimą, Komisija derasi dėl tarptautinių susitarimų, kurie palengvintų Eurojusto ir 13 trečiųjų šalių bendradarbiavimą dėl keitimosi asmens duomenimis siekiant kovoti su organizuotu nusikalstamumu ir terorizmu⁵⁶. Derybos su Armėnija ir Libanu jau baigtos, su Alžyru ir Kolumbija tebevyksta, o su Bosnija ir Hercegovina pradėtos. Komisija ragina Europos Parlamentą ir Tarybą iki Parlamento kadencijos pabaigos baigti sudaryti susitarimus su šiomis šalimis, kad būtų sustiprintas tarptautinis teisminis bendradarbiavimas ir išplėsta kova su tarpvalstybinio nusikalstamumu.

Europos prokuratūra

⁵⁵ https://cybersecurity-centre.europa.eu/strategic-agenda_en

⁵⁶ Alžyras, Argentina, Armėnija, Bosnija ir Hercegovina, Brazilija, Egiptas, Izraelis, Jordanija, Kolumbija, Libanas, Marokas, Tunisas ir Turkija.

Nuo operatyvinės veiklos pradžios 2021 m. birželio mėn. **Europos prokuratūra** pasirodė esanti galinga Sąjungos priemonė Sąjungos biudžetui kenkiančioms nusikalstamoms veikoms (įskaitant, kai kalbama apie nusikaltimus Sąjungos biudžetui, su dalyvavimu nusikalstamoje organizacijoje susijusias nusikalstamas veikas) tirti ir baudžiamajam persekiojimui už jas vykdyti. Komisija ragina valstybes nares, kurios dar neprisideda prie tvirtesnio bendradarbiavimo dėl Europos prokuratūros, kuo greičiau į ją įsitraukti, kad būtų išnaudotas visas Europos prokuratūros potencialas apsaugoti ES mokesčių mokėtojų pinigus.

EUDA

2023 m. birželio mėn. teisėkūros institucijoms patvirtinus naujus įgaliojimus, esamas Europos narkotikų ir narkomanijos stebėsenos centras (EMCDDA) taps visateise didesnes funkcijas atliekančia agentūra – **Europos Sąjungos narkotikų agentūra (EUDA)**. Agentūra galės visapusiškiau įvertinti naujas sveikatos ir saugumo problemas, kurias kelia neteisėti narkotikai, ir veiksmingiau prisidėti prie valstybių narių ir tarptautiniu lygmeniu vykdomo darbo. Pagrindinė agentūros užduotis ir toliau bus duomenų rinkimas, analizė ir sklaida, tačiau išplėsti įgaliojimai taip pat leis agentūrai plėtoti bendrus grėsmių sveikatai ir saugumui vertinimo pajėgumus, kad būtų galima nustatyti kylančias grėsmes, įskaitant kombinuotą narkotikų vartojimą, stiprinti bendradarbiavimą per nacionalinius ryšių punktus ir sukurti laboratorijų tinklą, kuris teiktų agentūrai teismo ekspertizes ir toksikologinę informaciją. Tai padės agentūrai skelbti perspėjimus, kai rinkoje atsiranda ypač pavojingų medžiagų, ir didinti informuotumą.

Komisija ragina Europos Parlamentą ir Tarybą kuo skubiau, bet kuriuo atveju iki šios Europos Parlamento kadencijos pabaigos, užbaigti tarpinstitucines derybas dėl šių dar nebaigtų nagrinėti dokumentų:

- pasiūlymo išdėstyti Finansinį reglamentą nauja redakcija.

Komisija ragina valstybes nares:

- aktyviai dalytis informacija su Komisija, kai jos žino apie galimą riziką, susijusią su organizacijomis, prašančiomis skirti ES finansavimą;
- skubiai įgyvendinti 2023–2024 m. Šengeno ciklo prioritetus siekiant saugesnės ir tvirtesnės Šengeno erdvės;
- imtis veiksmų reaguojant į prieš jas pradėtas pažeidimo nagrinėjimo procedūras, kad būtų užtikrintas tinkamas atitinkamų teisės aktų perkėlimas į nacionalinę teisę.

VII. Išvada

Pastaruosius trejus metus nuolat ir ryžtingai stengtasi, kad užmojis sukurti ES saugumo sąjungą neštų vaisių. Visose saugumo politikos srityse padaryta didžiulė pažanga. Grėsmėms nuolat kintant reikia visą laiką dėti pastangas su nauja motyvacija. Su teisės aktų sistema susijusį darbą reikia užbaigti likus pakankamai laiko iki Parlamento kadencijos pabaigos 2024 m. pavasarį. Valstybės narės visą laiką yra atsakingos už naujų teisės aktų perkėlimą į nacionalinę teisę, įgyvendinimą ir taikymą. Įgyvendinimui reikia suderintų pastangų, be kita ko, su ES agentūrų parama, o labai dažnai ir vis tvirtiau bendradarbiaujant su mūsų tarptautiniais partneriais.

Tik bendromis ir ryžtingomis visų suinteresuotųjų šalių pastangomis pasieksime tokį ES saugos ir saugumo lygį, kurio tikisi piliečiai, o dabartinėmis aplinkybėmis kiekvienas subjektas turėtų atlikti savo vaidmenį stiprinant ES saugumą.