Rådet for
Den Europæiske Union

Bruxelles, den 18. oktober 2023
(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**

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	18. oktober 2023
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2023) 665 final
Vedr.:	MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET om den sjette statusrapport om gennemførelsen af strategien for EU's sikkerhedsunion

Hermed følger til delegationerne dokument COM(2023) 665 final.

Bilag: COM(2023) 665 final

EUROPA-
KOMMISSIONEN

Bruxelles, den 18.10.2023
COM(2023) 665 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om den sjette statusrapport om gennemførelsen af strategien for EU's sikkerhedsunion

I. Indledning

For tre år siden vedtog Kommissionen strategien for sikkerhedsunionen 2020-2025[1], der fastlægger Unionens vigtigste prioriteter på sikkerhedsområdet. Siden da er der gjort store fremskridt inden for alle fire søjler i strategien — gennem vedtagelse af skelsættende lovgivning på alle områder lige fra beskyttelse af kritiske enheder til styrkelse af cyberrobustheden. Trusselsbilledet på sikkerhedsområdet i Europa og vores nabolande har imidlertid samtidigt udviklet sig løbende. Terrorangrebene på en skole i Frankrig og på gaden i Bruxelles i de seneste dage er en kraftig påmindelse om, at det haster med at tilpasse og styrke vores sikkerhedsarkitektur. Faren ved cyberangreb vokser fortsat, også i takt med at ondsindede aktører vælger side i de igangværende konflikter. Der kommer stadig flere hybride trusler, herunder i form af desinformation. Europol har identificeret den russiske angrebskrig mod Ukraine som årsagen til en betydelig stigning i antallet af cyberangreb på EU-mål med store angreb, der er politisk motiveret og koordineret af prorussiske hackergrupper[2]. Dette er sket i form af blokering af internetadgangen og afbrydelse af vigtige tjenester såsom energinet[3].

Strategien for sikkerhedsunionen blev udformet med henblik på at sætte EU i stand til bedre at modstå udviklingen i trusselsbilledet. Da vi har stået over for kriser som følge af pandemien og krigen, har begivenhederne vist betydningen af den tilgang, der er valgt i strategien — vores vilje til at skabe sammenhæng i hele EU's sikkerhedsøkosystem og nedbryde skellene mellem cyberdimensionen og den fysiske dimension af sikkerhed, herunder bekæmpelse af organiseret kriminalitet og terrorisme samt bekæmpelse af radikalisering.

Årvågenhed kræver imidlertid, at vi løbende bør undersøge, hvad der halter i vores bestræbelser på at beskytte vores borgere. I strategien er der fokus på prioriterede områder, hvor Unionen kan tilføre merværdi for at støtte medlemsstaterne i at fremme sikkerheden for alle, der bor i Europa. Siden vedtagelsen er der blevet taget fat på alle tiltag i strategien, og nye tiltag er blevet indarbejdet for at imødegå aktuelle sikkerhedsudfordringer.

Samlet set har Kommissionen fremlagt 36 lovgivningsinitiativer inden for rammerne af strategien for sikkerhedsunionen. For mere end halvdelen af disse forslag er de interinstitutionelle forhandlinger allerede afsluttet med solid ny lovgivning, jf. tabellen i bilaget. Flere vigtige initiativer, som Kommissionen har foreslået, er imidlertid stadig under forhandling i Europa-Parlamentet og Rådet. Da den nuværende valgperiode udløber med valget til Europa-Parlamentet i juni 2024, skal der gøres en hurtig indsats for at få afsluttet disse udestående lovgivningssager, således at borgerne kan drage fuld fordel af sikkerhedsunionen. I denne sjette statusrapport om sikkerhedsunionen er der derfor fokus på at skitsere de meget vigtige lovgivningsmæssige og ikkelovgivningsmæssige sager vedrørende sikkerhedsunionen vedtaget af Kommissionen, hvor der skal gøres mere for at afslutte sagerne og sikre en effektiv gennemførelse.

Med hensyn til de EU-love, der allerede er opnået enighed om, vil nyttevirkningen først kunne mærkes, når de gennemføres i praksis. I arbejdet skal der være fokus på, at medlemsstaterne omsætter, gennemfører og anvender dem korrekt og fuldt ud. I 2023 fortsatte Kommissionen

[1] COM(2020) 605.

[2] Distributed denial of service-angreb (DDoS-angreb): se Europol Spotlight-rapport "Cyber-attacks: the apex of crime-as-a-service", 13.9.2023.

[3] Wipere (malware) er blevet kraftigt benyttet under konflikten i Ukraine til at ødelægge data og systemer, og har f.eks. blokeret internetadgangen for tusindvis af abonnenter i EU og et stort tysk energiselskab, hvis fjernovervågningsadgang til over 5 800 vindmøller blev blokeret. Europa-Parlamentets undersøgelse fra september 2023 med titlen "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict" — PE 702.594.

med at sikre gennemførelsen af strategien for EU's sikkerhedsunion ved at anvende sine institutionelle beføjelser til at indlede traktatbrudsprocedurer, når medlemsstaterne ikke havde gennemført eller ikke havde gennemført EU-lovgivningen korrekt.

I denne rapport opsummeres det også, hvor medlemsstaternes og/eller EU-agenturernes indsats er af central betydning for gennemførelsen. EU's agenturer spiller en afgørende rolle med hensyn til at støtte gennemførelsen af initiativer vedrørende sikkerhedsunionen, og deres ansvar har udviklet sig i de seneste år. I rapporten skitseres nogle af de vigtigste nye opgaver, som de har fået tildelt for at yde øget støtte til medlemsstaterne i forbindelse med gennemførelsen af centrale initiativer inden for rammerne af sikkerhedsunionen.

Desuden har den geopolitiske situation understreget den eksterne sikkerheds betydning for vores interne sikkerhed. En stærkere intern EU-ramme på sikkerhedsområdet er uløseligt forbundet med stærkere partnerskaber og samarbejde med tredjelande. EU skal fortsat aktivt tilstræbe at sikre, at det globale engagement bidrager til at sikre borgernes sikkerhed hjemme.

II. Et fremtidssikret sikkerhedsmiljø

Kritisk infrastrukturs cybersikkerhed og modstandsdygtighed

I forbindelse med sikkerhedsunionen har Unionen forpligtet sig til at sørge for, at alle europæiske borgere og virksomheder er godt beskyttet både online og offline, og til at fremme et åbent, sikkert og stabilt cyberspace. På trods heraf udgør en stigning i cybersikkerhedshændelsers omfang, frekvens og virkning en stor trussel for net- og informationssystemers funktion og for det indre marked. Ruslands angrebskrig mod Ukraine har yderligere forværret denne trussel, og de nuværende geopolitiske spændinger forværres af angreb udført af en lang række forskellige statslige, kriminelle og hacktivistiske aktører. Sabotagen af Nord Stream-rørledningerne sidste efterår understregede, at vigtige sektorer såsom energi, digital infrastruktur, transport og rummet er afhængige af modstandsdygtig kritisk infrastruktur. Den nylige hændelse vedrørende en undersøisk gasrørledning og et undersøisk datakabel i Estland og Finland illustrerer behovet for et højt niveau af beredskab til at håndtere denne type situationer. Selv om årsagen til skaden fortsat er uklar, og undersøgelserne er i gang, har udvekslingen af oplysninger på forskellige niveauer mellem medlemsstaterne og Kommissionen været opmuntrende. Afbrydelserne havde ingen umiddelbare virkninger med hensyn til internetkonnektivitet eller gasforsyningssikkerheden på europæisk eller lokalt plan. Dette er et tegn på de fremskridt, der er gjort, og den styrkede beredskabsindsats i de seneste måneder.

En klar og solid retlig ramme er derfor afgørende for at sikre beskyttelsen og modstandsdygtigheden af disse kritiske infrastrukturer. I denne forbindelse blev der opnået et afgørende gennembrud med den parallelle vedtagelse af det reviderede direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2)[4] og direktivet om kritiske enheders modstandsdygtighed (CER)[5], som begge trådte i kraft den 16. januar 2023. Nu opfordres medlemsstaterne indtrængende til hurtigt og fuldt ud at gennemføre

[4] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og direktiv (EU) 2018/1972 (NIS 2-direktivet).

[5] Europa-Parlamentets og Rådets direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed og om ophævelse af Rådets direktiv 2008/114/EF.

disse grundlæggende retsakter senest den 17. oktober 2024 for at indføre en solid EU-ramme for beskyttelse af kritisk infrastruktur i Unionen mod fysiske trusler og cybertrusler.

I juli 2023 fastsatte Kommissionen i en delegeret forordning væsentlige tjenester i de 11 sektorer, der er omfattet af CER-direktivet[6]. Det næste skridt er, at medlemsstaterne foretager risikovurderinger af disse tjenester. Efter Rådets henstilling[7] af 8. december 2022 er arbejdet med stresstest af kritisk infrastruktur blevet intensiveret, begyndende med energisektoren, og med styrkelsen af samarbejdet med NATO og centrale partnerlande. Dette arbejde blev udmøntet i en rapport fra EU-NATO-taskforcen om kritisk infrastrukturs modstandsdygtighed i juni 2023, som kortlægger de aktuelle sikkerhedsudfordringer for kritisk infrastruktur i fire nøglesektorer (energi, transport, digital infrastruktur og rummet) og indeholder anbefalinger til styrkelse af modstandsdygtigheden. Anbefalingerne, herunder om øget koordinering, informationsudveksling og øvelser, gennemføres af EU's og NATO's personale inden for rammerne af den strukturerede dialog om modstandsdygtighed.

Sideløbende hermed vedtog Kommissionen den 6. september 2023 et forslag[8] til Rådets henstilling om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans. Den 4. oktober 2023 blev der afholdt en øvelse i form af en scenariebaseret drøftelse af planen for at afprøve, hvordan den ville finde anvendelse i praksis, og denne drøftelse indgår i de igangværende forhandlinger om forslaget i Rådet.

Efter opfordringer fra Rådet[9] har Kommissionen, den højtstående repræsentant og NIS-samarbejdsgruppen gennemført risikoevalueringer og opstillet risikoscenarier ud fra et cybersikkerhedsmæssigt perspektiv. Dette arbejde har i første omgang fokus på telekommunikations- og elsektoren. Inddragelsen af alle relevante agenturer og netværk, civile og militære, sikrer for første gang en omfattende og inklusiv vurdering på EU-plan. Den vil yderligere supplere de koordinerede sikkerhedsrisikovurderinger af kritiske forsyningskæder, der foretages i henhold til NIS 2, og risikovurderingerne og stresstestene af kritisk infrastruktur i sektorer såsom energi, digital infrastruktur, transport og rummet. Af hensyn til koordinering og sammenhæng bør disse aktiviteter bygge videre på hinanden for at bidrage til at fastlægge en standardtilgang, og de bør danne grundlag for udviklingen af fremtidige øvelser. En vellykket gennemførelse af disse foranstaltninger vil nu afhænge af medlemsstaternes aktive engagement.

Økonomiers og samfunds funktion afhænger i stigende grad af rumrelaterede tjenester og data, navnlig på sikkerheds- og forsvarsområdet. Rummet er et strategisk område, der i stadig større grad udfordres, og dets betydning for sikkerheden er vokset, navnlig i kølvandet på den russiske invasion af Ukraine. EU-rumstrategien for sikkerhed og forsvar blev vedtaget i marts 2023 for at styrke vores strategiske position og autonomi i rummet. Som en nøgleaktion, der udspringer af denne strategi, vil Kommissionen i 2024 foreslå en EU-rumlov, der regulerer sikkerheden, bæredygtigheden og modstandsdygtigheden af rumaktiviteter i EU.

Med hensyn til den eksterne dimension, understøtter sikker infrastruktur den globale økonomis og forsyningskædernes modstandsdygtighed[10], og derfor omfatter EU's Global Gateway-strategi en stærk sikkerhedsdimension. I betragtning af sammenkoblingerne mellem EU's og

---

6 C(2023) 4878.

7 Rådets henstilling af 8. december 2022 om en koordineret tilgang på EU-plan til styrkelse af kritisk infrastrukturs modstandsdygtighed.

8 COM(2023) 526.

9 Rådets konklusioner af 23. maj 2022 om udviklingen af Den Europæiske Unions cyberposition og Nevers opfordring af 9. marts 2022 til at styrke EU's cybersikkerhedskapacitet.

10 JOIN(2021) 30.

partnerlandenes infrastruktur er yderligere internationalt samarbejde ligeledes afgørende for at styrke cyberrobustheden på globalt plan og støtte et frit, åbent, sikkert og beskyttet cyberspace.

Forordningen om cyberrobusthed

Det er af central betydning for den europæiske cybersikkerhed at sikre, at forbrugere og virksomheder har adgang til sikre digitale produkter. Kommissionen søgte at imødekomme dette behov i sit forslag til forordning om cyberrobusthed[11], der blev vedtaget den 15. september 2022. Det vil indføre obligatoriske horisontale cybersikkerhedskrav for produkter med digitale elementer i fem år eller hele deres livscyklus (alt efter hvilken periode der er kortest). Det vil skabe betingelser for design og udvikling af sikre produkter med digitale elementer ved at sikre, at hardware- og softwareprodukter bringes i omsætning med så få sårbarheder som muligt. Dette vil være en vigtig milepæl med hensyn til at hæve Europas cybersikkerhedsstandarder på alle områder og vil sandsynligvis blive et internationalt referencepunkt og give klare fordele for Unionens cybersikkerhedsindustri på de globale markeder. Europa-Parlamentet og Rådet vedtog deres respektive holdninger i juli 2023, og forhandlingerne bør fremskyndes.

Cybersikkerhedscertificering spiller også en afgørende rolle med hensyn til at øge tilliden til IKT-produkter og -tjenester og give forbrugere, virksomheder og myndigheder mulighed for at træffe informerede valg med et passende cybersikkerhedsniveau. Arbejdet med cybersikkerhedscertificering skrider frem, og EU's cybersikkerhedscertificeringsordning baseret på fælles kriterier er ved at blive vurderet i en udvalgsprocedure. Forslaget til EU's certificeringsordning for cloudsikkerhed (EUCS) er i øjeblikket under udarbejdelse i Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) og drøftes i Den Europæiske Cybersikkerhedscertificeringsgruppe. Det intensive arbejde sammen med eksperter fra en række sektorer, forbrugere og udbydere bør udmunde i en forsvarlig juridisk og teknisk tilgang, der giver de nødvendige sikkerhedsgarantier, og som er i overensstemmelse med EU-retten, internationale forpligtelser og WTO-forpligtelser. ENISA er desuden i færd med at udarbejde forslaget til EU5G-ordningen og den europæiske digitale ID-tegnebog. En samordnet indsats fra alle medlemsstaters side er afgørende for at øge den generelle sikkerhed af IKT-produkter, -tjenester og -processer.

Forordninger om informationssikkerhed og cybersikkerhed i EU's institutioner, organer, kontorer og agenturer

Fremskridt med forslagene til forordninger om regulering af cybersikkerhed og informationssikkerhed i Unionens egne institutioner, der blev fremlagt sammen i marts 2022, er sket i forskelligt tempo. I juni blev der indgået en politisk aftale om forordningen om cybersikkerhed, der gør det muligt at styrke cybersikkerheden i alle EU's institutioner, organer, kontorer og agenturer og afspejler den betydning, som EU tillægger en hurtig gennemførelse af dette forslag. I denne situation er det særlig bekymrende, at der imod forventningen er gjort langsomme fremskridt med det parallelle forslag om informationssikkerhed, som er afgørende for at fuldende en solid lovgivningsmæssig ramme for EU's institutioner, organer, kontorer og agenturer. Begge forslag bør vedtages inden valget til Europa-Parlamentet for at gøre den europæiske forvaltning troværdig og modstandsdygtig i den nuværende geopolitiske kontekst. Et minimumssæt af regler og standarder for informationssikkerhed for alle EU's institutioner, organer, kontorer og agenturer vil skabe sikkerhed for alle involverede parter og sikre konsekvent beskyttelse mod nye trusler mod deres informationer, både EU-klassificerede og ikkeklassificerede. Samlet set vil disse nye regler skabe et stabilt grundlag for sikker udveksling af oplysninger på tværs af EU's institutioner, organer, kontorer og agenturer og med medlemsstaterne med standardiserede tilgange og foranstaltninger til beskyttelse af

[11] COM(2022) 454.

informationsstrømme. De imødekommer således flere opfordringer fra Rådet om at øge modstandsdygtigheden i EU's institutioner, organer, kontorer og agenturer og om at sikre en bedre beskyttelse af Unionens beslutningsproces mod ondsindet indblanding.

Forordningen om cybersolidaritet

Den foreslåede forordning om cybersolidaritet[12] vedtaget af Kommissionen den 18. april 2023, som bygger på en allerede eksisterende, stærk strategisk, politisk og lovgivningsmæssig ramme, vil yderligere forbedre opdagelsen af cybertrusler, modstandsdygtighed og beredskab på alle niveauer af Unionens cybersikkerhedsøkosystem. Disse målsætninger vil blive opfyldt gennem tre hovedforanstaltninger:

(1) etablering af et ***europæisk cyberskjold*** for at opbygge og styrke det fælles situationskendskab og den fælles kapacitet til at afsløre hændelser. Skjoldet vil bestå af nationale sikkerhedsoperationscentre ("nationale SOC'er") og grænseoverskridende sikkerhedsoperationscentre ("grænseoverskridende SOC'er")
(2) oprettelse af en ***cyberberedskabsmekanisme*** som støtte til medlemsstaterne, så de bedre kan forberede sig og reagere på samt sikre omgående genopretning efter væsentlige eller omfattende cybersikkerhedshændelser. Støtte til indsatsen i forbindelse med hændelser vil omfatte EU's cybersikkerhedsreserve, som også vil være tilgængelig for EU's institutioner, organer, kontorer og agenturer og tredjelande, der er tilknyttet programmet for et digitalt Europa, forudsat at deres associeringsaftale vedrørende programmet for et digitalt Europa indeholder bestemmelser herom
(3) oprettelse af en ***europæisk mekanisme til gennemgang af cybersikkerhedshændelser*** med henblik på at gennemgå og vurdere specifikke væsentlige eller omfattende hændelser. Evalueringsrapporten efter hændelsen vil blive koordineret og udarbejdet af ENISA.

Der er indledt drøftelser i Rådet og Europa-Parlamentet. Hvis forhandlingerne afsluttes inden udløbet af Europa-Parlamentets nuværende mandat, vil det sætte kraftigt skub i bestræbelserne på at beskytte borgere og virksomheder i hele Unionen.

Akademiet for cybersikkerhedskompetencer

Selv om cybertruslerne er stigende, har EU akut brug for fagfolk med de færdigheder og kompetencer, der er nødvendige for at forebygge, afsløre og afværge og forsvare EU mod cyberangreb. Behovet for en kvalificeret arbejdsstyrke inden for cybersikkerhed anslås i øjeblikket til 883 000 kvalificerede fagfolk, og antallet af ubesatte stillinger lå på mellem 260 000 og 500 000 i 2022. Alle dele af samfundet bør tilskyndes til at hjælpe med at udfylde dette hul, men navnlig i 2022 udgjorde kvinder kun 20 % af de færdiguddannede inden for cybersikkerhed og 19 % af specialisterne inden for informations- og kommunikationsteknologi. Som led i det europæiske år for færdigheder 2023 vedtog Kommissionen den 18. april 2023[13] et initiativ, der blev hilst velkommen af medlemsstaterne[14], om at oprette et akademi for cybersikkerhedskompetencer for at afhjælpe manglen på cybersikkerhedskompetencer. Akademiet for cybersikkerhedskompetencer vil samle eksisterende initiativer om cybersikkerhedskompetencer og forbedre koordineringen. Kommissionen opfordrer medlemsstaterne, regionale og lokale myndigheder samt europæiske offentlige enheder til at vedtage særlige strategier eller initiativer vedrørende cybersikkerhedskompetencer eller til at

[12] COM(2023) 209.
[13] COM(2023) 207.
[14] Rådets konklusioner af 22. maj 2023 om EU's cyberforsvarspolitik.

integrere cybersikkerhedskompetencer i relevante strategier eller initiativer med et bredere anvendelsesområde (f.eks. cybersikkerhed, digitale færdigheder, beskæftigelse osv.). Inddragelse af private interessenter vil også være afgørende for at afhjælpe manglen på cybersikkerhedskompetencer og den dermed forbundne mangel på arbejdskraft i Europa.

Droner

En anden stigende trussel mod det offentlige rum og kritiske infrastrukturer er den ondsindede brug af droner. Hændelser med droner er blevet hyppigere i dag i og uden for Unionen, og dronebekæmpelsesløsninger er et centralt redskab for de retshåndhævende myndigheder og andre offentlige myndigheder i Unionen samt for private operatører af kritisk infrastruktur. Samtidig yder lovlig brug af droner et vigtigt bidrag til den dobbelte grønne og digitale omstilling[15]. Som bebudet i dronestrategien 2.0, der blev vedtaget i november 2022, vedtager Kommissionen i dag en meddelelse om afværgelse af potentielle trusler fra droner ledsaget af to håndbøger med praktisk vejledning om centrale tekniske aspekter[16]. Initiativet har til formål at tilvejebringe en omfattende og harmoniseret politisk ramme med en fælles forståelse af de regler, der er indført for at bekæmpe eventuelle trusler fra droner og tilpasse sig den hurtige teknologiske udvikling i nødvendigt omfang. Medlemsstaterne og relevante private operatører opfordres til at arbejde tæt sammen med Kommissionen for at sikre, at det gennemføres fuldt ud.

Sikkerhed inden for søfart og luftfart

Ulovlige aktiviteter såsom pirateri, væbnede røverier til søs, smugling af migranter og menneskehandel, handel med våben og narkotika samt terrorisme er fortsat maritime sikkerhedsudfordringer og forværres af nye trusler, herunder hybride angreb og cyberangreb. Kommissionen og den højtstående repræsentant vedtog den 10. marts 2023 en fælles meddelelse om ajourføringen af EU-strategien for maritim sikkerhed[17], som nu bør gennemføres i overensstemmelse med den ajourførte handlingsplan.

På luftfartssikkerhedsområdet vedtog Kommissionen den 2. februar 2023 et arbejdsdokument fra Kommissionens tjenestegrene med titlen "Working towards a Enhanced and more resilient aviation security policy"[18], som indeholder et ambitiøst program, der skal 1) modernisere den reguleringsmæssige struktur for luftfartssikkerhed (2), fremme udviklingen og udbredelsen af mere innovative løsninger og 3) ajourføre referencescenariet for luftfartssikkerhed, således at Unionens lufthavne fuldt ud kan drage fordel af nye og banebrydende teknologier for at imødegå de højest prioriterede trusler. Fjorten flagskibsforanstaltninger skal gennemføres inden for to år.

Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigst muligt at afslutte forhandlingerne, under alle omstændigheder inden udløbet af det nuværende Europa-Parlaments mandat, om følgende sager:

- forslaget til forordning om cyberrobusthed
- forslaget til forordning om cybersolidaritet
- forslaget til forordning om informationssikkerhed for EU's institutioner, organer, kontorer og agenturer.

[15] COM(2022) 652.
[16] COM (2023) 659.
[17] JOIN(2023) 8.
[18] SWD(2023) 37.

Kommissionen opfordrer medlemsstaterne til at:

- gennemføre direktivet om kritiske enheders modstandsdygtighed som en prioritet samt foretage stresstest af kritisk infrastruktur i energisektoren
- vedtage Rådets henstilling om en plan for koordinering af reaktionen på EU-plan på forstyrrelser af kritisk infrastruktur af væsentlig grænseoverskridende relevans
- gennemføre NIS 2-direktivet fuldt ud og hurtigst muligt for at styrke cybersikkerheden for væsentlige og vigtige enheder
- deltage aktivt i udførelsen af cybersikkerhedsrisikovurderinger og opstille risikoscenarier for kritisk infrastruktur og forsyningskæder
- følge op på akademiet for cybersikkerhedskompetencer med et stærkt engagement på europæisk plan og særlige nationale strategier eller initiativer vedrørende cybersikkerhedskompetencer med inddragelse af centrale interessenter, herunder regionale og lokale myndigheder
- samarbejde med relevante private operatører og Kommissionen om at sikre gennemførelsen af alle de foranstaltninger, der er anført i meddelelsen om afværgelse af potentielle trusler fra droner
- gennemføre handlingsplanen for EU-strategien for maritim sikkerhed og regelmæssigt aflægge rapport om resultaterne
- gennemføre de 14 flagskibsforanstaltninger, der er udpeget til at øge luftfartssikkerheden.

III. Håndtering af foranderlige trusler

Nye geopolitiske spændinger har givet klar dokumentation for, hvordan sikkerhedsudfordringen for EU ikke blot er stigende, men er stadig mere ustabil og forstærket af den hybride karakter af mange trusler. Sikkerheden skal også tilpasses samfundsmæssige og teknologiske ændringer. Covid-19-pandemien styrkede de cyberkriminelles muligheder, og der var navnlig øget risiko med hensyn til materiale, der viser seksuelt misbrug af børn online. Kriminelle og ondsindede aktører er altid parate til at udnytte den teknologiske udvikling. I lyset af sådanne ofte komplekse og flerdimensionelle trusler er der behov for en stærk og konsekvent EU-indsats.

Forordning om bekæmpelse af seksuelt misbrug af børn online

Europols trusselsvurdering af organiseret internetkriminalitet viste, at omfanget af seksuel udnyttelse og seksuelt misbrug af børn i 2022 var steget yderligere med hensyn til hyppighed og alvor, idet gerningsmændene fortsat udnyttede de tekniske muligheder for at sløre deres handlinger og identiteter[19]. Det nuværende system, der er baseret på frivillig opsporing og indberetning fra virksomhederne, har ikke været effektivt nok til at beskytte børn. En midlertidig forordning gør det muligt for virksomheder at afsløre og indberette materiale frivilligt, forudsat at dette er lovligt i henhold til den generelle forordning om databeskyttelse (GDPR). Denne forordning udløber i august 2024. I maj 2022 foreslog Kommissionen en forordning[20] om imødegåelse af udnyttelsen af onlinetjenester med henblik på seksuelt misbrug

[19] Europols trusselsvurdering af organiseret internetkriminalitet — Internet Organised Crime Threat Assessment (IOCTA) 2023.

[20] COM(2022) 209.

af børn. I den foreslåede ramme lægges stor vægt på forebyggelse. Virksomhederne vil være forpligtet til at vurdere risikoen for seksuelt misbrug af børn via deres systemer og til at træffe forebyggende foranstaltninger. Som en sidste udvej kan nationale domstole eller uafhængige administrative myndigheder i tilfælde af en betydelig risiko udstede målrettede opsporingspåbud til tjenesteudbydere. Et nyt uafhængigt EU-center vil støtte udbydernes indsats ved at fungere som et ekspertisecenter, give pålidelige oplysninger om identificeret materiale, modtage og analysere onlineindberetninger om seksuelt misbrug af børn fra udbydere for at kortlægge fejlagtige indberetninger og yde støtte til ofre. Det er vigtigt, at de nye regler vedtages og gennemføres så hurtigt som muligt for at beskytte børn mod yderligere misbrug, forhindre, at materiale dukker op igen online, og for at retsforfølge gerningsmændene. Der er forhandlinger i gang i Rådet og i Parlamentet med det formål at nå til enighed om sagen inden udløbet af Parlamentets mandat.

Direktiv om bekæmpelse af vold mod kvinder og vold i hjemmet

Cybervold mod kvinder, herunder i forbindelse med vold i hjemmet, er opstået som en ny form for vold, der spredes i de enkelte medlemsstater via internettet og IT-værktøjer. I marts 2022 foreslog Kommissionen et direktiv om bekæmpelse af vold mod kvinder og vold i hjemmet, herunder specifikke regler om cybervold og foranstaltninger til at udfylde huller i forbindelse med beskyttelse, adgang til domstolsprøvelse og forebyggelse. Hurtig vedtagelse og gennemførelse vil give medlemsstaterne yderligere redskaber til at bekæmpe denne form for kriminalitet. De to lovgivere indledte interinstitutionelle forhandlinger i juli 2023 og sigter mod at afslutte forhandlingerne inden udløbet af det nuværende Europa-Parlaments mandat.

5G-cybersikkerhed

Sikkerheden i 5G-net er en vigtig prioritet for Kommissionen og en væsentlig del af strategien for sikkerhedsunionen. 5G-net er en central infrastruktur, der danner grundlag for en bred vifte af tjenester, der er afgørende for det indre markeds funktion og for vitale samfundsmæssige og økonomiske funktioner. Den 15. juni 2023 offentliggjorde EU-medlemsstaternes myndigheder, der er repræsenteret i NIS-samarbejdsgruppen, med støtte fra Kommissionen og ENISA den anden statusrapport om gennemførelsen af EU-værktøjskassen til cybersikkerhed i 5G-net. Ifølge rapporten har 24 medlemsstater vedtaget eller er i færd med at udarbejde lovgivningsmæssige foranstaltninger, der giver de nationale myndigheder beføjelser til at foretage en vurdering af leverandører og udstede restriktioner, og 10 medlemsstater har indført sådanne restriktioner. Der er imidlertid behov for en yderligere indsats for at undgå sårbarheder for Unionen som helhed med potentielt alvorlige negative konsekvenser for sikkerheden for individuelle brugere og virksomheder i hele Unionen og Unionens kritiske infrastruktur. Alle medlemsstater skal straks gennemføre værktøjskassen. Samme dag vedtog Kommissionen en meddelelse om medlemsstaternes gennemførelse af værktøjskassen og Kommissionens egne virksomhedskommunikations- og EU-finansieringsaktiviteter. Dette understregede den stærke bekymring over de risici for EU's sikkerhed, som leverandørerne af mobilkommunikationsudstyr Huawei og ZTE udgør for EU's sikkerhed. I denne forbindelse træffer Kommissionen foranstaltninger for at undgå, at dens virksomhedskommunikation eksponeres for mobilnet, der anvender Huawei og ZTE som leverandører. Der vil ikke blive anskaffet nye konnektivitetstjenester, som er afhængige af udstyr fra disse leverandører, og Kommissionen vil samarbejde med medlemsstaterne og teleoperatørerne om at sikre, at disse leverandører gradvist udfases fra eksisterende konnektivitetstjenester på Kommissionens websteder. Kommissionen undersøger også, hvordan denne afgørelse kan afspejles i relevante EU-finansieringsprogrammer og -instrumenter i fuld overensstemmelse med EU-retten.

Adgang til data med henblik på effektiv retshåndhævelse

I nutidens digitale tidsalder har næsten alle former for kriminalitet en digital komponent. Teknologier og værktøjer anvendes også til kriminelle formål, herunder teknologier og værktøjer, der er nødvendige for at sikre vores samfunds behov for cybersikkerhed, databeskyttelse og privatlivets fred. Dette gør det stadig vanskeligere at opretholde en effektiv retshåndhævelse i hele EU for at beskytte den offentlige sikkerhed og forebygge, opdage, efterforske og retsforfølge kriminalitet, og selv om der er gjort en betydelig indsats på EU-plan og nationalt plan, herunder gennem lovgivning samt kapacitetsopbygnings- og innovationsinitiativer, er der fortsat juridiske og tekniske udfordringer. Kommissionen har i samarbejde med formandskabet for Rådet nedsat en gruppe på højt plan om adgang til data med henblik på effektiv retshåndhævelse for at skabe en samarbejdsplatform for en bred vifte af interessenter og eksperter, der skal undersøge de udfordringer, som fagfolk inden for strafferetlig håndhævelse står over for (f.eks. kryptering, datalagring, 5G og standardisering). Kommissionen forventer, at gruppen på højt plan udarbejder afbalancerede, solide og gennemførlige anbefalinger senest i juni 2024, der afspejler disse spørgsmåls kompleksitet, herunder set ud fra et cybersikkerheds- og databeskyttelsesperspektiv. Medlemsstaterne og de deltagende eksperter opfordres derfor til at engagere sig aktivt i denne proces og arbejde hen imod effektive, lovlige og almindeligt anerkendte løsninger.

Hybride trusler

I lyset af den geopolitiske kontekst, hvor hybride trusler bliver stadig mere komplekse og sofistikerede, tilvejebragte EU's strategiske kompas for sikkerhed og forsvar[21] (det strategiske kompas) en fælles vurdering af de trusler og udfordringer, som Unionen står over for, samt en strategisk handlingsplan. Stigningen i statslige og ikkestatslige aktørers ondsindede adfærd i cyberspace, herunder i forbindelse med krigen mod Ukraine, har yderligere understreget, at cyberspace er et udenrigs- og sikkerhedspolitisk område. De potentielle risici for ondsindede handlinger og desinformation kræver særlig årvågenhed i valgperioder, herunder op til valget til Europa-Parlamentet i 2024.

I betragtning af den høje risiko for afsmittende virkninger er EU fortsat med at udvikle cyberkapacitetsopbygningsaktiviteter og fremme partnerskaber med tredjelande, herunder gennem særlige cyberdialoger, for aktivt at bidrage til EU's overordnede modstandsdygtighed. En række værktøjer er blevet udviklet, revideret og styrket for at forbedre Unionens evne til effektivt at imødegå hybride trusler som beskrevet i den syvende statusrapport om hybride trusler, der blev offentliggjort den 14. september 2023[22]. De omfatter:

- den hybride EU-værktøjskasse, som skal sikre en ramme for en koordineret og velinformeret reaktion på hybride trusler og kampagner
- det igangværende arbejde med oprettelsen af EU-hybridberedskabshold med henblik på kortsigtet skræddersyet støtte til medlemsstater, partnerlande og missioner og operationer under den fælles sikkerheds- og forsvarspolitik (FSFP)
- den reviderede EU-protokol for imødegåelse af hybride trusler ("EU-drejebogen")[23], der beskriver Unionens processer og strukturer til håndtering af hybride trusler og kampagner
- de reviderede retningslinjer for gennemførelsen af rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter[24] ("cyberdiplomatisk værktøjskasse"), der gør det muligt at udvikle bæredygtige, skræddersyede, sammenhængende og koordinerede strategier over for persistente cybertrusselsaktører

[21] Rådets dokument 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 af 8. juni 2023.

- værktøjskassen vedrørende udenlandsk informationsmanipulation og indblanding med henblik på at styrke Unionens eksisterende værktøjer til at forebygge, afværge og reagere på udenlandsk informationsmanipulation og indblanding
- EU's politik for cyberforsvar[25] med henblik på at styrke EU's cyberforsvarskapaciteter, øge situationsbevidstheden og koordinere hele spektret af tilgængelige forsvarsmuligheder for at styrke modstandsdygtigheden, reagere på cyberangreb og sikre solidaritet og gensidig bistand.

Medlemsstaterne opfordres derfor til at fortsætte og styrke deres samarbejde på dette område ved at sikre en effektiv gennemførelse af ovennævnte værktøjskasser, herunder gennem regelmæssige øvelser, og ved at nå til enighed om begrebet hybride beredskabshold med retningslinjer for yderligere skridt hen imod oprettelsen af holdene.

Kunstig intelligens i retshåndhævelsesmæssig sammenhæng

Kunstig intelligens (AI) er hurtigt blevet en almindelig del af dagligdagen. Virkningerne af anvendelsen af kunstig intelligens på cyberkriminalitet og cybersikkerhed er endnu ikke fuldt kendt, men vil klart skabe nye udfordringer. Selv om kunstig intelligens kan medføre fordele, når den anvendes på en sikker og kontrolleret måde, kan den være potentielt farlig i hænderne på ondsindede aktører, herunder ved at hjælpe kriminelle med at skjule deres identitet i forbindelse med forbrydelser såsom terrorisme og seksuelt misbrug af børn. Det er derfor afgørende, at myndighederne holder sig ajour med udviklingen for at forhindre misbrug og reagere på misbrug[26]. Forhandlingerne om den foreslåede retsakt om kunstig intelligens har til formål at løse disse problemer og er gået ind i en afgørende fase, hvor de to lovgivere nu drøfter tekniske og politiske spørgsmål, der vil være afgørende for samspillet med denne teknologi i de kommende år. Det vil være vigtigt at finde afbalancerede løsninger, navnlig med hensyn til højrisikoanvendelser, herunder på retshåndhævelsesområdet.

Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigst muligt at afslutte de interinstitutionelle forhandlinger, under alle omstændigheder inden udløbet af det nuværende Europa-Parlaments mandat, om følgende verserende sager:

- forslag til forordning om bekæmpelse af seksuelt misbrug af børn online
- forslag til direktiv om bekæmpelse af vold mod kvinder og vold i hjemmet
- forslag til forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens).

Kommissionen opfordrer medlemsstaterne til:

- at gennemføre hele EU-værktøjskassen til cybersikkerhed i 5G-net hurtigst muligt
- at støtte arbejdet i gruppen på højt plan om adgang til data med henblik på effektiv retshåndhævelse for at formulere klare, solide og gennemførlige anbefalinger til tackling af nuværende og forventede udfordringer på en forholdsmæssig måde
- i samarbejde med den højtstående repræsentant at tage skridt til at sikre en effektiv gennemførelse af den hybride EU-værktøjskasse, den reviderede cyberdiplomatiske værktøjskasse og værktøjskassen vedrørende udenlandsk informationsmanipulation og indblanding, herunder gennem regelmæssige øvelser og under hensyntagen til den globale dynamik

[25] JOIN (2022) 49.

[26] Se f.eks. Europols rapport offentliggjort 17. april 2023: "ChatGPT — the impact of Large Language Models on Law Enforcement".

- at nå til enighed om begrebet hybride beredskabshold.

IV. Beskyttelse af europæerne mod terrorisme og organiseret kriminalitet

Risikoen for, at globale eller lokale begivenheder udløser nye terrorhandlinger, er altid til stede. Sideløbende hermed er organiseret kriminalitet og narkotikahandel blandt de alvorligste trusler mod EU's sikkerhed. For at intensivere Unionens kollektive indsats for at bekæmpe disse trusler er der et kollektivt arbejde i gang med gennemførelsen af EU's strategi for bekæmpelse af organiseret kriminalitet[27], EU's strategi for bekæmpelse af menneskehandel[28], EU's narkotikadagsorden og -handlingsplan[29] og EU's dagsorden for bekæmpelse af terrorisme[30]. For at reagere på en foruroligende forværring af situationen med hensyn til organiseret kriminalitet og narkotikahandel er der imidlertid behov for en yderligere intensivering af medlemsstaternes og EU's indsats for at styrke vores kollektive indsats over for kriminelle netværk og beskytte ofre for kriminalitet bedre, og samtidig med denne rapport offentliggøres en EU-køreplan for bekæmpelse af narkotikahandel og organiseret kriminalitet[31].

På terrorbekæmpelsesområdet styrker EU også sin eksterne værktøjskasse[32] ved at gøre fuld brug af dialogerne på højt plan om terrorbekæmpelse og netværket af terrorbekæmpelses-/sikkerhedseksperter i EU-delegationer samt gennem sit engagement i multilaterale fora, herunder som medformand for Det Globale Forum for Terrorbekæmpelse (GCTF).

Narkotikahandel

Med det nye mandat for EU's Narkotikaagentur, der vil finde anvendelse fra juli 2024, vil EU være bedre rustet til at håndtere et komplekst sikkerheds- og sundhedsproblem, der berører millioner af mennesker i EU og globalt. Kommissionen er også i færd med at revidere[33] forordningerne om narkotikaprækursorer[34] for at imødegå de vigtigste udfordringer, der blev identificeret i evalueringen i 2020[35], som fremhævede behovet for at tackle de udfordringer, der er forbundet med designerprækursorer[36], for at reducere udbuddet af ulovlige stoffer.

I lyset af den hidtil usete stigning i udbuddet af ulovlige stoffer i Europa, skal bekæmpelsen af narkotikahandel imidlertid intensiveres i samarbejde med internationale partnere. Der er behov for en yderligere indsats fra medlemsstaternes og EU's side for at optrevle kriminelle netværk og beskytte ofre for kriminalitet bedre. Kommissionen fremlægger i dag en EU-køreplan for bekæmpelse af narkotikahandel og organiseret kriminalitet. Den indeholder 17 tiltag på fire prioriterede områder: styrkelse af modstandsdygtigheden i logistiske knudepunkter med en europæisk havnealliance, optrævling af kriminelle netværk, forøgelse af

[27] COM(2021) 170.
[28] COM(2021) 171.
[29] COM(2020) 606.
[30] COM(2020) 795.
[31] COM (2023) 641.
[32] Som krævet i det strategiske kompas og Rådets konklusioner om håndtering af den eksterne dimension af en terrortrussel og voldelig ekstremistisk trussel i konstant forandring med fokus på den eksterne dimension, der blev vedtaget i juni 2022.
[33] Narkotikaprækursorer: reviderede EU-regler (europa.eu).
[34] Rådets forordning (EF) nr. 273/2004 om narkotikaprækursorer og Rådets forordning (EF) nr. 111/2005 om regler for overvågning af handel med narkotikaprækursorer mellem Fællesskabet og tredjelande.
[35] COM(2020) 768.
[36] Foranstaltning nr. 23 i narkotikahandlingsplanen (COM (2020) 606).

forebyggelsesindsatsen og styrkelse af samarbejdet med internationale partnere. Disse tiltag skal gennemføres i 2024 og 2025.

Skydevåben

Ulovlig handel med skydevåben giver næring til organiseret kriminalitet i EU og i nabolandene. Det anslås, at der er op til 35 millioner ulovlige skydevåben i civile hænder i EU, og omkring 630 000 skydevåben er opført som stjålne eller forsvundne i Schengeninformationssystemet. Med udviklingen af hurtig pakkelevering og nye teknologier såsom 3D-printning antager ulovlig handel med skydevåben nye former med det formål at undslippe kontrol. Ruslands angrebskrig mod Ukraine har også øget risikoen for spredning af skydevåben. I oktober 2022 vedtog Kommissionen et forslag om at ajourføre den eksisterende lovgivning om import, eksport og transit af civile skydevåben for at lukke smuthuller i de eksisterende regler, som kan øge antallet af skydevåben, der smugles og omdirigeres til EU[37]. På mellemlang sigt vil disse nye regler bidrage til at mindske risikoen for omgåelse af embargoer ved eksport af skydevåben til civil brug og til at øge kontrollen med import af denne type skydevåben fra lande uden for EU. De to lovgivere skal vedtage deres holdninger til denne sag, således at de kan nå til enighed inden udløbet af det nuværende Parlaments mandat.

Menneskehandel

Menneskehandel er en særlig alvorlig form for organiseret kriminalitet og en alvorlig krænkelse af de grundlæggende rettigheder. Ofre handles inden for EU, hovedsagelig med henblik på seksuel udnyttelse og udnyttelse som arbejdskraft, men også med henblik på tvunget tiggeri og kriminalitet og andre ulovlige aktiviteter. Kommissionen foreslog i december 2022 at ændre direktivet om bekæmpelse af menneskehandel[38] med ajourførte regler for at afhjælpe mangler i den nuværende retlige ramme. Når det reviderede direktiv er vedtaget, vil navnlig tvangsægteskaber og ulovlig adoption være omfattet af direktivets anvendelsesområde, og der vil være indført en udtrykkelig henvisning til onlinedimensionen af menneskehandel. Det vil også omfatte en obligatorisk sanktionsordning for gerningsmænd og formalisere oprettelsen af nationale henvisningsmekanismer for at forbedre tidlig identifikation og grænseoverskridende henvisning med henblik på bistand og støtte til ofre. Bevidst brug af tjenester, der leveres af ofre for menneskehandel, vil blive en strafbar handling, og det vil blive obligatorisk at indsamle årlige data om menneskehandel, som skal offentliggøres af Eurostat. Rådet vedtog sin generelle indstilling i juni 2023, men Europa-Parlamentet har stadig ikke vedtaget sin holdning. Der skal handles hurtigt for at nå til enighed inden udløbet af det nuværende Parlaments mandat.

Miljøkriminalitet

Miljøkriminalitet er blevet en global trussel med en anslået vækst på mellem 5 og 7 % hvert år. De betydelige fortjenester, der kan opnås, juridiske smuthuller mellem medlemsstaterne og en lav risiko for afsløring giver grobund for organiseret kriminalitet. Ifølge Europol er der tegn på, at indtægterne fra disse aktiviteter anvendes til at finansiere terrorisme. I december 2021 vedtog Kommissionen et forslag om erstatning af direktivet fra 2008 om strafferetlig beskyttelse af miljøet. I forslaget er der fokus på at finjustere og ajourføre definitionerne af kategorier af miljøkriminalitet og definere effektive, afskrækkende og forholdsmæssige sanktionstyper og -niveauer for fysiske og juridiske personer. Nye forbrydelser omfatter lovovertrædelser i forbindelse med ulovlig skovrydning, overtrædelser af EU's kemikalielovgivning, ulovlig udvinding af overfladevand eller grundvand og ulovlig skibsophugning. Forslaget har til formål

[37] COM(2022) 480.
[38] COM(2022) 732.

at styrke retshåndhævelseskæden og det grænseoverskridende samarbejde mellem medlemsstaternes myndigheder og EU-agenturer og -organer betydeligt. Europa-Parlamentet og Rådet har vedtaget deres respektive holdninger til forslaget og er i en forhandlingsproces, som de bør kunne afslutte inden årets udgang. En revideret handlingsplan[39] for bekæmpelse af ulovlig handel med vilde dyr og planter skal gennemføres for at styrke forebyggelsen og håndhævelsen yderligere.

Inddrivelse og konfiskation af aktiver

Det er afgørende at fratage kriminelle deres ulovlige indtægter for at bremse den organiserede kriminalitet. Dette er grunden til, at Kommissionen ud over forslaget om at give de retshåndhævende myndigheder adgang til bankkontooplysninger i hele EU[40] (som der blev opnået politisk enighed om i juni 2023) fremsatte et forslag om inddrivelse og konfiskation[41] af aktiver i maj 2022 for at styrke kapaciteten til sporing, identifikation, beslaglæggelse, konfiskation og forvaltning af aktiver. De vigtigste bestemmelser i forslaget vedrører kravene til finansielle efterforskninger og yderligere beføjelser og værktøjer til kontorer for inddrivelse af aktiver samt adgang til mere effektive beslaglæggelses- og konfiskationsforanstaltninger i forbindelse med en bredere vifte af forbrydelser. En af de nye strafbare handlinger, som disse foranstaltninger vil finde anvendelse på, er overtrædelse af Unionens restriktive foranstaltninger. I december 2022 vedtog Kommissionen et særskilt forslag om harmonisering af de strafferetlige definitioner af og sanktioner for overtrædelse af Unionens restriktive foranstaltninger. En effektiv gennemførelse og håndhævelse af Unionens restriktive foranstaltninger er fortsat en topprioritet for Kommissionen, styrket af arbejdet i "Freeze og Seize"-taskforcen, som Kommissionen har oprettet som reaktion på Ruslands angrebskrig mod Ukraine. For begge forslags vedkommende har Europa-Parlamentet og Rådet vedtaget deres holdninger med henblik på at nå frem til en aftale inden årets udgang.

Pakken om bekæmpelse af hvidvask af penge

Hvidvask af penge er forbundet med stort set alle kriminelle aktiviteter, der genererer indtægter fra kriminelle aktiviteter i EU[42], og er derfor et vigtigt fokuspunkt i bekæmpelsen af kriminalitet i EU. I juli 2021 fremsatte Kommissionen ambitiøse forslag til styrkelse af EU's foranstaltninger til forebyggelse af hvidvask af penge og finansiering af terrorisme[43] med fire lovgivningsforslag, der skal styrke forebyggelsen og afsløringen af kriminelles forsøg på at hvidvaske ulovlige indtægter eller finansiere terroraktiviteter gennem det finansielle system. Et af pakkens fire initiativer, der skal sikre sporbarheden af overførsler af kryptoaktiver, blev vedtaget af de to lovgivere i maj 2023[44]. Denne forordning vil finde anvendelse fra den 30. december 2024, hvorefter alle udbydere af kryptoaktivtjenester skal indsamle og opbevare oplysninger om afsenderen og modtageren af overførsler af kryptoaktiver. De resterende tre forslag har til formål i) at oprette en ny EU-myndighed for bekæmpelse af hvidvask af penge for at sikre konsekvent tilsyn af høj kvalitet i hele det indre marked, herunder med de mest risikofyldte grænseoverskridende enheder, og støtte og koordinere de finansielle efterretningsenheders arbejde, ii) at fastsætte harmoniserede regler for den private sektor,

[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, 2020.
[43] COM(2021) 420.
[44] Europa-Parlamentets og Rådets forordning (EU) 2023/1113 af 31. maj 2023 om oplysninger, der skal medsendes ved pengeoverførsler og ved overførsler af visse kryptoaktiver og om ændring af direktiv (EU) 2015/849.

herunder indføre en EU-dækkende grænse på 10 000 EUR for store kontantbetalinger for tjenesteydelser og varer, og iii) at styrke de kompetente myndigheders beføjelser og samarbejdsværktøjer. Denne pakke forventes at forbedre EU's evne til at bekæmpe hvidvask af penge og beskytte EU-borgerne mod terrorisme og organiseret kriminalitet væsentligt. De tre udestående forslag forhandles i øjeblikket af de to lovgivere med det formål at nå til enighed om sagen inden udløbet af dette Parlaments mandat.

Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigst muligt at afslutte de interinstitutionelle forhandlinger, under alle omstændigheder inden udløbet af det nuværende Europa-Parlaments mandat, om følgende verserende sager:

- forslag til direktiv om inddrivelse og konfiskation af aktiver
- forslag til direktiv om harmonisering af de strafferetlige definitioner af og sanktioner for overtrædelse af Unionens restriktive foranstaltninger.
- forslag til direktiv om bekæmpelse af menneskehandel
- forslag til direktiv om strafferetlig beskyttelse af miljøet
- forslag til en pakke om bekæmpelse af hvidvask af penge
- forslag om ajourføring af den eksisterende lovgivning om indførsel, udførsel og transit af civile skydevåben.

Kommissionen opfordrer medlemsstaterne og EU-agenturer og -organer til at:

- samarbejde om gennemførelsen af de 17 tiltag i EU's køreplan for bekæmpelse af narkotikahandel og organiseret kriminalitet i 2023 og 2024.

V. Et stærkt europæisk sikkerhedsøkosystem

I de senere år er sikkerhedstrusler blevet stadig mere grænseoverskridende, hvilket kræver yderligere synergier og tættere samarbejde på alle niveauer. Siden vedtagelsen af strategien for sikkerhedsunionen er der taget vigtige initiativer til at maksimere det grænseoverskridende samarbejde, strømline og opgradere de tilgængelige instrumenter og procedurer både ved de ydre grænser og i Schengenområdet og forbedre udvekslingen af oplysninger mellem retshåndhævende og retlige myndigheder for bedre at kunne bekæmpe organiseret kriminalitet. På denne baggrund er en effektiv gennemførelse af interoperabilitetsrammen for udveksling af data en vigtig søjle for at øge sikkerheden og en effektiv europæisk reaktion på grænseoverskridende trusler, samtidig med at der sikres fri bevægelighed internt.

Øget udveksling af oplysninger i Schengenområdet: forhåndsinformation om passagerer (API), passagerlisteoplysninger (PNR) og Prüm II

De to API-forslag, som Kommissionen vedtog i december 2022[45] , vil styrke Unionens indre sikkerhed ved at give medlemsstaternes retshåndhævende myndigheder yderligere redskaber til at bekæmpe grov kriminalitet og terrorisme. Forhåndsinformation om passagerer vedrørende flyvninger inden for EU, der anvendes sammen med flyrejsendes PNR-oplysninger, vil navnlig gøre det muligt for medlemsstaternes retshåndhævende myndigheder at øge effektiviteten af deres efterforskninger betydeligt med mere målrettede interventioner. Det er vigtigt, at de foreslåede regler vedtages så hurtigt som muligt. Dette vil ikke blot understøtte bekæmpelsen

[45] COM(2022) 729, COM(2022) 73.

af organiseret kriminalitet og terrorisme, men også i væsentlig grad mindske behovet for systematisk kontrol af alle rejsende i tilfælde af en midlertidig genindførelse af kontrol ved de indre grænser, lette flyrejser og den frie bevægelighed. Den 6. september 2023 henstillede Kommissionen til Rådet at godkende forhandlingerne med Schweiz, Island og Norge om aftaler om overførsel af PNR-oplysninger. Vedtagelsen af disse tre henstillinger vil understøtte en sammenhængende eksterne politik for PNR-oplysninger i EU.

Politiet udveksler dagligt data inden for Prümrammen for at bekæmpe organiseret kriminalitet, narkotika, terrorisme, seksuel udnyttelse og menneskehandel. Forslaget til forordning om elektronisk udveksling af data med henblik på politisamarbejde ("Prüm II")[46] reviderer den eksisterende Prümramme med henblik på at lukke informationshuller og fremme forebyggelse, afsløring og efterforskning af strafbare handlinger i EU. De reviderede regler om elektronisk udveksling af data med henblik på politisamarbejde supplerer forslagene om politisamarbejde i denne mandatperiode sammen med Rådets allerede vedtagne henstilling om styrkelse af det operationelle grænseoverskridende samarbejde og direktivet om udveksling af oplysninger mellem retshåndhævende myndigheder. En hurtig vedtagelse og gennemførelse af disse relaterede instrumenter vil forbedre, lette og fremskynde dataudvekslingen mellem de retshåndhævende myndigheder og gøre det lettere at identificere kriminelle.

Fuldt interoperabelt grænseforvaltningssystem for et sikkert, stærkt, digitalt og forenet Schengenområde

Et velfungerende Schengenområde uden indre grænser kræver gensidig tillid mellem medlemsstaterne. Dette er baseret på effektiv kontrol, enten ved Unionens ydre grænser eller i form af alternative foranstaltninger på medlemsstaternes område. I Kommissionens ændringsforslag til Schengengrænsekodeksen[47] fastsættes det, hvordan medlemsstaterne kan gøre bedre brug af alternativer til kontrol ved de indre grænser, der kan sikre et højt sikkerhedsniveau. Det er vigtigt, at ændringen af Schengengrænsekodeksen vedtages og gennemføres fuldt ud for at sikre et højt og forholdsmæssigt sikkerhedsniveau i Schengenområdet. Den nye arkitektur for EU's informationssystemer er ligeledes fortsat under udvikling, således at de nationale myndigheders arbejde med at garantere sikkerhed samt grænse- og migrationsforvaltning kan understøttes bedre. Den omfatter det fornyede Schengeninformationssystem, det europæiske system vedrørende rejseinformation og rejsetilladelse, ind- og udrejsesystemet, ajourføringen af visuminformationssystemet og interoperabilitetsrammen for sammenkobling af systemer i fuld sikkerhed. Når denne nye arkitektur er fuldendt, vil den give de nationale myndigheder mere omfattende og pålidelige sikkerhedsoplysninger. Alle komponenter i interoperabilitetsrammen er afgørende, hvilket betyder, at en forsinkelse i ét aspekt eller i én medlemsstat forsinker udrulningen i alle medlemsstater. Forsinkelser i den tekniske udvikling af ind- og udrejsesystemet bør reduceres til et minimum, således at ind- og udrejsesystemet kan idriftsættes så hurtigt som muligt, og alle centrale elementer i interoperabilitetsrammen kan indføres.

Forslaget om screening[48] vil øge sikkerheden i Schengenområdet ved at skabe ensartede regler for identifikation af tredjelandsstatsborgere, der ikke opfylder indrejsebetingelserne som omhandlet i Schengengrænsekodeksen, og underkaste dem helbredstjek og sikkerhedskontrol ved de ydre grænser. Det foreslåede Eurodac-system vil støtte disse mål, idet en screening kan vise, om en person kan udgøre en trussel mod den indre sikkerhed. Dette vil lette

[46] COM(2021) 784.
[47] COM(2021) 891.
[48] COM(2020) 612.

gennemførelsen af den foreslåede forordning om asylforvaltning og migrationsstyring. Kommissionen opfordrer de to lovgivere til hurtigt at afslutte forhandlingerne om disse sager inden udgangen af den nuværende valgperiode.

Bekæmpelse af korruption

Korruption er yderst skadelig for vores demokratier, økonomien og vores sikkerhed, da den fungerer som katalysator for organiseret kriminalitet og fjendtlig udenlandsk indblanding. Det er af afgørende betydning at sikre en vellykket forebyggelse og bekæmpelse af korruption både for at beskytte EU's værdier og effektiviteten af EU's politikker og for at værne om retsstaten og opretholde tilliden til dem, der styrer, og de offentlige institutioner. Som bebudet af kommissionsformand Ursula von der Leyen i sin tale om Unionens tilstand 2022 vedtog Kommissionen den 3. maj 2023 en pakke af foranstaltninger til bekæmpelse af korruption[49]. Kommissionens forslag til direktiv om bekæmpelse af korruption omfatter skærpede regler, der gør korruptionsrelaterede lovovertrædelser strafbare og harmoniserer straffe i hele EU. Det muliggør også effektiv efterforskning og retsforfølgning og sætter stærkt fokus på forebyggelse og skabelse af en integritetskultur, hvor korruption ikke tolereres. Drøftelserne om dette forslag er indledt i Europa-Parlamentet og Rådet. Desuden opfordres medlemsstaterne til at gennemføre henstillingerne fra søjlen om bekæmpelse af korruption i rapporten om retsstatssituationen 2023, der blev vedtaget den 5. juli 2023. I et forslag fra den højtstående repræsentant, der støttes af Kommissionen, foreslås det ligeledes at indføre en særlig sanktionsordning for den fælles udenrigs- og sikkerhedspolitik (FUSP) med henblik på at bekæmpe alvorlig korruption i hele verden.

Styrkelse af ofres rettigheder

Den 12. juli 2023 foreslog Kommissionen ændringer til direktivet om ofres rettigheder for at styrke ofres adgang til information, støtte og beskyttelse, deltagelse i straffesager og adgang til erstatning. Et af de overordnede mål med revisionen er at bidrage til et højt sikkerhedsniveau ved at skabe sikrere rammer for ofre for at tilskynde dem til at anmelde forbrydelser og mindske frygten for repressalier.

Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigst muligt at afslutte de interinstitutionelle forhandlinger, under alle omstændigheder inden udløbet af det nuværende Europa-Parlaments mandat, om følgende verserende sager:

- forslag til Prüm II-forordningen
- forslag om forhåndsinformation om passagerer (API)
- forslag om bekæmpelse af korruption og navnlig om indførelse af en særlig sanktionsordning for den fælles udenrigs- og sikkerhedspolitik (FUSP)
- forslag til ændring af forordningen om Schengengrænsekodeksen
- forslag til direktiv om ofres rettigheder
- forslag om screening.

Kommissionen opfordrer medlemsstaterne til:

- at sikre, at ind- og udrejsesystemet træder i kraft så hurtigt som muligt for at fuldføre gennemførelsen af EU's arkitektur for udveksling af oplysninger.

VI. Gennemførelse

[49] COM(2023) 234.

Det er et fælles ansvar at varetage sikkerheden generelt i Europa, og alle aktører udfylder en rolle, fra Kommissionens og de to lovgiveres vedtagelse af nye stærke, omfattende og praktiske regler til medlemsstaternes rettidige gennemførelse og anvendelse af sådanne regler, og det operationelle arbejde, der udføres ude omkring af myndigheder, organisationer og interessenter. EU's agenturer på områderne retlige og indre anliggender og cybersikkerhed spiller også en central rolle, som er blevet større som følge af nylige udvidelser af deres ansvarsområder.

Øget screening af modtagere af EU-midler

I forbindelse med gennemførelsen af EU-budgettet har Kommissionen et ansvar for at sikre, at modtagere af EU-midler respekterer EU's værdier. De mekanismer og kontrolsystemer, der afgør, hvem der kan modtage EU-finansiering, er allerede robuste, og de igangværende forhandlinger om omarbejdning af finansforordningen har også til formål at give Kommissionen stærkere retlige midler til at handle, hvis det er nødvendigt. Kommissionen undersøger desuden i øjeblikket, hvordan screeningen af nuværende og potentielle fremtidige modtagere af EU-midler kan forbedres yderligere ved at forbedre vejledningen om forpligtelser vedrørende respekt for EU's værdier og de konsekvenser, der bør følge af en overtrædelse af EU's værdier. Dette vil præcisere ansvarsområderne for både støttemodtagere og de aktører, der udfører kontrol på EU-plan, og kan bruges som inspirationskilde på nationalt plan. I tilfælde af overtrædelse af finansieringsbetingelserne tøver Kommissionen ikke og vil ikke tøve med at standse samarbejdet med støttemodtagerne under det pågældende projekt og om nødvendigt inddrive midler. Det er vigtigt, at medlemsstaterne proaktivt udveksler oplysninger med Kommissionen, når de har kendskab til mulige risici i forbindelse med organisationer, der ansøger om EU-midler.

Overtrædelser

På sikkerhedsområdet har Kommissionen gennemført mange traktatbrudsprocedurer. I 2023 blev der f.eks. indledt et stort antal traktatbrudssager på grund af manglende overholdelse af forpligtelserne i henhold til forordningen fra 2021 om udbredelse af terrorrelateret indhold online (16 medlemsstater)[50], og i løbet af 2022 og 2023 modtog 20 medlemsstater yderligere åbningsskrivelser på grund af ukorrekt gennemførelse af direktivet fra 2011 om bekæmpelse af seksuelt misbrug af børn[51]. Der er stadig et betydeligt antal uafsluttede traktatbrudssager vedrørende manglende overensstemmelse mellem national ret og direktivet om bekæmpelse af terrorisme fra 2017[52] og manglende gennemførelse af regler, der letter brugen af finansielle og andre oplysninger til forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger[53]. Andre områder, hvor der er verserende traktatbrudssager, er lovgivningen om skydevåben, regler om psykoaktive stoffer, der anvendes i narkotika, bekæmpelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter, bekæmpelse af hvidvask af penge, udveksling af oplysninger fra strafferegistre mellem EU's medlemsstater og direktivet om ofres rettigheder. Støtte (teknisk og finansiel) er blevet stillet til rådighed for medlemsstater, der gennemfører vedtagne initiativer og foranstaltninger, og Kommissionen står fortsat til rådighed for at samarbejde med medlemsstaterne om at optimere gennemførelsen.

---

[50] Forordning (EU) 2021/784 om håndtering af udbredelsen af terrorrelateret indhold online.

[51] Direktiv 2011/93/EU om bekæmpelse af seksuelt misbrug af børn.

[52] Europa-Parlamentets og Rådets direktiv (EU) 2017/541 af 15. marts 2017 om bekæmpelse af terrorisme og om erstatning af Rådets rammeafgørelse 2002/475/RIA og ændring af Rådets afgørelse 2005/671/RIA.

[53] Europa-Parlamentets og Rådets direktiv (EU) 2019/1153 af 20. juni 2019 om regler, der letter brugen af finansielle og andre oplysninger med henblik på forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger, og om ophævelse af Rådets afgørelse 2000/642/RIA.

Overvågning gennem Schengenevalueringer og det nye forvaltningssystem

Schengenevaluerings- og overvågningsmekanismen har fortsat bidraget til en effektiv gennemførelse af Schengenreglerne, som har til formål at øge sikkerheden i området uden kontrol ved de indre grænser. I 2023 blev de første evalueringer under den styrkede Schengenevaluerings- og overvågningsmekanisme gennemført, hvilket gav mulighed for rettidig identifikation og afhjælpning af strategiske sårbarheder, som har en grænseoverskridende indvirkning på sikkerheden i EU. Desuden iværksatte Kommissionen i 2023 en tematisk Schengenevaluering for at vurdere praksis i de medlemsstater, der står over for lignende udfordringer i forbindelse med bekæmpelse af narkotikahandel til EU, navnlig med fokus på narkotikahandel i stort omfang. Med disse evalueringer kom der et styrket og mere omfattende fokus på sikkerhedselementerne i Schengen. På grundlag af resultaterne af de periodiske, tematiske og uanmeldte Schengenevalueringer fastlagde Rådet i juni 2023 prioriteterne for Schengencyklussen for 2023-2024. Der er fastlagt fokusområder, som der skal sættes yderligere skub i, for at gøre Schengenområdet mere sikkert og stærkere. En effektiv og hurtig gennemførelse af disse prioriteter vil sammen med øget politikkoordinering i Schengenrådet yderligere styrke bekæmpelsen af organiseret kriminalitet og maksimere det grænseoverskridende operationelle samarbejde.

EU-agenturernes og -organernes rolle

Partnerskab er afgørende for gennemførelsen af initiativer inden for rammerne af sikkerhedsunionen, da det arbejde, der udføres af forskellige nationale og europæiske myndigheder og organer, er nødvendigt for at opnå konkrete resultater. EMPACT (den europæiske tværfaglige platform mod kriminalitetstrusler) muliggør f.eks. struktureret tværfagligt samarbejde mellem medlemsstaterne med støtte fra alle EU's institutioner, organer, kontorer og agenturer (såsom Europol, Frontex, Eurojust, Cepol, OLAF og eu-LISA). De operationer, der udføres af EMPACT, herunder gennem særlige operationelle taskforcer, koordinerer medlemsstaternes og de operationelle partneres indsats for at bekæmpe kriminelle netværk og grov kriminalitet. Alene i 2022 resulterede EMPACT i 9 922 anholdelser, aktiver og pengebeløb på over 180 mio. EUR blev beslaglagt, der blev indledt 9 263 efterforskninger, 4 019 ofre blev identificeret, over 62 ton narkotika blev beslaglagt, 51 højværdimål blev identificeret, og 12 personer blev arresteret, og der blev gennemført operationer i forbindelse med angrebskrigen mod Ukraine, navnlig for at bekæmpe menneskehandel og trusler relateret til skydevåben.

Frontex, Det Europæiske Agentur for Søfartssikkerhed (EMSA) og Det Europæiske Fiskerikontrolagentur (EFCA) styrker fortsat deres samarbejde om kystvagtfunktioner for at støtte de nationale myndigheders indsats for at øge sikkerheden til søs. Disse agenturer vil yde et vigtigt bidrag til gennemførelsen af EU-strategien for maritim sikkerhed.

Flere initiativer inden for rammerne af sikkerhedsunionen har givet relevante agenturer nye ansvarsområder og opgaver, nogle gange med konsekvenser for de menneskelige ressourcer.

Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)

Med hensyn til beredskab og indsats i forbindelse med hændelser for at øge cybersikkerheden har Kommissionen oprettet en kortsigtet foranstaltning ved at overføre midler fra programmet for et digitalt Europa til **Den Europæiske Unions Agentur for Cybersikkerhed (ENISA)** for at styrke beredskabet og kapaciteten til at reagere på større cyberhændelser. Forslaget til forordning om cybersolidaritet, der blev vedtaget i april 2023, bygger på denne foranstaltning

og kan, når det er vedtaget af de to lovgivere, overdrage ENISA yderligere opgaver såsom driften og administrationen af den fremtidige EU-cybersikkerhedsreserve eller udarbejdelsen af en rapport om hændelsen efter omfattende cybersikkerhedshændelser. Den foreslåede forordning om cyberrobusthed vil pålægge ENISA at modtage underretninger fra fabrikanter om sårbarheder i produkter med digitale elementer og hændelser, der indvirker på disse produkters sikkerhed, som ENISA forventes at videresende til de relevante CSIRT-netværk eller til de relevante centrale kontaktpunkter i medlemsstaterne. Det forventes også, at ENISA hvert andet år udarbejder en teknisk rapport om nye tendenser med hensyn til cybersikkerhedsrisici forbundet med produkter med digitale elementer og forelægger den for NIS-samarbejdsgruppen.

Det Europæiske Kompetencecenter for Cybersikkerhed

Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC) er sammen med Netværket af Nationale Koordinationscentre Unionens nye organ til støtte for innovation og industripolitik inden for cybersikkerhed. Dette økosystem vil styrke cybersikkerhedsteknologiens kapacitet, opretholde topforskning og styrke EU-industriens konkurrenceevne på dette område. ECCC og de nationale koordinationscentre vil træffe strategiske investeringsbeslutninger og samle ressourcer fra Unionen, medlemsstaterne og indirekte fra industrien for at forbedre og styrke den teknologiske og industrielle cybersikkerhedskapacitet. ECCC spiller derfor en central rolle med hensyn til at opfylde de ambitiøse cybersikkerhedsmål i programmerne for et digitalt Europa og Horisont Europa.

ECCC har ansat mere end halvdelen af sit personale og vil snart ansætte sin administrerende direktør. Der arbejdes allerede nu med cybersikkerhedsdelen af programmet for et digitalt Europa og en ny strategisk dagsorden[54] for udvikling og udbredelse af teknologier, som fastsætter prioriterede foranstaltninger, der skal støtte SMV'ernes udvikling og anvendelse af strategiske cybersikkerhedsteknologier, -tjenester og -processer, støtte og øge den professionelle arbejdsstyrke og styrke forsknings-, udviklings- og innovationsekspertise i det bredere europæiske cybersikkerhedsøkosystem.

Europol

Med et helt nyt mandat vil **Europol** være bedre rustet til at støtte medlemsstaterne i bekæmpelsen af organiseret kriminalitet. Bekæmpelse af narkotikahandel er en nøgleprioritet i betragtning af dens voksende betydning og stigende negative indvirkning på EU-borgernes sikkerhed. Efter bemyndigelse fra Rådet for Den Europæiske Union den 15. maj 2023 har Kommissionen aktivt arbejdet hen imod indgåelse af internationale aftaler med Bolivia, Brasilien, Ecuador, Mexico og Peru om udveksling af personoplysninger med Europol med henblik på at forebygge og bekæmpe grov kriminalitet og terrorisme.

Eurojust

Med over 20 års erfaring med at yde juridisk støtte til nationale myndigheder med henblik på at bekæmpe en lang række alvorlige og komplekse grænseoverskridende forbrydelser har **Eurojust** cementeret sin stilling i EU's område med frihed, sikkerhed og retfærdighed. For at styrke samarbejdet generelt forhandler Kommissionen internationale aftaler for at lette samarbejdet mellem Eurojust og 13 tredjelande om udveksling af personoplysninger for at bekæmpe organiseret kriminalitet og terrorisme[55]. Forhandlingerne med Armenien og Libanon allerede afsluttet, igangværende med Algeriet og Colombia og indledt med Bosnien-

[54] https://cybersecurity-centre.europa.eu/strategic-agenda_da.

[55] Algeriet, Argentina, Armenien, Bosnien-Hercegovina, Brasilien, Colombia, Egypten, Israel, Jordan, Libanon, Marokko, Tunesien og Tyrkiet.

Hercegovina. Kommissionen opfordrer Europa-Parlamentet og Rådet til at afslutte indgåelsen af aftaler med disse lande inden udgangen af valgperioden for at styrke det tværnationale retlige samarbejde og udvide bekæmpelsen af grænseoverskridende kriminalitet.

EPPO

Siden **Den Europæiske Anklagemyndighed (EPPO)** påbegyndte sine operationelle aktiviteter i juni 2021, har den vist sig at være et effektivt redskab i Unionens værktøjskasse til efterforskning og retsforfølgning af strafbare handlinger, der skader Unionens budget, herunder lovovertrædelser i forbindelse med deltagelse i en kriminel organisation, når der er fokus på strafbare handlinger, der skader Unionens budget. Kommissionen opfordrer de medlemsstater, der endnu ikke deltager i det forstærkede samarbejde i EPPO, til at gøre dette hurtigst muligt for at drage fordel af EPPO's fulde potentiale med hensyn til at beskytte EU's skatteyderes penge.

EUDA

Med et nyt mandat, der blev vedtaget af de to lovgivere i juni 2023, vil det eksisterende Europæiske Overvågningscenter for Narkotika og Narkotikamisbrug (EMCDDA) blive til et egentligt agentur — **Den Europæiske Unions Narkotikaagentur (EUDA)** — med en styrket rolle. Agenturet vil være i stand til at vurdere nye sundheds- og sikkerhedsmæssige udfordringer i forbindelse med ulovlig narkotika på en mere omfattende måde og bidrage mere effektivt til arbejdet i medlemsstaterne og på internationalt plan. Indsamling, analyse og formidling af data vil fortsat være agenturets hovedopgave, men det udvidede mandat vil også gøre det muligt for agenturet at udvikle generelle trusselsvurderingskapaciteter på sundheds- og sikkerhedsområdet med henblik på at identificere nye trusler, herunder blandingsbrug, styrke dets samarbejde gennem nationale kontaktpunkter og oprette et netværk af laboratorier, der giver agenturet kriminaltekniske og toksikologiske oplysninger. Dette vil gøre det lettere for agenturet at udsende varslinger, når der dukker særligt farlige stoffer op på markedet, og oplyse herom.

Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigst muligt at afslutte de interinstitutionelle forhandlinger, under alle omstændigheder inden udløbet af det nuværende Europa-Parlaments mandat, om følgende verserende sager:

- forslag til omarbejdning af finansforordningen.

Kommissionen opfordrer medlemsstaterne til:

- proaktivt at udveksle oplysninger med Kommissionen, når de har kendskab til mulige risici i forbindelse med organisationer, der ansøger om EU-midler
- hurtigt at gennemføre prioriteterne i Schengencyklussen 2023-2024 for at gøre Schengenområdet mere sikkert og stærkere
- behandle de traktatbrudsprocedurer, der er indledt mod dem, for at sikre en korrekt gennemførelse af den pågældende lovgivning.

VII. Konklusion

De seneste tre år har været karakteriseret ved en konstant og beslutsom indsats for at opfylde ambitionen om at skabe en sikkerhedsunion for EU. Der er gjort meget store fremskridt på hele det sikkerhedspolitiske område. I dag kræver de konstant foranderlige trusler, at der gøres en kontinuerlig indsats med fornyet motivation. Arbejdet med den lovgivningsmæssige ramme skal afsluttes i god tid inden udgangen af valgperioden i foråret 2024. Medlemsstaterne har et løbende ansvar for at omsætte, gennemføre og anvende ny lovgivning. Gennemførelsen kræver en samordnet indsats, herunder med støtte fra EU-agenturerne — og meget ofte et stadig stærkere samarbejde med vores internationale partnere.

Kun gennem en kollektiv og beslutsom indsats fra alle berørte parters side kan vi opnå de sikkerhedsniveauer i EU, som borgerne forventer — og under de nuværende omstændigheder bør det være en prioritet for alle aktører at spille deres rolle i styrkelsen af EU's sikkerhed.