Rådet for
Den Europæiske Union

Bruxelles, den 3. april 2025
(OR. en)

7750/25

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

FØLGESKRIVELSE

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	2. april 2025
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union
Komm. dok. nr.:	COM(2025) 148 final
Vedr.:	MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET ProtectEU – en EU-strategi for indre sikkerhed

Hermed følger til delegationerne dokument COM(2025) 148 final.

Bilag: COM(2025) 148 final

EUROPA-
KOMMISSIONEN

Strasbourg, den 1.4.2025
COM(2025) 148 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, RÅDET, DET EUROPÆISKE ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

ProtectEU – en EU-strategi for indre sikkerhed

1. ProtectEU – en EU-strategi for indre sikkerhed

Sikkerhed er det fundament, som alle vores frihedsrettigheder bygger på. Demokratiet, retsstaten, de grundlæggende rettigheder, europæernes velfærd, konkurrenceevnen og velstanden – det hele afhænger grundlæggende af vores evne til at garantere sikkerheden. I den nye æra med sikkerhedstrusler, vi nu oplever, er EU-medlemsstaternes evne til at garantere deres borgeres sikkerhed mere end nogensinde betinget af, at der en **fælles europæisk tilgang til beskyttelse af den indre sikkerhed**. I et geopolitisk landskab, der til stadighed udvikler sig, skal Europa fortsat leve op til sit varige løfte om fred.

De første skridt i retning af at opbygge et europæisk sikkerhedsapparat er allerede taget. De seneste ti år har vi givet Unionen forbedrede kollektive indsatsmekanismer inden for retshåndhævelse og retligt samarbejde, grænsesikkerhed, bekæmpelse af grov og organiseret kriminalitet, bekæmpelse af terrorisme og voldelig ekstremisme og beskyttelse af EU's fysiske og digitale kritiske infrastruktur. Det er fortsat afgørende, at tidligere vedtaget lovgivning og fastlagte politikker gennemføres på korrekt vis.

Nutidens trusler og den iboende forbindelse mellem EU's indre og ydre sikkerhed kræver, at vi går endnu længere.

Trusselsbilledet er alvorligt. Grænserne mellem **hybride trusler** og åben krigsførelse er udviskede. Rusland har ført en hybrid online- og offlinekampagne mod EU og dets partnere for at forstyrre og underminere samhørigheden i samfundet og de demokratiske processer og for at sætte EU's solidaritet med Ukraine på prøve. Fjendtlige udenlandske stater og statsstøttede aktører forsøger at infiltrere og forstyrre vores kritiske infrastruktur og forsyningskæder, stjæle følsomme oplysninger og positionere sig med henblik på fremover at skabe de størst mulige forstyrrelser. De bruger kriminalitet som en tjeneste og kriminelle som stedfortrædere. Derudover gør vores afhængighed af tredjelande med hensyn til forsyningskæderne os mere sårbare over for fjendtlige staters hybride kampagner.

Som fremhævet i EU's trusselsvurdering af grov og organiseret kriminalitet (SOCTA), som Europol for nylig fremlagde[1], spreder stadig flere magtfulde **organiserede kriminelle netværk** sig i Europa, øger deres styrke ved hjælp af internettet og infiltrerer vores økonomi og vores samfund. Når organiseret kriminalitet først har fået fodfæste i et lokalsamfund eller en økonomisk sektor, bliver det en kamp op ad bakke at udrydde den: En tredjedel af de mest truende kriminelle netværk har været aktive i over ti år. Ved hjælp af kryptovalutaer og parallelle finansielle systemer hvidvasker og skjuler de deres udbytte fra strafbart forhold.

Terrortrusselsniveauet i Europa er fortsat højt. Regionale kriser uden for EU har en afsmittende virkning, der giver terroraktører på tværs af hele det ideologiske spektrum ny motivation til at rekruttere, mobilisere eller opbygge deres kapacitet. De målretter deres radikaliserings- og rekrutteringsindsats specifikt mod de mest sårbare grupper i vore samfund og navnlig bestemte grupper af unge. De inspirerer enkeltpersoner til at gennemføre angreb og skaber en kraftig stigning i den systemfjendtlige ekstremisme, hvis mål er at forstyrre den demokratiske retsorden.

De store og hurtige **teknologiske fremskridt**, der gøres, giver os vigtige redskaber til at forbedre vores sikkerhedsapparat. Udnyttelsen af nye teknologier såsom kunstig intelligens bevirker imidlertid, at der hyppigere forekommer cyberangreb og udenlandsk informationsmanipulation. Børn, unge og ældre er særligt udsatte online, og udbredelsen af hadpropaganda på internettet truer ytringsfriheden og den sociale samhørighed.

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

Vores liv er blevet mindre sikkert, og det mærker europæerne i stigende grad. Deres **opfattelse af tryghed og sikkerhed i EU** er blevet svækket i en sådan grad, at når de bliver spurgt om fremtiden, giver 64 % udtryk for bekymring med hensyn til EU's sikkerhed[2]. Virksomhederne bliver også i stigende grad berørt. Misinformation og desinformation, kriminalitet og ulovlig aktivitet samt cyberspionage hører alt sammen til blandt de ti største risici, der er kortlagt i Det Verdensøkonomiske Forums "Global Risks Report 2025"[3].

Europæerne bør **kunne leve deres liv uden frygt**, hvad enten det er på gaden, hjemme, på offentlige steder, i metroen eller på internettet. Beskyttelsen af mennesker, navnlig dem, der er mest sårbare over for angreb, som har tendens til at ramme børn, kvinder og mindretal, herunder jødiske og muslimske samfund, uforholdsmæssigt hårdt, er kernen i EU's arbejde for sikkerhed. Det er afgørende for at opbygge modstandsdygtige og sammenhængende samfund.

Kommissionen er ved at udforme en **EU-strategi for indre sikkerhed** for bedre at kunne imødegå trusler i de kommende år. Med et sæt skarpere retlige værktøjer, et tættere samarbejde og øget informationsudveksling vil vi øge vores modstandsdygtighed og kollektive evne til at foregribe, forebygge, opdage og reagere effektivt på sikkerhedstrusler. En fælles strategi for indre sikkerhed kan hjælpe medlemsstaterne med at udnytte teknologi til at styrke og ikke svække sikkerheden, samtidig med at der skabes et sikkert digitalt rum for alle. Ved hjælp af strategien vil medlemsstaterne desuden i højere grad i fællesskab kunne reagere på globale politiske og økonomiske forandringer, der påvirker Unionens indre sikkerhed.

Strategien er baseret på **tre principper**, og centralt i den er respekten for retsstatsprincippet og de grundlæggende rettigheder.

For det første fastsættes der heri en ambition om at ændre kulturen på sikkerhedsområdet. Vi har brug for **en tilgang, hvor hele samfundet inddrages**, og som involverer alle borgere og interessenter, herunder civilsamfundet, forskere, den akademiske verden og private enheder Foranstaltningerne inden for rammerne af strategien bygger derfor på en integreret tilgang med inddragelse af flere interessenter, hvor det er muligt.

For det andet skal **sikkerhedshensyn medtages og integreres i al EU-lovgivning og i alle EU-politikker og -programmer**, herunder EU's optræden udadtil. Lovgivning, politikker og programmer skal udarbejdes, revideres og gennemføres ud fra et sikkerhedsmæssigt perspektiv, så det sikres, at der tages de nødvendige sikkerhedsmæssige hensyn, for derved at fremme en sammenhængende og samlet tilgang til sikkerhed.

Endelig kræver et sikkert og modstandsdygtigt Europa **betydelige investeringer fra EU, medlemsstaterne og den private sektor**. De prioriteter og foranstaltninger, der er fastsat i denne strategi, kræver, at der stilles tilstrækkelige menneskelige og finansielle ressourcer til rådighed til at sikre gennemførelsen heraf. Som fastsat i meddelelsen om vejen til den næste flerårige finansielle ramme[4] vil Europa skulle øge de offentlige udgifter til sikkerhed og fremme forskning og investeringer på sikkerhedsområdet for derved at styrke sin strategiske autonomi.

Denne strategi supplerer **strategien for en beredskabsunion**[5], hvori der fastsættes en integreret tilgang til beredskab over for konflikter, menneskeskabte katastrofer og naturkatastrofer og kriser, og som omfatter alle farer, og **hvidbogen om europæisk forsvarsberedskab 2030**[6], som støtter udviklingen og anskaffelsen af forsvarsressourcer i hele EU for at afskrække udenlandske modstandere. Kommissionen vil også fremsætte forslag til et **europæisk**

[2] Flash Eurobarometer-undersøgelse FL550: EU challenges and priorities.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, s. 17.
[4] COM(2025) 46 final.
[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.

demokratiskjold for at styrke den demokratiske modstandsdygtighed i EU. Med disse initiativer udstikkes der en vision for et trygt, sikkert og modstandsdygtigt EU.

En ny forvaltning af Europas indre sikkerhed

Kommissionen vil arbejde tæt sammen med medlemsstaterne og EU-agenturerne om at opgradere EU's tilgang til den indre sikkerhed på både strategisk og operationelt plan.

Det skal gøres ved:

- **fra starten og gennem hele forhandlingsprocessen konsekvent at kortlægge de sikkerheds- og beredskabsmæssige virkninger af Kommissionens initiativer**
- **regelmæssigt at holde møder i Kommissionens projektgruppe om EU's indre sikkerhed, der understøttes af et strategisk tværsektorielt samarbejde i hele Kommissionen**
- **at fremlægge trusselsanalyser vedrørende den indre sikkerhed til støtte for sikkerhedsakademiets arbejde**
- **på grundlag af trusselsanalysen at drøfte udviklingen i udfordringerne i forbindelse med den indre sikkerhed og centrale politiske prioriteter med medlemsstaterne i Rådet**
- **regelmæssigt at rapportere til Europa-Parlamentet og Rådet for at følge og støtte gennemførelsen af vigtige initiativer**

2. Integreret situationsbevidsthed og trusselsanalyse

Vi vil sikre, at EU råder over nye måder til at dele og kombinere oplysninger på, og udarbejde en regelmæssig trusselsanalyse, hvad angår EU's indre sikkerhed, der bidrager til en omfattende risiko- og trusselsvurdering.

Sikkerhed begynder med en **effektiv foregribelse**. EU skal forlade sig på en omfattende, tilstrækkeligt uafhængig og ajourført situationsbevidsthed og trusselsanalyse. Handlingsrettede efterretninger, som medlemsstaterne opfordres til at styrke yderligere gennem den fælles efterretningsanalysekapacitet (SIAC), der er det centrale kontaktpunkt for medlemsstaternes efterretninger, er afgørende for at vurdere og imødegå trusler og i sidste ende som grundlag for politiske og lovgivningsmæssige tiltag[7]. Vi er nødt til at udnytte **efterretningsbaserede analyser** og **trusselsvurderinger** på EU-plan på mere effektiv og samarbejdsorienteret vis.

På grundlag af de forskellige risiko- og trusselsvurderinger, der udarbejdes på EU-plan og for specifikke sektorer[8], vil Kommissionen udarbejde **regelmæssige trusselsanalyser vedrørende EU's indre sikkerhed** for at kortlægge de vigtigste sikkerhedsudfordringer, hvilket skal danne grundlag for fastlæggelsen af politiske prioriteter. De vil bidrage til at fastlægge en smidig og reaktionsdygtig intern sikkerhedspolitik til at håndtere nye trusler effektivt, beskytte mennesker og virksomheder bedre mod angreb og muliggøre målrettede politiske indgreb rettidigt. Disse trusselsanalyser vedrørende EU's indre sikkerhed vil også bidrage til **EU's omfattende risikovurdering og trusselsvurdering (der er tværsektoriel og omfatter alle farer)**, der er

[7] Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readines, s. 23.

[8] De sektorspecifikke trusselsvurderinger, der bl.a. skal danne grundlag for denne trusselsanalyse, omfatter EU's trusselsvurdering af grov og organiseret kriminalitet (SOCTA), EU's rapport om situationen og udviklingen med hensyn til terrorisme i EU (TE-SAT), den fælles cybervurderingsrapport (JCAR) og fremtidige vurderinger af trusler, risici og metoder på området hvidvask af penge og finansiering af terrorisme, der skal foretages af Kommissionen og Myndigheden for Bekæmpelse af Hvidvask af Penge.

udarbejdet af Kommissionen og den højtstående repræsentant, som fastsat i strategien for en beredskabsunion.

Tillid og sikker håndtering er afgørende for udvekslingen af oplysninger, og dette kræver pålidelig og sikker infrastruktur. EU's institutioner, organer og agenturer skal sikre, at de er i stand til at anvende **sikre kommunikationskanaler** til udveksling af følsomme og klassificerede oplysninger indbyrdes og med medlemsstaterne. Investeringer i **interoperable sikre systemer** og pålidelig teknologi vil styrke EU's autonomi og evne til at håndtere kriser og sikre operationel modstandsdygtighed. I den forbindelse opfordrer Kommissionen indtrængende Europa-Parlamentet og Rådet til at afslutte forhandlingerne om **forslaget til forordning om informationssikkerhed i Unionens institutioner, organer, kontorer og agenturer**, navnlig for at sikre en fælles ramme for håndtering af følsomme ikkeklassificerede og klassificerede oplysninger[9].

For at sikre sin egen operationelle sikkerhed og situationsbevidsthed vil Kommissionen revidere sin ramme for styring af sikkerheden og oprette **et integreret sikkerhedsoperationscenter (ISOC)** for at beskytte mennesker, fysiske aktiver og operationer på tværs af alle Kommissionens lokaliteter. Kommissionen vil også styrke sin operationelle og analytiske kapacitet til at indkredse og afbøde hybride trusler.

I overensstemmelse med strategien for en beredskabsunion vil beredskabs- og sikkerhedshensyn blive medtaget og integreret i al EU-lovgivning og i alle EU's politikker og programmer. Ved udarbejdelsen eller revisionen af lovgivning, politikker og programmer vil Kommissionen ud fra et beredskabs- og sikkerhedsmæssigt perspektiv konsekvent kortlægge, hvordan den foretrukne politiske løsning kan påvirke beredskabet og sikkerheden. Dette vil blive understøttet af regelmæssig uddannelse af beslutningstagere i Kommissionen.

For at støtte medlemsstaterne vil Kommissionen drøfte udviklingen i udfordringerne i forbindelse med den indre sikkerhed og centrale politiske prioriteter med Rådet og regelmæssigt orientere den om gennemførelsen af strategien. Derudover vil Kommissionen holde Europa-Parlamentet og relevante interessenter underrettet og involveret i alle relevante foranstaltninger.

Vigtige tiltag

Kommissionen vil:

- **udarbejde og fremlægge regelmæssige trusselsanalyser af udfordringerne i forbindelse med EU's indre sikkerhed**

Medlemsstaterne opfordres til at:

- **styrke udvekslingen af efterretninger med SIAC og sikre bedre informationsudveksling med EU-agenturer og -organer**

Europa-Parlamentet og Rådet opfordres til at:

- **afslutte forhandlingerne om forslaget til forordning om informationssikkerhed i Unionens institutioner, organer, kontorer og agenturer**

3. Styrkelse af EU's sikkerhedsmæssige kapacitet

Vi vil udvikle nye værktøjer til retshåndhævelse såsom et moderniseret Europol og bedre midler til at koordinere og sikre sikker udveksling af og lovlig adgang til oplysninger.

[9] COM(2022) 119 final.

For effektivt at imødegå nye trusler skal EU styrke sin sikkerhedsmæssige kapacitet og fremme innovation. De retshåndhævende og de retslige myndigheder har som de primære aktører til bekæmpelse af trusler mod den indre sikkerhed brug for de rette operationelle værktøjer og kapaciteter til at handle hurtigt og effektivt. Det er vigtigt, at disse myndigheder er i stand til at kommunikere og koordinere på tværs af grænser og tjenester for effektivt at forebygge, opdage, efterforske og retsforfølge strafbare handlinger.

EU-agenturer og -organer for den indre sikkerhed

EU-agenturerne og -organerne vedrørende retlige anliggender, indre anliggender og cybersikkerhed spiller en nøglerolle i EU's sikkerhedsarkitektur – en rolle, som bliver stadig større, efterhånden som deres ansvar bliver udvidet.

I dag 25 år efter oprettelsen af **Europol** spiller agenturet en mere central rolle end nogensinde før for EU's sikkerhedsramme. Det støtter komplekse grænseoverskridende efterforskninger, letter udvekslingen af oplysninger, udvikler innovative værktøjer til politiarbejde og yder avanceret ekspertise til retshåndhævelse. Flere faktorer forhindrer imidlertid Europol i fuldt ud at nå sit operationelle potentiale med hensyn til at støtte efterforskningsmæssige og operationelle aktiviteter til bekæmpelse af grænseoverskridende kriminalitet: De spænder lige fra utilstrækkelige ressourcer til det forhold, at dets nuværende mandat ikke omfatter nye sikkerhedstrusler såsom sabotage, hybride trusler eller informationsmanipulation. Derfor vil Kommissionen fremsætte forslag til **en ambitiøs revision af Europols mandat** for at gøre det til et reelt operationelt politiagentur, der i højere grad støtter medlemsstaterne. Målet er at styrke Europols teknologiske ekspertise og kapacitet til at støtte de nationale retshåndhævende myndigheder, forbedre koordineringen med andre agenturer og organer og med medlemsstaterne, styrke de strategiske partnerskaber med partnerlande og den private sektor og sikre et øget tilsyn med Europol.

Kommissionen vil desuden arbejde på yderligere at **forbedre komplementariteten mellem EU's agenturer og organer for indre sikkerhed og deres effektivitet samt styrke et gnidningsløst samarbejde** mellem dem.

Eurojusts mandat vil blive vurderet og styrket med henblik på et mere effektivt retligt samarbejde, der øger komplementariteten og samarbejdet med Europol. Det omfatter forbedring af Eurojusts effektivitet og dets kapacitet til at yde proaktiv støtte til og stille analyser til rådighed for medlemsstaternes retslige myndigheder. I betragtning af **EPPO's** unikke kompetence til at efterforske og retsforfølge strafbare handlinger, der skader Unionens finansielle interesser, vil Kommissionen desuden overveje, hvordan EPPO's kapacitet til at beskytte Unionens midler bedst kan forbedres. Det vil bl.a. omfatte en styrkelse af samarbejdet mellem EPPO og Europol.

Effektiv og sikker udveksling af oplysninger mellem agenturer er afgørende for samarbejdet. Europol og Frontex har brug for hurtig gensidig udveksling af oplysninger, bl.a. til operationelle formål, som opfølgning på den fælles erklæring fra januar 2024[10]. **eu-LISA** spiller en central rolle med hensyn til at sikre sikker lagring og tilgængelighed af oplysninger med henblik på bedre koordinering og mere effektiv informationsudveksling mellem agenturerne. **Den Europæiske Unions Agentur for Grundlæggende Rettigheder** yder ekspertise inden for beskyttelse af grundlæggende rettigheder i forbindelse med fastlæggelse og gennemførelse af sikkerhedspolitikker.

EU's Myndighed for Bekæmpelse af Hvidvask af Penge (AMLA) har fået beføjelse til på grundlag af hit/intet hit at krydstjekke oplysninger med oplysninger fra Europol, EPPO,

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

Eurojust og EU's Kontor for Bekæmpelse af Svig med henblik på at foretage fælles analyser af grænseoverskridende sager.

ENISA spiller en central rolle i forbindelse med gennemførelsen af europæisk lovgivning om cybersikkerhed. I forbindelse med den kommende **revision af forordningen om cybersikkerhed** vil Kommissionen vurdere dets mandat og fremsætte forslag til en modernisering af det for at øge dets EU-merværdi.

Samarbejdet mellem toldmyndighederne og andre retshåndhævende myndigheder vil blive øget med den foreslåede oprettelse af **EU-Toldmyndigheden** og **EU's tolddatacenter** inden for rammerne af EU's toldreformpakke. Oplysninger fra det fremtidige tolddatacenter og relaterede oplysninger fra Europol, Eurojust, EPPO, OLAF, AMLA og Frontex inden for rammerne af deres respektive beføjelser vil styrke den fælles analyse og bidrage til mere sammenhængende operationelle aktiviteter, navnlig ved de ydre grænser. Kommissionen opfordrer Europa-Parlamentet og Rådet til hurtigt at afslutte forhandlingerne om EU's toldreform og vil fortsat bistå dem med henblik herpå.

Den øgede komplementaritet mellem EPPO, OLAF, Europol, Eurojust, AMLA og den foreslåede EU-Toldmyndighed vil også bygge på resultaterne af den igangværende revision af **EU's struktur for bekæmpelse af svig**. Denne helhedsorienterede tilgang med fokus på bedre anvendelse af både strafferetlige og administrative midler, interoperabilitet mellem IT-systemer og forbedret samarbejde vil gavne den indre sikkerhed.

Kritisk kommunikation

I dag fungerer **kritiske kommunikationssystemer**[11] i de fleste tilfælde isoleret på nationalt plan. Det betyder, at beredskabspersonel ofte ikke kan kommunikere med deres modparter, når de krydser grænsen til andre medlemsstater. I nogle medlemsstater er der også begrænsninger for kommunikationen mellem forskellige typer beredskabspersonel (f.eks. politi og ambulanceførere). Standarderne for de fleste systemer opfylder ikke de nuværende krav med hensyn til funktionalitet og modstandsdygtighed, hvilket i væsentlig grad begrænser beredskabspersonellets reaktionskapacitet, navnlig på tværs af grænserne.

For at forbedre EU's kapacitet til at reagere på kriser vil Kommissionen fremsætte forslag til lovgivning med henblik på oprettelse af et **europæisk system for kritisk kommunikation (EUCCS)**, der skal forbinde medlemsstaternes næste generation af systemer for kritisk kommunikation i EU. Målet er, at EUCCS skal baseres på tre strategiske søjler: operationel mobilitet, stærk modstandsdygtighed og strategisk autonomi. Med EUCCS-initiativet vil der blive fastsat harmoniserede krav, og det vil bidrage til at modernisere medlemsstaternes systemer for kritisk kommunikation, så de kan fungere gnidningsløst. Det vil også udvide systemdækningen ved hjælp af det fremtidige multiorbitale IRIS^2-system[12]. Ved hjælp af EU-finansierede projekter vil den tekniske kapacitet for EUCCS, der primært har europæiske teknologileverandører, blive opbygget for derved at fremme EU's strategiske autonomi i denne følsomme sektor.

Lovlig adgang til oplysninger

Retshåndhævende og retslige myndigheder skal kunne efterforske og gribe ind over for kriminalitet. Nu til dags har næsten alle former for grov og organiseret kriminalitet et digitalt

[11] Dvs. de netværk, der anvendes af de retshåndhævende myndigheder, grænsevagter, toldmyndigheder, civilbeskyttelsespersonel, brandmænd, medicinsk katastrofeberedskabspersonel og andre nøgleaktører på området offentlig sikkerhed.
[12] EU-infrastruktur for modstandsdygtighed, sammenkobling og sikkerhed via satellit.

fodaftryk[13]. Omkring 85 % af de strafferetlige efterforskninger afhænger i dag af de retshåndhævende myndigheders mulighed for at tilgå digitale oplysninger[14].

Gruppen på Højt Plan om Adgang til Data med henblik på Effektiv Retshåndhævelse fremhævede i sin afsluttende rapport[15], at de retshåndhævende myndigheder og retsvæsenet har mistet terræn til de kriminelle i løbet af det seneste årti, da de kriminelle benytter sig af værktøjer og produkter, som stilles til rådighed i andre jurisdiktioner af udbydere, der har truffet foranstaltninger, der fratager dem muligheden for at samarbejde, når der fremsættes retslige begæringer i individuelle straffesager. Systematisk samarbejde mellem retshåndhævende myndigheder og private parter, herunder tjenesteudbydere, er derfor afgørende i de fremtidige bestræbelser på at bekæmpe de mest truende kriminelle netværk og enkeltpersoner i og uden for Unionen.

Efterhånden som digitalisering bliver mere udbredt og udgør en stadig større kilde til nye værktøjer for kriminelle, er det vigtigt at have en ramme for adgang til oplysninger, der imødekommer behovet for at håndhæve vores lovgivning og beskytte vores værdier. Samtidig er det lige så vigtigt at sikre, at digitale systemer fortsat er sikret mod uautoriseret adgang, for at bevare cybersikkerheden og beskytte mod nye sikkerhedstrusler. Disse rammer for adgang til oplysninger skal også være i overensstemmelse med de grundlæggende rettigheder og bl.a. sikre, at privatlivets fred og personoplysninger beskyttes tilstrækkeligt.

I de seneste år har EU med vedtagelsen af regler om elektronisk bevismateriale, der vil gælde fuldt ud fra august 2026[16], truffet foranstaltninger til både at bekæmpe **onlinekriminalitet og lette adgangen til digitalt bevismateriale for alle forbrydelser**. De vil blive suppleret med internationale instrumenter til udveksling af oplysninger og bevismateriale. Kommissionen vil snart foreslå, at **FN's nye konvention imod cyberkriminalitet** undertegnes og indgås.

For at følge op på anbefalingerne fra gruppen på højt plan[17] vil Kommissionen i første halvdel af 2025 fremlægge en **køreplan for de retlige og praktiske foranstaltninger**, som den foreslår, der træffes for at **sikre lovlig og effektiv adgang til oplysninger**. Som opfølgning på denne køreplan vil Kommissionen prioritere, at der foretages en vurdering af virkningen af **datalagringsreglerne** på EU-plan, og at der udarbejdes en **teknologikøreplan for kryptering** med henblik på at kortlægge og vurdere, hvilke teknologiske løsninger der vil gøre det muligt for retshåndhævende myndigheder at tilgå krypterede oplysninger på en lovlig måde og beskytte cybersikkerheden og de grundlæggende rettigheder.

Operationelt samarbejde

Kommissionen vil sammen med medlemsstaterne, EU-agenturer og -organer og partnerlande arbejde for at styrke det operationelle samarbejde, hvilket er afgørende for en mere effektiv tilgang til bekæmpelse af grænseoverskridende organiseret kriminalitet og terrorisme.

Den europæiske tværfaglige platform mod kriminalitetstrusler (EMPACT) har som den vigtigste EU-ramme for en fælles indsats mod grov og organiseret kriminalitet opnået betydelige operationelle resultater. Den næste EMPACT-cyklus 2026-2029 giver mulighed for at styrke denne ramme yderligere. For at bekæmpe de mest truende kriminelle netværk og

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:52019PC0070.
[15] Concluding report of the High-Level Group on access to data for effective law enforcement - 15/11/2024 (foreligger ikke på dansk), 4802e306-c364-4154-835b-e986a9a49281_en.
[16] Europa-Parlamentets og Rådets forordning (EU) 2023/1543 af 12. juli 2023 om europæiske editionskendelser og europæiske sikringskendelser om elektronisk bevismateriale i straffesager og om fuldbyrdelse af frihedsstraffe idømt som led i en straffesag (EUT L 191 af 28.7.2023).
[17] Rådets konklusioner om adgang til data med henblik på effektiv retshåndhævelse (12. december 2024), https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/da/pdf.

enkeltpersoner skal Unionen strømline og fokusere sin indsats på de mest presserende prioriteter, øge medlemsstaternes forpligtelser og sikre en effektiv anvendelse af ressourcerne.

Med henblik herpå vil Kommissionen samarbejde med Rådets formandskaber og medlemsstaterne om at **maksimere EMPACT's potentiale og tage fat på de vigtigste prioriteter for den næste EMPACT-cyklus 2026-2029**. På tværs af disse prioriterede områder er der behov for efterretninger om de mest truende kriminelle netværk, fælles efterforskning og operationelle taskforcer samt en stærk retlig reaktion, herunder en "følg pengene"-tilgang. Unionen er desuden nødt til at bekæmpe rekrutteringen til kriminelle netværk og kriminel infiltration og øge det tværgående og internationale samarbejde om retshåndhævelse og uddannelse på området.

Kommissionen vil også støtte andre former for **grænseoverskridende operationelt retshåndhævelsessamarbejde mellem medlemsstaterne og de associerede Schengenlande**. For at sikre et højt niveau af indre sikkerhed i Schengenområdet uden kontrol ved de indre grænser kræves der et tæt samarbejde og udveksling af oplysninger mellem medlemsstaternes retshåndhævende myndigheder. I dag står de retshåndhævende myndigheder stadig over for udfordringer, når de foretager overvågning eller træffer hasteforanstaltninger på tværs af grænserne[18], og bekæmpelse af hybride trusler kræver også et øget grænseoverskridende samarbejde. Der bør nedsættes en **gruppe på højt plan om det fremtidige operationelle retshåndhævelsessamarbejde** med henblik på at udforme en fælles strategisk vision.

En effektiv udveksling af oplysninger mellem retshåndhævende myndigheder er også afgørende for et effektivt grænseoverskridende samarbejde. Når **interoperabilitetsarkitekturen** er oprettet, vil den give de retshåndhævende myndigheder og Europol effektiv adgang til vigtige oplysninger. Samtidig bør EU og dets medlemsstater i samarbejde med eu-LISA og Europol prioritere bilateral og multilateral udveksling af oplysninger gennem den retlige og tekniske gennemførelse af **Prüm II-forordningen**[19]. Det vil muliggøre sikker elektronisk udveksling af fingeraftryk, DNA-profiler, oplysninger fra køretøjsregistre, ansigtsbilleder og oplysninger fra politiregistre gennem EU's routere. På nationalt plan skal medlemsstaterne gennemføre **direktivet om informationsudveksling**[20] og forbedre informationsudvekslingskanalerne med henblik på at fremme gnidningsløse grænseoverskridende informationsstrømme, samtidig med at det sikres, at disse kanaler integreres i systemerne på EU-plan såsom SIENA[21].

Et effektivt grænseoverskridende samarbejde forudsætter også, at der skabes en **fælles retshåndhævelseskultur i EU**. Fælles uddannelse, ekspertisecentre og mobilitetsprogrammer er afgørende for at nå dette mål. Kommissionen vil undersøge, hvordan EU bedst kan støtte uddannelsen af medlemsstaternes myndigheder med hjælp fra **Cepol** som EU's agentur for uddannelse inden for retshåndhævelse.

[18] Som anført i Kommissionens vurdering af medlemsstaternes gennemførelse af Rådets henstilling (EU) 2022/915 af 9. juni 2022 om operationelt retshåndhævelsessamarbejde (5909/25).

[19] Europa-Parlamentets og Rådets forordning (EU) 2024/982 af 13. marts 2024 om automatiseret søgning og udveksling af data med henblik på politisamarbejde, og om ændring af Rådets afgørelse 2008/615/RIA og 2008/616/RIA og Europa-Parlamentets og Rådets forordning (EU) 2018/1726, (EU) 2019/817 og (EU) 2019/818 (Prüm II-forordningen) (EUT L, 2024/982, 5.4.2024).

[20] Europa-Parlamentets og Rådets direktiv (EU) 2023/977 af 10. maj 2023 om udveksling af oplysninger mellem medlemsstaternes retshåndhævende myndigheder og om ophævelse af Rådets rammeafgørelse 2006/960/RIA (EUT L 134 af 22.5.2023, s. 1).

[21] Netværksprogram til sikker informationsudveksling.

Øget grænsesikkerhed

Øget modstandsdygtighed og sikkerhed ved de ydre grænser er afgørende for at imødegå hybride trusler såsom anvendelse af migration som våben, forhindre trusselsaktører og varer i at komme ind i EU og effektivt bekæmpe grænseoverskridende kriminalitet og terrorisme. **Schengeninformationssystemet (SIS) skal efter planen forbedres** i 2026 for at gøre det muligt for medlemsstaterne at indlæse indberetninger om tredjelandsstatsborgere, der er involveret i terrorisme, herunder fremmedkrigere, og i anden alvorlig kriminalitet på grundlag af oplysninger, som tredjelande deler med Europol.

Forbedret **interoperabilitet** mellem de store EU-informationssystemer vil give medlemsstaterne væsentlige oplysninger om personer fra tredjelande, der passerer eller har til hensigt at passere de ydre grænser, hvilket vil hjælpe myndighederne med at vurdere, om betingelserne for at tillade indrejse på medlemsstaternes område, er opfyldt[22]. Kommissionen vil fortsat arbejde tæt sammen med medlemsstaterne og eu-LISA om en hurtig gennemførelse af disse systemer, navnlig **ind- og udrejsesystemet (EES), det europæiske system vedrørende rejsetilladelse (ETIAS) og det reviderede visuminformationssystem (VIS)**, for at sikre, at de fungerer gnidningsløst og giver sikkerhedsmæssige fordele.

For yderligere at øge grænsesikkerheden og styrke EU's samarbejde i lyset af nye trusler **vil Kommissionen fremsætte forslag til en styrkelse af Frontex**. Der bør over tid ske en tredobling af den europæiske grænse- og kystvagts størrelse til 30 000 medarbejdere. Agenturet bør få stillet avanceret teknologi til rådighed med henblik på overvågning og situationsbevidsthed, herunder efterretninger, der er relevante for integreret europæisk grænseforvaltning, og få adgang til robuste statslige EU-jordobservationstjenester til grænsekontrol, der skal indsættes senest i 2027. Dette bør yderligere styrke agenturets evne til at opdage, forebygge og bekæmpe grænseoverskridende kriminalitet ved de ydre grænser og til at yde øget støtte til medlemsstaterne i forbindelse med gennemførelsen af tilbagesendelser, navnlig i tilfælde af tredjelandsstatsborgere, der udgør en sikkerhedsrisiko.

Dokument- og identitetssvig fremmer smugling af migranter, menneskehandel, hemmelige kriminelle bevægelser og handel med ulovlige varer. **Multiidentitetsdetektoren (MID)**[23] vil, når den bliver operationel, forbedre de nationale myndigheders evne til at identificere personer med flere identiteter og bekæmpe identitetssvig. Kommissionen vil undersøge, hvordan sikkerheden i forbindelse med rejse- og opholdsdokumenter, der udstedes til EU-borgere og tredjelandsstatsborgere, kan forbedres Derudover vil Kommissionen vurdere, hvordan de europæiske digitale identitetstegnebøger, der inden udgangen af 2026 skal indføres i medfør af den europæiske ramme for digital identitet, kan bidrage til at forbedre rejsedokumenters sikkerhed og forbedre identitetskontrollen. Dette vil supplere forslagene om digital rejselegitimation og EU's digitale rejseapp[24].

Rejseoplysninger er afgørende for, at myndighederne kan kortlægge og efterforske kriminelles, terroristers og andre sikkerhedsmæssigt truende aktørers bevægelser. Selv om der

[22] Ind- og udrejsesystemet (EES) vil navnlig sætte medlemsstaterne i stand til at identificere tredjelandsstatsborgere ved Schengenområdets ydre grænser og registrere deres ind- og udrejser, hvilket vil gøre det muligt systematisk at identificere personer, hvis tilladelse til ophold er udløbet. Inden en tredjelandsstatsborger ankommer til de ydre grænser, vil det europæiske system vedrørende rejseinformation og rejsetilladelse (ETIAS) og visuminformationssystemet (VIS) give medlemsstaterne mulighed for på forhånd at vurdere, om en tredjelandsstatsborgers tilstedeværelse på EU's område vil udgøre en sikkerhedsrisiko.

[23] MID er en af de interoperabilitetskomponenter, der blev indført ved forordning (EU) 2019/818 og (EU) 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/da/ip_24_5047.

findes en EU-ramme for oplysninger om passagerer på kommercielle flyvninger[25], er behandlingen af oplysninger om passagerer, der benytter andre transportformer, med henblik på retshåndhævelse fragmenteret. Derfor kan kriminelle og terrorister udnytte forskellige transportformer til ulovlige aktiviteter, uden at det opdages. Kommissionen vil samarbejde med medlemsstaterne og transportsektoren om at **styrke rammen for rejseinformation** ved at se nærmere på en EU-ordning, der kræver, at operatører af private flyvninger indsamler og overfører passageroplysninger, evaluere reglerne for behandling af passagerlisteoplysninger og vurdere, hvordan behandlingen af oplysninger om passagerer på sørejser kan strømlines. Med hensyn til vejtransport vil Kommissionen vurdere en udvidet anvendelse af **systemer til automatisk nummerpladegenkendelse (ANPR)** og øge mulighederne for synergier med SIS.

En strategi baseret på fremsynethed, innovation og kapacitet

Kommissionen vil udvikle **en omfattende fremtidsorienteret strategi for den indre sikkerhed på EU-plan** på grundlag af bedste praksis, der er fastlagt på nationalt plan. Strategien vil støtte den politiske beslutningstagning og sikre, at investeringer ledes i retning af relevant EU-finansieret sikkerhedsforskning og -innovation.

Forskning og innovation spiller en afgørende rolle for den indre sikkerhed, idet det er ved hjælp heraf, at der findes løsninger til at imødegå nye trusler, herunder som følge af teknologisk misbrug[26]. EU skal gennem EU-finansieret sikkerhedsforskning og -innovation[27] fortsætte med at investere i udvikling af innovative værktøjer og løsninger til håndtering af sikkerhedstrusler, samtidig med at EU's regler og grundlæggende rettigheder overholdes. Kommissionen bør støtte overgangen fra forskning til udbredelse af resultaterne heraf for at sikre en effektiv anvendelse af disse moderne kapaciteter, idet hovedvægten lægges på **moderne teknologier** såsom kunstig intelligens. Denne tilgang bør omfatte uddannelse med henblik på at forbedre de retshåndhævende og de retslige myndigheders anvendelse af AI-systemer og andre tekniske kapaciteter. Derudover bør potentialet ved teknologier med dobbelt anvendelse, hvor det er relevant, udnyttes i begge retninger (fra civil anvendelse til forsvarsmæssig anvendelse og fra forsvarsmæssig anvendelse til civil anvendelse)[28].

Det Europæiske Innovationscenter for Indre Sikkerhed[29], der er et netværk af innovationslaboratorier, der sikrer de seneste innovationsopdateringer og effektive løsninger til støtte for det arbejde, der udføres af aktører inden for indre sikkerhed i EU og medlemsstaterne, vil bidrage til at integrere forskning i praksis og politik. Hvis Europol skal gøres mere effektivt, kræves der en styrkelse af Europols værktøjsregister (ETR), så det kan finde frem til, udvikle, i fællesskab indkøbe og anvende avancerede teknologier operationelt. Kommissionen vil desuden oprette et **center for sikkerhedsforskning og -innovation** på Det Fælles Forskningscenter og samle forskere for at afkorte cyklussen fra forskningsresultater til innovation, udvikling og vellykket gennemførelse, samtidig med at omkostningerne til udvikling, afprøvning og validering reduceres.

[25] Rammen for passagerlisteoplysninger (PNR) og forhåndsoplysninger om passagerer (API), der er fastsat ved direktiv (EU) 2016/681 ("PNR-direktivet") og forordning (EU) 2025/12 og (EU) 2025/13 ("API-forordningerne").
[26] Se Kommissionens Fælles Forskningscenters rapport "Emerging risks and opportunities for EU internal security stemming from new technologies" (foreligger ikke på dansk), https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025 (foreligger ikke på dansk), https://data.europa.eu/doi/10.2837/0004501.
[28] Som fastsat i Niinistö-rapporten.
[29] Det Europæiske Innovationscenter for Indre Sikkerhed | Europol.

Vores **europæiske forskningsrum** er i sagens natur samarbejdsbaseret og dermed sårbar over for udenlandsk indblanding og desinformation. Efter vedtagelsen af Rådets henstilling om forskningssikkerhed[30] er Kommissionen og medlemsstaterne ved at træffe foranstaltninger med henblik på at styrke relevante aktører, bl.a. ved at oprette et ekspertisecenter for forskningssikkerhed.

Vigtige tiltag

Kommissionen vil vedtage:

- **et lovgivningsforslag om at omdanne Europol til en reelt operationel retshåndhævende myndighed i 2026**
- **et lovgivningsforslag om styrkelse af Eurojust i 2026**
- **et lovgivningsforslag om styrkelse af Frontex' rolle og opgaver i 2026**
- **et lovgivningsforslag om oprettelse af et europæisk kritisk kommunikationssystem i 2026**

Kommissionen vil:

- **i 2025 fremlægge en køreplan, der beskriver vejen frem med hensyn til lovlig og effektiv adgang til oplysninger med henblik på retshåndhævelse**
- **i 2025 udarbejde en konsekvensanalyse med henblik på at ajourføre reglerne om lagring af oplysninger på EU-plan, hvis det er relevant**
- **i 2026 fremlægge en teknologikøreplan for kryptering med henblik på at finde og vurdere teknologiske løsninger, der giver de retshåndhævende myndigheder lovlig adgang til oplysninger**
- **arbejde hen imod at oprette en gruppe på højt plan for at styrke det operationelle retshåndhævelsessamarbejde**
- **i 2026 oprette et center for sikkerhedsforskning og -innovation på Det Fælles Forskningscenter**

Kommissionen vil i samarbejde med medlemsstaterne og relevante EU-agenturer:

- **styrke EMPACT-arkitekturen**
- **arbejde hen imod en hurtig udrulning af interoperabilitetsarkitekturen og gennemførelse af Prüm II-forordningen**
- **styrke rammen for rejseinformation**

Medlemsstaterne opfordres til at:

- **omsætte og gennemføre direktivet om udveksling af oplysninger fuldt ud**

4. Modstandsdygtighed over for hybride trusler og andre fjendtlige handlinger

Vi vil opbygge modstandsdygtighed over for hybride trusler ved at forbedre beskyttelsen af kritisk infrastruktur, styrke cybersikkerheden, sikre transportknudepunkter og havne og bekæmpe onlinetrusler.

Hyppigheden og sofistikeringsgraden af fjendtlige handlinger, der underminerer EU's sikkerhed, er steget, og ondsindede aktører har udvidet deres arsenal betydeligt. De hybride kampagner mod EU, dets medlemsstater og partnere er blevet intensiveret med sabotagehandlinger rettet mod kritisk infrastruktur, brandstiftelse, cyberangreb, indblanding i valg, udenlandsk informationsmanipulation og indblanding, herunder desinformation, og

[30] EUT C/2024/3510, 30.5.2024.

anvendelse af migration som våben. På grund af den politiske og operationelle rolle, som Unionens institutioner, organer, kontorer og agenturer ("EU-enheder") spiller, og arten af de oplysninger, de håndterer, skånes de ikke.

EU skal **øge sin modstandsdygtighed**, udnytte de nuværende værktøjer effektivt og udvikle nye metoder til at imødegå disse nye trusler fra statslige og ikkestatslige aktører, både nu og i fremtiden.

Kritisk infrastruktur

Trusler mod **kritisk infrastruktur**, herunder hybride trusler såsom sabotage og ondsindede cyberaktiviteter, er et stort problem, navnlig for den infrastruktur, der forbinder medlemsstaterne – det være sig energisamkøringsforbindelser eller grænseoverskridende kommunikationskabler samt transport. Siden indledningen af Ruslands angrebskrig mod Ukraine er sabotagehandlingerne mod kritisk infrastruktur steget, navnlig i 2024, hvilket har påvirket mange medlemsstater. Samarbejdet mellem retshåndhævende myndigheder, sikkerheds- og cybersikkerhedstjenester, militæret og civilbeskyttelsestjenester samt private operatører er afgørende for at foregribe, opdage, forebygge og reagere effektivt på sådanne handlinger.

Det er bydende nødvendigt at mindske kritiske enheders sårbarhed og styrke deres modstandsdygtighed for at sikre uafbrudt levering af væsentlige tjenester, der er afgørende for økonomien og samfundet. En rettidig og korrekt gennemførelse i alle medlemsstaterne af direktivet om **kritiske enheders modstandsdygtighed**[31] og **direktivet om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2)**[32] er derfor afgørende med henblik herpå.

For at sikre hurtige fremskridt vil Kommissionen i samarbejde med **Gruppen for Kritiske Enheders Modstandsdygtighed og NIS-samarbejdsgruppen** støtte medlemsstaterne med henblik på at indkredse kritiske enheder[33] og udveksle god praksis om nationale strategier og risikovurderinger for så vidt angår væsentlige tjenester. Hvis der skulle ske afbrydelser af kritisk infrastruktur med betydelig grænseoverskridende virkning, vil der inden for rammerne af **EU-planen for kritisk infrastruktur** blive koordineret en reaktion på EU-plan. Kommissionen opfordrer Rådet til hurtigt at vedtage **EU's cyberplan**, som yderligere vil styrke koordineringen i forbindelse med krisestyring og fremme et tættere samarbejde mellem myndighederne om fysisk og digital modstandsdygtighed Efter vellykkede stresstest i energisektoren i 2023 vil Kommissionen fremme **frivillige stresstest** i andre nøglesektorer med henblik på den indre sikkerhed. Desuden vil Kommissionen til støtte for medlemsstaternes risikovurderinger give **et overblik på EU-plan over grænseoverskridende og tværsektorielle risici** for væsentlige tjenester, som skal danne grundlag for en omfattende risikovurdering på EU-plan. Sideløbende med strategien for en beredskabsunion vil Kommissionen sammen med medlemsstaterne undersøge, om der er andre sektorer og tjenester, der ikke er omfattet af den nuværende lovgivning, og hvor der måske skal sættes ind.

[31] 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.

[32] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet).

[33] De sektorer, der er omfattet af direktivet, er energi, transport, bankvæsen, finansmarkedsinfrastruktur, sundhedsvæsenet, drikkevand, spildevand, digital infrastruktur, offentlig forvaltning, rumfart samt fødevareproduktion, -forarbejdning og -distribution.

Inden for rammerne af **EU-NATO-taskforcen om kritisk infrastrukturs modstandsdygtighed** er der skabt et godt samarbejde om udveksling af bedste praksis og øget modstandsdygtighed i energisektoren, transportsektoren, sektoren for digital infrastruktur og rumsektoren. Dette arbejde vil fortsætte inden for rammerne af **den strukturerede dialog mellem EU og NATO om modstandsdygtighed**. Ved hjælp af **EU's værktøjer til at imødegå hybride trusler** ydes der en solid støtte til medlemsstaterne og partnere, når de skal forberede sig på og imødegå hybride trusler. **EU-hybridberedskabshold**[34] yder efter anmodning skræddersyet kortsigtet bistand til medlemsstaterne og forskellige EU-missioner og -partnere. Kommissionen vil desuden fremme EU's samarbejde om bekæmpelse af sabotage gennem ekspertaktiviteter[35], herunder et **særligt fælles arbejdsprogram** for eksperterne for at strømline informationsudvekslingen og kortlægge modforanstaltninger.

De hændelser, der har påvirket **undersøiske kabler** i Europa, har tydeliggjort behovet for stærkere foranstaltninger og klarere reaktioner. Som skitseret i **EU's handlingsplan for kabelsikkerhed**[36] vil Kommissionen sammen med den højtstående repræsentant samarbejde med medlemsstaterne, EU-agenturer og partnere som NATO om at forebygge, opdage, reagere på og afværge trusler mod undersøiske kabler. For at udarbejde et integreret situationsbillede af truslerne vil Kommissionen samarbejde med medlemsstaterne om på frivillig basis at udvikle og anvende en integreret overvågningsmekanisme for undersøiske kabler pr. havområde, begyndende med et nordisk/baltisk regionalt knudepunkt.

Cybersikkerhed

Den vedvarende karakter af de **ondsindede cyberaktiviteter**, som ofte er en del af en bredere vifte af flerdimensionelle og hybride trusler, kræver fortsat opmærksomhed og handling på europæisk plan. I de seneste år har Unionen vedtaget en række cybersikkerhedsforskrifter, der styrker cyberrobustheden i de NIS 2-enheder, der opererer i EU's kritiske sektorer, samt i EU-enheder[37], forbedrer sikkerheden ved digitale produkter (forordningen om cyberrobusthed) og skaber en ramme for støtte til beredskab og reaktion på hændelser (forordningen om cybersolidaritet). I januar 2025 vedtog Kommissionen en **europæisk handlingsplan for cybersikkerhed for hospitaler og sundhedstjenesteydere**[38] med henblik på at forbedre mulighederne for at opdage trusler og styrke beredskabet og kriseresponsen. Det er afgørende, at den gennemføres fuldt ud. For at imødegå nye trusler og hændelser er vi samtidig nødt til at intensivere vores indsats, navnlig hvad angår informationsudveksling, sikkerheden i forsyningskæder, ransomware og cyberangreb samt teknologisk suverænitet.

Desuden kræver gennemførelsen, at den nuværende mangel på 299 000 personer med cybersikkerhedsfærdigheder afhjælpes. Kommissionen vil inden for rammerne af færdighedsunionen[39] samarbejde med medlemsstaterne om at udvide arbejdsstyrken inden for cybersikkerhed, navnlig ved at anvende det nye akademi for cybersikkerhedskompetencer. Den strategiske plan for STEM-uddannelser[40] bidrager til at forbedre talentpipelinen og Europas

[34] EU's strategiske kompas for sikkerhed og forsvar 2022, s. 22,
[35] EU's sikkerhedsrådgivere, Det Europæiske Netværk for Ammunitionsrydning (EEODN), Atlasnetværket, EU's højrisikosikkerhedsnetværk (EU HRSN), den rådgivende gruppe om CBRN-sikkerhed og Gruppen for Kritiske Enheders Modstandsdygtighed (CERG).
[36] JOIN(2025) 9 final.
[37] Europa-Parlamentets og Rådets forordning (EU, Euratom) 2023/2841 af 13. december 2023 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i Unionens institutioner, organer, kontorer og agenturer (EUT L, 2023/2841, 18.12.2023).
[38] https://digital-strategy.ec.europa.eu/da/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM(2025) 90 final.
[40] COM(2025) 89 final.

reaktion på behovene på arbejdsmarkedet for personer med færdigheder inden for cybersikkerhed.

EU vil sideløbende med at øge sin modstandsdygtighed fortsat gøre fuld brug af rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter (**den cyberdiplomatiske værktøjskasse**) for at forebygge, afværge og reagere på cybertrusler fra statslige og ikkestatslige aktører.

Sikring af forsyningskæderne inden for informations- og kommunikationsteknologi

EU-værktøjskassen til 5G-cybersikkerhed udgør den relevante ramme for beskyttelse af 5G-net, men gennemføres i øjeblikket ikke i tilstrækkelig grad af medlemsstaterne. Der er fortsat uacceptable sikkerhedsrisici, navnlig med hensyn til udskiftning af højrisikoudbydere. En harmoniseret tilgang til sikkerheden i IKT-forsyningskæden kan afhjælpe den nuværende fragmentering på det indre marked som følge af forskellige tilgange på nationalt plan, forhindre kritisk afhængighed og mindske den risiko for vores IKT-forsyningskæder, som højrisikoleverandører medfører, og dermed sikre vores kritiske infrastruktur.

I overensstemmelse med denne tilgang vil Kommissionen i den kommende **revision af forordningen om cybersikkerhed** se mere bredt på sikkerheden og modstandsdygtigheden i forbindelse med IKT-forsyningskæder og -infrastruktur. Kommissionen vil desuden fremsætte forslag til at forbedre **den europæiske ramme for cybersikkerhedscertificering** for at sikre, at fremtidige certificeringsordninger kan vedtages rettidigt og imødekomme politiske behov.

På grundlag af eksisterende eller igangværende sektorspecifikke vurderinger[41] vil Kommissionen sammen med medlemsstaterne udforme en **strategisk plan for koordinerede cybersikkerhedsrisikovurderinger**.

Cloud- og telekommunikationstjenester er blevet en fast bestanddel af forsyningskæderne i forbindelse med kritisk infrastruktur, virksomheder og offentlige myndigheder. Kommissionen vil træffe foranstaltninger til at tilskynde kritiske enheder til at vælge **cloud- og telekommunikationstjenester, der tilbyder et passende cybersikkerhedsniveau**, under hensyntagen til ikke blot tekniske risici, men også strategiske risici og afhængighedsforhold.

Ransomware og cyberangreb

En vedvarende større udfordring for cybersikkerheden i EU og på verdensplan er **ransomware**. I en rapport anslås det, at de årlige omkostninger på verdensplan vil beløbe sig til mere end 250 mia. EUR i 2031[42]. Både **NIS 2-direktivet** og **forordningen om cyberrobusthed** vil i væsentlig grad forbedre enhedernes sikkerhedsstatus og gøre det dyrere for ransomwarenetværk at udføre deres angreb. Kommissionen vil desuden arbejde tæt sammen med medlemsstaterne for at sikre, at flere ransomwareangreb, navnlig avancerede vedvarende trusler, og betaling af løsepenge indberettes til de retshåndhævende myndigheder for derved at lette efterforskningen.

For at forebygge og standse cyberangreb er EU nødt til at styrke informationsudvekslingen mellem retshåndhævende myndigheder, cybersikkerhedsmyndigheder og -enheder samt private parter inden for rammerne af Europol og EU's Agentur for Cybersikkerhed (ENISA).

Europol og Eurojust bør fortsat bygge videre på de resultater, de har opnået med hensyn til at bekæmpe ransomwareoperationer og støtte retshåndhævelsessamarbejdet. Med henblik herpå bør de retshåndhævende myndigheder maksimere anvendelsen af samarbejdsmekanismer, herunder **Europols internationale ransomwareberedskabsmodel** og **det internationale**

[41] F.eks. 5G-net, telekommunikation, elektricitet, vedvarende energi og opkoblede køretøjer.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

initiativ til bekæmpelse af ransomware (CRI)[43], og ENISA og Europol bør samarbejde om at udvide registret over dekrypteringsværktøjer til ransomwaretyper[44].

Teknologisk suverænitet

Cybersikkerhed og teknologisk suverænitet er tæt forbundne, og teknologisk afhængighed skal anses for at være en prioritet. Unionen skal **styre udviklingen og udbredelsen af nye teknologier**, og Kommissionen skal arbejde for at **forbedre kapaciteten inden for strategiske teknologier** såsom kunstig intelligens, kvanteteknologi, avanceret konnektivitet, cloud, edge og tingenes internet[45] gennem kommende initiativer såsom handlingsplanen for et AI-kontinent og strategien for kvanteteknologi[46]. Kommissionen vil fortsat støtte en rettidig udrulning af de senest tilgængelige internationalt aftalte **internetprotokoller**, som er afgørende for at opretholde et skalerbart og effektivt internet med et øget cybersikkerhedsniveau. Der er også behov for yderligere tiltag for at imødegå **frekvensrelaterede udfordringer**, f.eks. i forbindelse med GNSS-spoofing, jamming, risici i forsyningskæden og afhængighed, såsom anvendelse af kvantesensingteknologier og undersøgelse af udviklingen af kapacitet til radiofrekvensovervågning.

Anvendelsen af **postkvante-kryptografiløsninger** (PQC) vil være afgørende for at sikre følsom kommunikation og data i hvile og for at beskytte digitale identiteter i den nye kvantetidsalder. På grundlag af henstillingen fra 2024 om en koordineret køreplan for gennemførelse af omstillingen til PQC[47] samarbejder Kommissionen med medlemsstaterne om at fremme denne omstilling. I den forbindelse bør medlemsstaterne indkredse højrisikosituationer i forbindelse med kritiske enheder og sørge for kvantesikker kryptering for disse højrisikosituationer så hurtigt som muligt og senest ved udgangen af 2030. Kommissionen arbejder også sammen med medlemsstaterne og Den Europæiske Rumorganisation (ESA) om at udvikle og udrulle **den europæiske kvantekommunikationsinfrastruktur (EuroQCI)**[48] baseret på kvantenøglefordeling (QKD) som led i **IRIS²**, EU's program for sikker konnektivitet. Begge initiativer vil i sidste ende gøre det muligt for enheder at overføre oplysninger og lagre dem sikkert.

Kvanteteknologier vil også spille en central rolle i forbindelse med sikkerhedsapplikationer: Som led i **strategien for kvanteteknologi** vil der blive udarbejdet **en køreplan for kvantesensing i sikkerhedsapplikationer**. På samme måde arbejder Kommissionen på at kvantesikre sine sikkerhedskritiske systemer, herunder sine klassificerede IT-systemer.

En erhvervsvenlig ramme for cybersikkerhed

Den kommende revision af forordningen om cybersikkerhed giver mulighed for at **forenkle EU's cybersikkerhedslovgivning** i overensstemmelse med konkurrenceevnekompasset. Kommissionen vil arbejde tæt sammen med medlemsstaterne for at sikre en hurtig, sammenhængende og erhvervsvenlig gennemførelse af den horisontale ramme for cybersikkerhed, der er fastsat i NIS 2-direktivet, forordningen om cyberrobusthed og forordningen om cybersolidaritet, fremme enkelhed og sammenhæng og undgå fragmentering eller overlapning af cybersikkerhedsregler i EU-retten og national lovgivning.

[43] https://counter-ransomware.org/.
[44] Tilgængelig via No More Ransom-projektet, https://www.nomoreransom.org/da/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] F.eks. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, Quantum Flagship Webside for Quantum Flagship | Quantum Flagship, 3C-nettet (COM(2024) 81 final) og EU's handlingsplan for kabelsikkerhed (JOIN(2025) 9 final).
[47] Henstilling om en koordineret gennemførelseskøreplan for overgangen til kvantesikker kryptografi | Europas digitale fremtid i støbeskeen.
[48] https://digital-strategy.ec.europa.eu/da/policies/european-quantum-communication-infrastructure-euroqci.

For at muliggøre sikker adgang til onlinetjenester og styrke den digitale sikkerhed i hele EU vil den **europæiske ramme for digital identitet** sikre alle EU-borgere og andre, der har bopæl i EU, pålidelige digitale identitetstegnebøger inden udgangen af 2026. Den kommende **europæiske virksomhedstegnebog** vil gøre samspillet mellem virksomheder og offentlige forvaltninger lettere og mere sikkert. Begge er forudsætninger for, at det datadrevne indre marked kan fungere sikkert og mere effektivt med værktøjer såsom den fælles digitale portal, e-fakturering, e-indkøb og det digitale produktpas.

Onlinesikkerhed

Nogle af de mest alvorlige hybride trusler, der bringer EU-borgernes sikkerhed i fare, og som er rettet mod EU's demokratiske sfære, forekommer online. Disse trusler omfatter ulovlige aktiviteter og ulovligt indhold online, informationsmanipulation ved kunstig forstærkning, vildledende information samt udenlandsk informationsmanipulation og indblanding.

En streng håndhævelse af **forordningen om digitale tjenester** er afgørende for at sikre et sikkert og tilgængeligt onlinemiljø med ansvarlige aktører, som også er modstandsdygtigt over for hybride trusler. Forordningen om digitale tjenester forpligter udbydere af meget store onlineplatforme og af meget store onlinesøgemaskiner til at foretage risikovurderinger og træffe afbødende foranstaltninger i forbindelse med systemiske risici som følge af den måde, hvorpå deres tjenester er udformet og fungerer eller anvendes, bl.a. i form af negative konsekvenser for samfundsdebatten og afviklingen af valg samt for den offentlige sikkerhed såsom vidtrækkende indblanding fra ondsindede udenlandske statslige aktørers side, f.eks. i afviklingen af valg. Det er vigtigt at uddanne medlemsstaternes kompetente myndigheder i brugen af retlige værktøjer til omgående at fjerne ulovligt onlineindhold, navnlig når det kommer til kønsbestemt cybervold. Forordningen om digitale tjenester indeholder bestemmelser om en kriseresponsmekanisme, som kan aktiveres, når ekstraordinære omstændigheder medfører en alvorlig trussel mod den offentlige sikkerhed eller folkesundheden i Unionen eller i væsentlige dele heraf. Som supplement til denne mekanisme har Kommissionen og de nationale kompetente myndigheder, der er udpeget som koordinatorer for digitale tjenester, også udviklet en frivillig **ramme for reaktion på hændelser i forbindelse med forordningen om digitale tjenester**. Koordinatorerne for digitale tjenester har også truffet foranstaltninger for at bidrage til beskyttelsen af integriteten af valg, f.eks. ved at tilrettelægge rundbordsdrøftelser og stresstest[49]. Forordningen om digitale tjenester udgør sammen med forordningen om politisk reklame[50] tiltag på et af flere indsatsområder, der er knyttet til beskyttelsen af demokratiet og integriteten af demokratiske processer, som er sårbare over for fjendtlige aktørers indblanding, bl.a. via digitale værktøjer og på sociale medier.

Gennemførelsen af værktøjskassen vedrørende **udenlandsk informationsmanipulation og indblanding** er en anden vigtig komponent, der giver mulighed for central støtte på EU-plan. Støtte til digital kunnen og mediekendskab og kritisk tænkning er også afgørende for disse bestræbelser[51].

Bekæmpelse af brugen af migration som våben

Rusland har med hjælp og afgørende støtte fra Belarus bevidst brugt migration som våben og ulovligt fremmet migrationsstrømmene hen imod EU's ydre grænser med det formål at destabilisere vores samfund og undergrave sammenholdet i Den Europæiske Union. Dette bringer ikke alene medlemsstaternes nationale sikkerhed og suverænitet i fare, men også

[49] DSA Elections Toolkit for Digital Services Coordinators 2025 (foreligger ikke på dansk) (https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators).
[50] Europa-Parlamentets og Rådets forordning (EU) 2024/900 af 13. marts 2024 om gennemsigtighed og målretning i forbindelse med politisk reklame (EUT L, 2024/900, 20.3.2024).
[51] Handlingsplanen for digital uddannelse (2021-2027) – Det europæiske uddannelsesområde.

Schengenområdets sikkerhed og integritet og sikkerheden i Unionen som helhed. Det Europæiske Råd understregede i sine konklusioner fra oktober 2024, at hverken Rusland og Belarus eller noget andet land må få lov til at misbruge vores værdier, herunder retten til asyl, og undergrave vores demokrati.

Som anført i Kommissionens meddelelse fra 2024 om brugen af migration som våben har Unionen foruden stærk politisk støtte truffet finansielle, operationelle og diplomatiske foranstaltninger, herunder samarbejde med oprindelses- og transitlande, for effektivt at bekæmpe disse trusler[52]. Denne reaktion indebærer anvendelse af den nye ramme, som Rådet har fastlagt, til gennem indefrysning af aktiver og rejseforbud at sanktionere enkeltpersoner og organisationer, der er indblandet i handlinger og politikker som f.eks. Ruslands brug af migration som våben[53]. EU vil fortsat anvende denne ramme, når det er nødvendigt, og hjælpe medlemsstaterne med at bekæmpe denne trussel.

Transportsikkerhed

Søhavne, lufthavne og landinfrastruktur er vigtige ind- og udrejsesteder. De spiller en afgørende rolle i EU's økonomi og samfund og har stor betydning for militær mobilitet. Disse transportknudepunkter og -midler er dog også oplagte mål for eksterne trusler og kriminelle aktiviteter. Nylige hændelser, herunder brud på luftfartssikkerheden og angreb på jernbaneinfrastruktur, fremhæver de alvorlige risici. **Transportvirksomheder** kan være både mål og instrumenter for ondsindede aktører. EU's eksisterende retlige instrumenter har forbedret luftfartssikkerheden[54], men det høje trusselsniveau inden for civil luftfart kræver en metode til at forudsige hændelser og hurtigt at konsultere de relevante medlemsstater. Kommissionen vil samarbejde med medlemsstaterne om at ændre den eksisterende gennemførelseslovgivning på luftfartssikkerhedsområdet med henblik på udveksling af klassificerede informationer om **luftfartssikkerhedsrelaterede hændelser**. Desuden vil Kommissionen overveje **lovgivningsmæssige foranstaltninger** for at imødegå nye trusler såsom **luftfragtrelaterede hændelser** og styrke luftfartssikkerhedsnormerne. Dette vil også indebære en styrkelse af **lovgivningen om luftfartssikkerhed (AVSEC)** for at muliggøre øjeblikkelige beredskabsforanstaltninger, samtidig med at "one-stop security"-området i EU's lufthavne opretholdes.

I forbindelse med udviklingen af den kommende **EU-havnestrategi**, der bygger på **EU's havnealliance**, vil Kommissionen undersøge, hvordan lovgivningen om maritim sikkerhed kan styrkes yderligere for effektivt at imødegå nye trusler, sikre havne og forbedre sikkerheden i EU's forsyningskæde. Med henblik herpå vil Kommissionen sikre en solid gennemførelse heraf og arbejde på at harmonisere national praksis og styrke baggrundskontrollen i havne. Ud over de sikkerhedsprotokoller, der er fastlagt for luftfragt, vil Kommissionen samarbejde med medlemsstaterne og den private sektor om at udvide disse protokoller med henblik på at sikre søtransportkæderne.

Den foreslåede EU-toldmyndighed vil analysere og vurdere risici baseret på **toldoplysninger** vedrørende varer, der indføres i, udføres af eller er i transit gennem EU, for at hjælpe medlemsstaterne med at forhindre, at ondsindede aktører udnytter internationale forsyningskæder. I overensstemmelse med EU-strategien for maritim sikkerhed[55] vil den kommende **europæiske havpagt** spille en central rolle med hensyn til at øge den maritime

[52] COM(2024) 570 final.
[53] Rådets forordning (EU) 2024/2642 af 8. oktober 2024 om restriktive foranstaltninger på baggrund af Ruslands destabiliserende aktiviteter (T/8744/2024/INIT, EUT L, 2024/2642, 9.10.2024).
[54] Europa-Parlamentets og Rådets forordning (EF) nr. 300/2008 af 11. marts 2008 om fælles bestemmelser om sikkerhed (security) inden for civil luftfart (EUT L 97 af 9.4.2008, s. 72).
[55] JOIN(2023) 8 final.

sikkerhed i havområderne omkring og uden for EU, bl.a. ved at tilskynde til opskalering af maritime operationer og øvelser med flere formål.

Forsyningskæders modstandsdygtighed

Europa er nødt til at blive mindre afhængig af teknologier fra tredjelande, da dette kan føre til afhængigheds- og sikkerhedsrisici. Kommissionen agter at mindske afhængigheden af enkelte udenlandske leverandører, nedbringe de risici for vores forsyningskæder, der er forbundet med højrisikoleverandører, og sikre kritisk infrastruktur og industriel kapacitet på EU's område som fastsat i **konkurrenceevnekompasset**[56]og **aftalen om ren industri**[57]. Kommissionen vil fremme en **industripolitik for indre sikkerhed** ved at samarbejde med EU's industrier inden for nøglesektorer (f.eks. transportknudepunkter og kritisk infrastruktur) for at udvikle sikkerhedsløsninger såsom detektionsudstyr, biometriske teknologier og droner med indbygget sikkerhed. Som led i **revisionen af EU's udbudsregler** vil Kommissionen vurdere, om sikkerhedshensynene i direktivet fra 2009 om udbud på forsvars- og sikkerhedsområdet[58] er tilstrækkelige til at imødekomme behovene inden for retshåndhævelse og kritiske enheders modstandsdygtighed.

Kommissionen vil støtte medlemsstaterne i forbindelse med **screening af udenlandske direkte investeringer (FDI)** og indkøb af udstyr til logistikknudepunkter, så det sikres, at kritisk infrastruktur og teknologi forbliver sikre.

Når **forordningen om nødsituationer for det indre marked og det indre markeds modstandsdygtighed (IMERA)** begynder at finde anvendelse, vil EU bedre være i stand til at håndtere kriser, der forstyrrer kritiske forsyningskæder og den frie bevægelighed for varer, tjenesteydelser og personer. Forordningen vil muliggøre hurtig krisekoordinering og kortlægning af kriserelevante varer og tjenesteydelser og indeholde en værktøjskasse til sikring af deres tilgængelighed. Desuden vil Kommissionen i tæt samarbejde med medlemsstaterne foreslå, at der oprettes **en varslingsmekanisme for transport- og forsyningskædesikkerhed, der omfatter flere instanser**, for at garantere en sikker og rettidig udveksling af relevante oplysninger, som er nødvendige for at foregribe og imødegå trusler.

Med gennemførelsen af forordningen om kritiske råstoffer og forordningen om nettonulindustri vil en øget anvendelse af kriterier for bæredygtighed, modstandsdygtighed og europæisk præference i EU's offentlige udbud desuden fremme udviklingen af pionermarkeder. Styrkede handelsforbindelser, f.eks. gennem partnerskaber om råstoffer og om ren handel og investering, vil bidrage til at diversificere forsyningskæderne.

Modstandsdygtighed og beredskab over for kemiske, biologiske, radiologiske og nukleare trusler

Ruslands angrebskrig mod Ukraine har øget risikoen for **kemiske, biologiske, radiologiske og nukleare trusler (CBRN-trusler)**. For at forhindre potentiel erhvervelse af CBRN-materialer og anvendelse af dem som våben vil Kommissionen støtte medlemsstaterne og partnerlandene gennem målrettet uddannelse og målrettede øvelser. Kommissionen vil inden for rammerne af en ny **handlingsplan for CBRN-beredskab og -indsats** også styrke beredskabs- og indsatskapaciteten på dette område ved hjælp af en prioritering af trusler, innovationsmidler til modforanstaltninger, rescEU-kapaciteter og opbygning af lagre af medicinske

[56] COM(2025) 30 final.
[57] COM(2025) 85 final.
[58] Direktiv 2009/81/EF om samordning af fremgangsmåderne ved ordregivende myndigheders eller ordregiveres indgåelse af visse bygge- og anlægs-, vareindkøbs- og tjenesteydelseskontrakter på forsvars- og sikkerhedsområdet (EUT L 216 af 20.8.2009).

modforanstaltninger. For at beskytte EU mod pandemier og CBRN-trusler vil EU med sin **strategi for medicinske modforanstaltninger** desuden støtte udviklingen af medicinske modforanstaltninger – fra forskning til fremstilling og distribution.

EU har på grundlag af erfaringerne fra covid-19-pandemien styrket sundhedssikkerhedsrammen[59]. Kommissionen udpeger EU-referencelaboratorier inden for folkesundhed for at styrke kapaciteten til overvågning og hurtig opdagelse på EU-plan og nationalt plan. Der vil i 2025 blive offentliggjort en EU-plan for beredskab, forebyggelse og indsats inden for sundhedssikkerhed.

Vigtige tiltag

Kommissionen vil:

- **i 2025 gennemgå og revidere forordningen om cybersikkerhed**
- **udvikle foranstaltninger til sikring af cybersikker brug af cloudtjenester**
- **i 2025 foreslå en EU-havnestrategi**
- **i 2026 revidere EU's udbudsregler på forsvars- og sikkerhedsområdet**
- **i 2026 fremlægge en ny handlingsplan for CBRN-beredskab og -indsats**

Kommissionen vil i samarbejde med medlemsstaterne:

- **udvikle og udrulle den europæiske kvantekommunikationsinfrastruktur (EuroQCI)**
- **sikre en effektiv håndhævelse af forordningen om digitale tjenester**
- **arbejde på at bekæmpe brugen af migration som våben**
- **oprette et system for luftfartssikkerhedsrelaterede hændelser**
- **arbejde på at oprette en varslingsmekanisme for transport- og forsyningskædesikkerhed, der omfatter flere instanser**

Rådet opfordres til at:

- **vedtage Rådets henstilling om EU's cyberplan**

Medlemsstaterne opfordres til at:

- **omsætte og fuldt ud gennemføre CER- og NIS 2-direktiverne**

5. Stramning af nettet omkring grov og organiseret kriminalitet

Vi vil bidrage til at udrydde organiseret kriminalitet ved at foreslå strengere regler for bekæmpelse af organiserede kriminelle netværk, herunder hvad angår efterforskning, gøre unge i EU mindre sårbare over for at blive rekrutteret til kriminalitet og intensivere foranstaltningerne til afskæring af adgangen til kriminelle værktøjer og aktiver.

Organiseret kriminalitet udnytter et miljø i forandring og spreder sig eksponentielt. Den gør brug af avancerede teknologier, er aktiv på tværs af flere jurisdiktioner og har stærke forbindelser, der rækker ud over EU's grænser. I betragtning af disse komplekse, tværnationale trusler er koordinering og støtte på EU-plan afgørende.

Forebyggelse af kriminalitet

Rekruttering af unge til organiseret kriminalitet er et voksende problem i EU. For at bekæmpe organiseret kriminalitet skal der tages fat på de **grundlæggende årsager** ved gennem en tilgang, som inddrager hele samfundet, at tilbyde uddannelse og alternativer til et liv i

[59] Navnlig forordning (EU) 2022/2371 om alvorlige grænseoverskridende sundhedstrusler.

kriminalitet. Kommissionen vil støtte integrationen af sikkerhedshensyn i EU's uddannelses-, social-, beskæftigelses- og regionalpolitik. EU vil **fremme evidensbaserede kriminalitetsforebyggelsespolitikker**[60], der er skræddersyet til lokale forhold.

For at beskytte modtagere af onlinetjenester, navnlig mindreårige, mod bl.a. seksuelt misbrug af børn, menneskehandlere og onlinerekruttering til kriminalitet eller voldelig ekstremisme kræves det i henhold til bestemmelserne i **forordningen om digitale tjenester**, at udbydere af onlineplatforme, der er tilgængelige for mindreårige, skal håndtere risici og reagere på ulovligt indhold, herunder hadefuld tale. Kommissionen planlægger at udstede **retningslinjer for beskyttelse af mindreårige** for at hjælpe udbydere af onlineplatforme med at sikre et højt niveau for beskyttelse af privatlivets fred og sikkerhed for mindreårige online. Retningslinjerne vil indeholde et sæt anbefalinger til alle digitale tjenester, der opererer i Unionen, med det formål at øge beskyttelsen af mindreårige online. I 2025 planlægger Kommissionen også at fremme en **EU-alderskontrolløsning til beskyttelse af privatlivets fred**, som vil udfylde hullet, indtil den europæiske digitale identitetstegnebog bliver tilgængelig i slutningen af 2026. Kommissionen vil også fremlægge en handlingsplan mod cybermobning.

Herudover vil Kommissionen fortsat støtte frivilligt flerpartssamarbejde med onlineplatforme og andre relevante aktører, herunder gennem EU's internetforum og målrettede adfærdskodekser i henhold til forordningen om digitale tjenester, f.eks. adfærdskodeksen for bekæmpelse af ulovlig hadefuld tale på internettet fra 2025. Målet er at øge bevidstheden herom, reagere på aktuelle og nye trusler i fællesskab og udarbejde og udveksle god praksis for så vidt angår afbødende foranstaltninger.

På lokalt plan viser konsekvenserne af organiseret kriminalitet tydeligt, at der er behov for regionale løsninger til at mindske sårbarheden og ulovlige aktiviteters tiltrækningskraft. I EU's dagsorden for byer tages der fat på sikkerhedsmæssige udfordringer i byerne med udgangspunkt i initiativet om EU's byer mod radikalisering. Kommissionen vil gennem Den Europæiske Fond for Regionaludvikling hjælpe medlemsstaterne med at øge sikkerheden i byer og regioner.

Et stærkere uddannelsesmæssigt grundlag og færdigheder understøtter modstandsdygtige og sammenhængende samfund. Unionen vil gennem **færdighedsunionen** og **handlingsplanen for integration og inklusion** arbejde på at hjælpe mennesker med at blive mere modstandsdygtige over for mis- og desinformation, radikalisering og rekruttering til kriminalitet.

Beskyttelse af børn mod alle former for vold, herunder kriminalitet og fysisk eller psykisk vold, online såvel som offline, er et vigtigt mål for EU. For at imødekomme de specifikke behov hos særligt sårbare grupper såsom børn, der i stigende grad udsættes for rekruttering og radikalisering, grooming og seksuelt misbrug, cybermobning, desinformation og andre trusler, vil EU udarbejde en **handlingsplan for beskyttelse af børn mod kriminalitet**, der omfatter online- og offlinedimensionen. Den vil indeholde en sammenhængende og koordineret tilgang baseret på de tilgængelige rammer og værktøjer, herunder det fremtidige EU-center for forebyggelse og bekæmpelse af seksuelt misbrug af børn og andre EU-organer og -agenturer, samt forslag til løsninger på de områder, hvor der fortsat er mangler.

Optrævling af kriminelle netværk og deres katalysatorer

Bekæmpelsen af kriminelle højrisikonetværk, bandeledere og katalysatorer skal intensiveres. Trods bemærkelsesværdige resultater den seneste tid[61] står forældede regler og inkonsekvente definitioner af kriminelle netværk i vejen for en effektiv strafferetlig indsats og et effektivt grænseoverskridende samarbejde. Kommissionen vil gennemgå forældet lovgivning på dette

[60] https://www.eucpn.org/.
[61] Herunder nylige EMPACT-sager.

område og foreslå en ny **retlig ramme vedrørende organiseret kriminalitet** for at styrke indsatsen.

Administrativ håndhævelse kan supplere retshåndhævelsen med henblik på at opnå hurtigere resultater, således som EPPO og Det Europæiske Kontor for Bekæmpelse af Svig (OLAF) har vist i forbindelse med håndteringen af **grænseoverskridende svig og kriminalitet, der skader EU's finansielle interesser**. Tilskudssvindlere fokuserer på sektorer som f.eks. vedvarende energi og forskningsprogrammer samt landbrugssektoren[62]. Kommissionen vil undersøge, hvordan anvendelsen af strafferetlige og administrative værktøjer kan koordineres, så samarbejdet med Europol, Eurojust og EPPO styrkes. Kommissionen vil også fortsat støtte en bredere anvendelse af **den administrative tilgang** for at sætte lokale og andre administrative myndigheder i stand til at sætte en stopper for kriminel infiltration[63].

EU arbejder på at styrke sin retlige ramme for bekæmpelse af **korruption**[64]. Europa-Parlamentet og Rådet bør hurtigt afslutte forhandlingerne om den ajourførte ramme for bekæmpelse af korruption, som Kommissionen har foreslået. Kommissionen vil fremlægge en EU-strategi for bekæmpelse af korruption for at fremme integriteten og styrke koordineringen mellem alle relevante myndigheder og interessenter på dette område.

Skydevåben udgør en væsentlig faktor bag den stigende vold, der begås af organiserede kriminelle grupper. Kommissionen vil foreslå fælles strafferetlige standarder i forbindelse med ulovlig handel med skydevåben. En ny **EU-handlingsplan om ulovlig handel med skydevåben** vil fokusere på at beskytte det lovlige marked, begrænse kriminelle aktiviteter på grundlag af bedre efterretninger og styrke det internationale samarbejde med særligt fokus på Ukraine og Vestbalkan.

Pyrotekniske artikler, der er erhvervet på ulovlig vis og anvendes til kriminalitet, kræver foranstaltninger til at sikre en bedre forebyggelse og sporbarhed. Kommissionen er i øjeblikket i færd med at evaluere direktivet om pyrotekniske artikler og vil også overveje **strafferetlige sanktioner i forbindelse med ulovlig handel med pyrotekniske artikler**.

Følg pengene

For at bekæmpe organiseret kriminalitet og terrorisme er det afgørende at **følge pengene**, selv om der stadig er mange udfordringer i forbindelse hermed. Forbindelsen mellem organiseret kriminalitet og pengestrømme kræver en intens og kombineret indsats for at sætte en stopper for kriminelle netværks adgang til finansieringskilder og for bedre at beskytte mennesker, virksomheder og offentlige budgetter.

EU har styrket sin indsats med de nye regler for bekæmpelse af hvidvask af penge, herunder oprettelsen af **EU's Myndighed for Bekæmpelse af Hvidvask af Penge (AMLA)**[65]. Samarbejde mellem AMLA, OLAF, EPPO, Eurojust og Europol er afgørende for at foretage effektive finansielle efterforskninger. Kommissionen vil støtte oprettelsen af **partnerskaber**, både dem, der letter samarbejdet mellem agenturer, og dem, der involverer den private sektor.

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

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

[64] Forslag til Europa-Parlamentets og Rådets direktiv om bekæmpelse af korruption, om erstatning af Rådets rammeafgørelse 2003/568/RIA og konventionen om bekæmpelse af bestikkelse, der involverer tjenestemænd ved De Europæiske Fællesskaber eller i Den Europæiske Unions medlemsstater, og om ændring af Europa-Parlamentets og Rådets direktiv (EU) 2017/1371 (COM(2023) 234 final, Bruxelles, den 3.5.2023).

[65] https://www.amla.europa.eu/index_en.

For at fjerne de økonomiske drivkræfter bag organiseret kriminalitet er det afgørende at beslaglægge aktiver og konfiskere udbytte fra kriminelle aktiviteter. Medlemsstaterne bør hurtigst muligt gennemføre og fuldt ud anvende de nyligt vedtagne skærpede regler om **inddrivelse og konfiskation af aktiver**[66]. Bekæmpelse af parallelle finansielle systemer, der omgår EU's ramme for bekæmpelse af hvidvask af penge, herunder kryptobaserede systemer, kræver også innovative tiltag, udveksling af bedste praksis mellem medlemsstaterne og øget støtte fra Europol og Eurojust. Kommissionen vil undersøge gennemførligheden af et nyt EU-dækkende system til sporing af udbytte fra organiseret kriminalitet og finansiering af terrorisme samt tilskynde til rettidige og udvidede informationsstrømme fra **finansielle efterretningsenheder** med henblik på retshåndhævelse. Kommissionen vil undersøge, hvordan smuthuller kan lukkes, støtte medlemsstaterne i forbindelse med kapacitetsopbygning og arbejde videre med at styrke samarbejdet med tredjelande, der misbruges af kriminelle til illegale bankoperationer.

Bekæmpelse af grov kriminalitet

For at bekæmpe grov kriminalitet er det ud over at optrævle kriminelle netværk nødvendigt med en målrettet indsats. For at styrke vores evne til at bekæmpe **onlinesvindel**, som forvolder stor økonomisk skade[67], vil Kommissionen støtte forebyggende foranstaltninger og mere effektive retshåndhævelsestiltag samt samarbejde med medlemsstaterne og interessenter om at støtte og beskytte ofre, herunder ved at hjælpe dem med at få deres penge tilbage. Denne indsats vil blive formaliseret i en **handlingsplan vedrørende onlinesvindel**.

Med udgangspunkt i EU-strategien om bekæmpelse af **seksuelt misbrug af børn**[68] for 2020-2025 vil Kommissionen hjælpe Europa-Parlamentet og Rådet med at færdiggøre de to lovgivningsforslag[69] for at forebygge og bekæmpe seksuelt misbrug af børn online og gøre retshåndhævelsestiltag mod seksuelt misbrug og seksuel udnyttelse af børn mere effektive. Da de midlertidige regler kun gælder indtil april 2026, er det afgørende at indføre en permanent retlig ramme, og Kommissionen opfordrer Europa-Parlamentet og Rådet til at indlede forhandlinger om forslaget til forordning om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn. Europa-Parlamentet og Rådet opfordres også til at gøre fremskridt med forhandlingerne om direktivet om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og materiale med seksuelt misbrug af børn, som vil fastsætte minimumsregler for, hvad der udgør strafbare handlinger, og sanktioner i forbindelse med seksuel udnyttelse af børn.

Halvdelen af de farligste kriminelle netværk i EU er involveret i voldelig **narkotikahandel**. Selv om EU for nylig har styrket bekæmpelsen af denne type kriminalitet[70], navnlig ved at udvide mandatet for **EU's Narkotikaagentur**, er der behov for yderligere tiltag. Kommissionen vil arbejde tæt sammen med medlemsstaterne om at foreslå en ny **EU-narkotikastrategi**. Den vil også revidere den retlige **ramme vedrørende narkotikaprækursorer** og foreslå en **EU-handlingsplan for bekæmpelse af narkotikahandel** for at sætte en stopper for smuglerruterne og ødelægge forretningsmodellerne. **EU-havnealliancens offentlig-private partnerskab** om styrket havnebeskyttelse vil blive udvidet til at omfatte mindre havne og indlandshavne og sikre, at reglerne om maritim sikkerhed håndhæves. I erkendelse af de alvorlige lokale virkninger af narkotikahandel vil Kommissionen fortsat støtte en afbalanceret, evidensbaseret

[66] Europa-Parlamentets og Rådets direktiv (EU) 2024/1260 af 24. april 2024 om inddrivelse og konfiskation af aktiver (EUT L, 2024/1260, 2.5.2024).
[67] Global Anti-Scam Report 2024(foreligger ikke på dansk).
[68] COM(2020) 607 final.
[69] COM(2022) 209 final og COM(2024) 60 final.
[70] COM(2023) 641 final.

og tværfaglig narkotikapolitik, som gør det muligt at gribe ind over for pludselig narkotikaindstrømning, navnlig af syntetiske opioider.

For at bekæmpe udnyttelse af mennesker har EU vedtaget nye regler[71] og vil indføre en **ny EU-strategi for bekæmpelse af menneskehandel** (2026-2030), der dækker alle faser – lige fra forebyggelse til retsforfølgning – med fokus på støtte til ofre på både EU-plan og internationalt plan.

For at bekæmpe **smugling af migranter** vil Kommissionen i samarbejde med Europol, Eurojust og Frontex lede indsatsen sammen med centrale partnere gennem den nye globale alliance til bekæmpelse af smugling af migranter, herunder også online. Kommissionens forslag om bekæmpelse af smugling[72] bør hurtigst muligt vedtages og gennemføres. Herudover har Kommissionen efter vedtagelsen af **værktøjskassen vedrørende transportvirksomheder**[73] øget kontakten til udenlandske myndigheder og virksomheder og vil fortsat samarbejde med luftfartsindustrien og organisationer inden for civil luftfart[74] for at øge bevidstheden om smugling af migranter ad luftvejen[75].

Miljøkriminalitet truer miljøet, folkesundheden og økonomien på lang sigt. Kommissionen vil støtte medlemsstaterne i forbindelse med gennemførelsen af direktivet om miljøkriminalitet[76] og styrke operationelle netværk og tiltag på dette område[77]. En solid håndhævelse er af afgørende betydning. Desuden vil Europarådets nyligt vedtagne konvention om strafferetlig beskyttelse af miljøet[78] bidrage til at sikre en solid og sammenlignelig indsats for at bekæmpe miljøkriminalitet, både i og uden for Europa.

Den strafferetlige indsats

Kriminalitet og terrorisme kan påvirke alle, så det er vigtigt at støtte og beskytte **ofres** rettigheder for at mindske skaderne og øge den overordnede sikkerhed og tillid til myndighederne. Kommissionen vil på grundlag af direktivet om ofres rettigheder indføre en ny **EU-strategi for ofres rettigheder**.

EU's strafferetlige systemer har brug for effektive værktøjer til at imødegå nye trusler. Med henblik herpå har Kommissionen lanceret et **forum på højt plan om fremtiden for EU's strafferet**. Dette forum samler medlemsstaterne, Europa-Parlamentet, EU-agenturer og -organer og andre relevante interessenter. Målet er at drøfte, hvordan vi kan sikre, at vores strafferetlige systemer forbliver effektive, retfærdige og modstandsdygtige i lyset af nye

[71] Direktiv (EU) 2024/1712 af 13. juni 2024 om ændring af direktiv 2011/36/EU om forebyggelse og bekæmpelse af menneskehandel og beskyttelse af ofrene herfor (EUT L, 2024/1712, 24.6.2024).
[72] COM(2023) 755 final og COM(2023) 754 final.
[73] Toolbox addressing the use of commercial means of transport to facilitate irregular migration to the EU(foreligger ikke på dansk).
[74] Herunder Organisationen for International Civil Luftfart (ICAO).
[75] Kommissionen vil også støtte færdiggørelsen af forordningen om foranstaltninger over for transportvirksomheder, der letter eller deltager i menneskehandel eller smugling af migranter (COM(2021) 753 final).
[76] Europa-Parlamentets og Rådets direktiv (EU) 2024/1203 af 11. april 2024 om strafferetlig beskyttelse af miljøet (EUT L, 2024/1203, 30.4.2024).
[77] EU-netværket til gennemførelse og håndhævelse af miljølovgivning (Impel), det europæiske netværk af miljøanklagere (ENPE), EnviCrimeNet og EU's forum for miljødommere (EUFJE).
[78] Ekspertudvalget vedrørende strafferetlig beskyttelse af miljøet (PC-ENV) – Europarådets Styringskomité for Strafferetlige Problemer.

udfordringer, samtidig med at det retlige samarbejde og den gensidige tillid styrkes, herunder gennem digitalisering[79].

Vigtige tiltag

Kommissionen vil:

- **i 2026 fremsætte et lovgivningsforslag om moderniserede regler vedrørende organiseret kriminalitet**
- **i 2025 fremsætte et lovgivningsforslag om revision af den retlige ramme vedrørende narkotikaprækursorer**
- **i 2025 fremsætte et lovgivningsforslag om fælles strafferetlige standarder i forbindelse med ulovlig handel med skydevåben**
- **vurdere behovet for at revidere direktiverne om pyrotekniske artikler og eksplosivstoffer til civil brug**
- **vurdere behovet for yderligere at styrke den europæiske efterforskningskendelse og den europæiske arrestordre**
- **i 2026 fremlægge en ny EU-strategi for bekæmpelse af menneskehandel**
- **i 2026 fremlægge en ny EU-strategi for ofres rettigheder**
- **senest i 2027 fremlægge en EU-handlingsplan for beskyttelse af børn mod kriminalitet**
- **i 2025 fremlægge en EU-handlingsplan for bekæmpelse af narkotikahandel**
- **i 2026 fremlægge en EU-handlingsplan om ulovlig handel med skydevåben**
- **fra 2025 gradvist udvide EU's havnealliance**
- **i 2026 vedtage retningslinjer for beskyttelse af mindreårige i henhold til forordningen om digitale tjenester**
- **i 2026 fremlægge en EU-handlingsplan mod cybermobning**

Medlemsstaterne opfordres til at:

- **gennemføre de nye regler om inddrivelse og konfiskation af aktiver fuldt ud inden udgangen af 2026 og anvende dem fuldt ud**
- **gennemføre den administrative tilgang til bekæmpelse af kriminel infiltration**
- **oprette offentlig-private partnerskaber til bekæmpelse af hvidvask af penge**
- **omsætte og gennemføre direktivet om forebyggelse og bekæmpelse af vold mod kvinder og vold i hjemmet fuldt ud**

Europa-Parlamentet og Rådet opfordres til at:

- **gøre fremskridt med forhandlingerne om forordningen om regler til forebyggelse og bekæmpelse af seksuelt misbrug af børn og direktivet om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og materiale, der viser seksuelt misbrug af børn**
- **afslutte forhandlingerne om direktivet om bekæmpelse af korruption**

[79] Navnlig gennem oprettelsen af eCODEX (e-Justice Communication via Online Data Exchange) og ECRIS-TCN (det europæiske informationssystem til udveksling af oplysninger fra strafferegistre vedrørende tredjelandsstatsborgere).

6. Bekæmpelse af terrorisme og voldelig ekstremisme

Vi vil indføre en omfattende terrorbekæmpelsesdagsorden med henblik på at forebygge radikalisering, sikre onlinemiljøer og offentlige områder, tilintetgøre finansieringskanaler og reagere i tilfælde af angreb.

Terrortrusselsniveauet i EU er fortsat højt. Det hænger tæt sammen med de afsmittende virkninger af geopolitiske begivenheder, nye teknologier og nye midler til finansiering af terrorisme. Vi er nødt til at sikre, at EU er godt rustet til at foregribe trusler, forebygge radikalisering (både offline og online), beskytte borgerne og offentlige områder mod angreb og reagere effektivt i tilfælde af angreb. For at fastlægge EU's fremtidige indsats vil der i 2025 blive fremlagt en **ny EU-dagsorden for forebyggelse og bekæmpelse af terrorisme og voldelig ekstremisme**. I overensstemmelse med den nye dagsorden vil EU og Vestbalkan i 2025 undertegne den nye **fælles handlingsplan** om forebyggelse og bekæmpelse af terrorisme og voldelig ekstremisme.

Forebyggelse af radikalisering og beskyttelse af mennesker online

Ligesom med bekæmpelse af organiseret kriminalitet begynder bekæmpelse af terrorisme og voldelig ekstremisme med **bekæmpelse af de grundlæggende årsager hertil**. **EU-videncentret om forebyggelse af radikalisering** vil øge sin støtte til fagfolk og politiske beslutningstagere med en ny **omfattende forebyggelsesværktøjskasse**, der giver mulighed for tidligt at indkredse sårbare personer, navnlig mindreårige, og gribe ind. Radikaliseringen sker ofte i fængsler, og for at hjælpe medlemsstaterne med at løse dette problem vil Kommissionen fremsætte nye henstillinger.

Terrorister og voldelige ekstremister bruger onlineplatforme til at sprede terrorrelateret og skadeligt indhold, indsamle midler og rekruttere. Sårbare brugere, navnlig mindreårige, bliver radikaliseret online i et alarmerende tempo. **Forordningen om terrorrelateret onlineindhold** har været afgørende for bekæmpelsen af udbredelsen af terrorrelateret onlineindhold og gjort det muligt hurtigt at fjerne det mest afskyelige og farlige materiale[80]. Kommissionen er i øjeblikket ved at evaluere, hvordan forordningen fungerer, og vil vurdere, hvordan denne ramme bedst kan styrkes.

EU's kriseprotokol for en fælles og hurtig reaktion fra de retshåndhævende myndigheders og techindustriens side i forbindelse med terrorangreb vil blive ændret for at sikre skalerbarhed og fleksibilitet til at kunne reagere på den voksende onlinedimension af terrorangreb. EU's internetforum vil fortsat være den vigtigste kanal for frivilligt samarbejde med techindustrien om at bekæmpe terrorrelateret og skadeligt indhold online. Desuden deltager Kommissionen i internationale initiativer såsom Christchurch Call Foundation og det globale internetforum til terrorbekæmpelse (GIFCT).

Bekæmpelse af finansiering af terrorisme

Terrorister finansierer deres aktiviteter med crowdfundingkampagner, kryptoaktiver, neobanker eller onlinebetalingsplatforme. Det er nødvendigt, at de retshåndhævende myndigheder opdager og undersøger disse finansielle strømme. Dette kræver midler, værktøjer og ekspertise. **Netværket af finansielle efterforskere inden for terrorbekæmpelse** spiller en central rolle. Kommissionen vil undersøge mulighederne for at oprette et **nyt EU-dækkende system til sporing af finansiering af terrorisme**, der omfatter transaktioner inden for EU og

[80] Pr. 31. december 2024 var der udstedt 1 426 påbud om at fjerne terrorrelateret indhold eller blokere adgangen hertil, hvoraf langt de fleste påbud var rettet mod jihadistisk terrorrelateret indhold, men også højreekstremistisk terrorindhold.

SEPA, overførsler af kryptoaktiver, onlinebetalinger og pengeoverførsler, som supplement til aftalen mellem EU og USA om programmet til sporing af finansiering af terrorisme (TFTP).

EU-budgettet skal **beskyttes, så det ikke misbruges til at fremme radikale/ekstremistiske synspunkter** i medlemsstaterne. Med den reviderede **finansforordning** udgør en dom for "tilskyndelse til forskelsbehandling, had eller vold" nu en begrundelse for udelukkelse fra EU-finansiering. Kommissionen vil fortsat undersøge, hvordan denne værktøjskasse bedst kan anvendes fuldt ud, herunder ved udvælgelsen af potentielle støttemodtagere. Beskyttelsen af EU-budgettet afhænger også af en høj grad af samarbejde og udveksling af oplysninger med nationale myndigheder og EU-agenturer og -organer.

Beskyttelse mod angreb

Ud over investeringer i forebyggelse af radikalisering er det et vigtigt element i beskyttelsen af borgerne, at terroristers og kriminelles midler til at begå angreb begrænses. Der er behov for handling, både hvad angår de redskaber, som terroristerne anvender, og for at beskytte de mål, der er i fare for at blive angrebet.

Ud over foranstaltninger vedrørende skydevåben vil Kommissionen også **revidere reglerne** om **udgangsstoffer til eksplosivstoffer**, så de også omfatter kemikalier i højrisikogruppen. **Offentlige områder** er fortsat de mest almindelige mål for terrorangreb, navnlig for soloaktører. For at beskytte borgerne vil **EU's rådgivningsprogram vedrørende beskyttelse af sikkerheden** blive styrket med henblik på at foretage sårbarhedsvurderinger af offentlige områder, kritisk infrastruktur og højrisikobegivenheder efter anmodning fra medlemsstaterne og finansieret over EU-budgettet inden for rammerne af Fonden for Intern Sikkerhed. EU påtænker at udvide den finansiering, der er til rådighed til beskyttelse af offentlige områder. Kommissionen tilbyder støtte til medlemsstaternes myndigheder og private operatører gennem målrettet vejledning og målrettede værktøjer såsom videncentret for beskyttelse af offentlige områder[81], og der er siden 2020 allerede blevet stillet 70 mio. EUR til rådighed til støtte for beskyttelsen af offentlige områder.

Kommissionen vil også undersøge mulighederne for at indføre krav til organisationer om at overveje eller anvende sikkerhedsforanstaltninger på offentligt tilgængelige steder gennem samarbejde med lokale myndigheder og private partnere.

På grund af åbenlyse sårbarheder vil **EU-strategien for bekæmpelse af antisemitisme og fremme af jødisk liv (2021-2030)** fortsat være retningsgivende for Kommissionens indsats for at beskytte det jødiske samfund. Kommissionen vil ligeledes sikre, at der findes passende værktøjer til støtte for medlemsstaterne til **bekæmpelse af antimuslimsk had**.

Brugen af **droner** til spionage og angreb udgør en stadig større sikkerhedsmæssig udfordring. Kommissionen vil udvikle en **harmoniseret metode til afprøvning af dronebekæmpelsessystemer**, oprette et **ekspertisecenter for dronebekæmpelse** og vurdere behovet for at harmonisere medlemsstaternes lovgivning og procedurer[82].

Fremmedkrigere

For at identificere fremmedkrigere, der vender tilbage eller indrejser ved EU's ydre grænser, er der behov for oplysninger om personer, der udgør en terrortrussel. Med henblik herpå vil Kommissionen sammen med Europol styrke sit **samarbejde med centrale tredjelande for at indhente personoplysninger og biometriske oplysninger for enkeltpersoner, der kan udgøre en terrortrussel**, herunder fremmedkrigere, med henblik på efterfølgende at indføre dem i Schengeninformationssystemet i fuld overensstemmelse med gældende EU-retlige og

[81] Videncenter for beskyttelse af offentlige områder.
[82] I forlængelse af de vigtige foranstaltninger i dronebekæmpelsesmeddelelsen fra 2023 (COM(2023) 659 final).

nationale retlige rammer. Det er derfor vigtigt, at medlemsstaterne gør brug af alle eksisterende værktøjer. Dette omfatter indførelse af alle relevante oplysninger i **SIS**, styrkelse af biometrisk kontrol og obligatorisk systematisk kontrol af alle personer ved EU's ydre grænser[83]. Desuden vil de **fælles risikoindikatorer**, som Frontex har udviklet, fortsat støtte medlemsstaternes grænsekontrolmyndigheder i deres arbejde med at identificere potentielle fremmedkrigere og vurdere disses mistænkelige rejseaktiviteter.

For at sikre, at medlemsstaterne bevarer adgangen til **bevismateriale fra kampområder**, som FN's efterforskningshold til fremme af ansvarliggørelse for forbrydelser begået af Da'esh/ISIL (UNITAD) har indsamlet med henblik på retsforfølgning af fremmedkrigere, vil Kommissionen sammen med Eurojust desuden vurdere muligheden for at opbevare dette bevismateriale i Eurojusts database med bevismateriale om de alvorligste internationale forbrydelser. Desuden vil det nye europæiske **retlige terrorbekæmpelsesregister** fortsat være til hjælp for medlemsstaternes domstole, når de hurtigt skal identificere grænseoverskridende forbindelser i terrorsager.

Vigtige tiltag

Kommissionen vil:

- **i 2025 vedtage en ny EU-dagsorden for forebyggelse og bekæmpelse af terrorisme og voldelig ekstremisme**
- **i 2025 undertegne en ny fælles handlingsplan om forebyggelse og bekæmpelse af terrorisme og voldelig ekstremisme med Vestbalkan**
- **udvikle en ny omfattende forebyggelsesværktøjskasse sammen med EU-videncentret**
- **i 2026 evaluere anvendelsen af forordningen om terrorrelateret onlineindhold**
- **i 2025 ændre EU's kriseprotokol**
- **i 2026 fremsætte et lovgivningsforslag om revision af forordningen om markedsføring og anvendelse af udgangsstoffer til eksplosivstoffer**
- **undersøge gennemførligheden af et nyt EU-dækkende system til sporing af finansiering af terrorisme**

Medlemsstaterne opfordres til at:

- **forbedre den biometriske kontrol og foretage obligatorisk systematisk kontrol ved EU's ydre grænser**
- **gøre fuld brug af det europæiske retlige terrorbekæmpelsesregister**

7. EU som en stærk global aktør på sikkerhedsområdet

For at øge sikkerheden i EU vil vi styrke det operationelle samarbejde gennem partnerskaber med centrale regioner såsom EU's udvidelses- og naboskabspartnere, Latinamerika og lande i Middelhavsområdet. Der vil i det internationale samarbejde blive taget hensyn til EU's sikkerhedsinteresser, herunder ved at udnytte EU's værktøjer og instrumenter.

De seneste år har vist de iboende forbindelser mellem EU's ydre og indre sikkerhed. Ruslands angrebskrig mod Ukraine, konflikten i Gaza, situationen i Syrien og nye konflikter rundt om i verden har haft alvorlige afsmittende virkninger på den indre sikkerhed i EU. For at modvirke den globale ustabilitets indvirkning på den indre sikkerhed i EU er **EU nødt til aktivt at forsvare sine sikkerhedsinteresser** ved at imødegå eksterne trusler, sætte en stopper for

[83] I fuld overensstemmelse med Schengengrænsekodeksen og screeningforordningen.

smuglerruter og beskytte korridorer af strategisk interesse såsom handelsruter. Samtidig vil EU forblive en stærk allieret for partnerlande og arbejde sammen om at øge den globale sikkerhed og opbygge gensidig modstandsdygtighed over for trusler.

I de seneste år har EU taget betydelige skridt til at styrke sit sikkerhedssamarbejde. Der er indgået operationelle aftaler om retshåndhævelse og retligt samarbejde samt andre typer ordninger med partnerlande. EU stræber aktivt mod at indgå yderligere internationale aftaler i overensstemmelse med Rådets forhandlingsdirektiver og kapacitetsopbyggende initiativer, som fremmes af EU's agenturer og organer. NDICI – et globalt Europa er også afgørende for at styrke sikkerheden med partnerlandene.

Den **regelbaserede multilaterale orden** er en vigtig forudsætning for at styrke den globale sikkerhed. Sikkerhedsdialoger, herunder tematiske dialoger, er afgørende for at styrke disse bestræbelser. Gennemførelsen af det **strategiske kompas for sikkerhed og forsvar** sideløbende med bilaterale og multilaterale samarbejdsrammer såsom stabiliserings- og associeringsaftaler og associeringsaftaler samt samarbejde med organisationer som FN og NATO er afgørende for udviklingen af effektive sikkerhedsløsninger. EU vil fortsat påtage sig sin rolle i multilaterale fora[84] og styrke sit samarbejde med relevante internationale og regionale organisationer og rammer, herunder NATO, De Forenede Nationer, Europarådet, Interpol, G7, OSCE og civilsamfundet.

Regionalt samarbejde

Det skal prioriteres og er politisk og geostrategisk nødvendigt at fortsætte EU's urokkelige støtte til **Ukraine** og styrke sikkerheden og modstandsdygtigheden i **EU-udvidelseslande**. Støtte til EU's sikkerhed bør gå hånd i hånd med en **fremskyndet integration af kandidatlandene** i **EU's sikkerhedsarkitektur** sideløbende med konsolideringen af deres regionale samarbejde. Kommissionen vil anvende EU's udvidelsespolitik til støtte for EU-kandidatlandes og potentielle kandidatlandes kapacitet til at reagere på trusler, øge det operationelle samarbejde og informationsudvekslingen og sikre overensstemmelse med EU's principper, lovgivning og værktøjer. Instrumentet til førtiltrædelsesbistand (IPA III) samt faciliteten for Ukraine, Moldova og Vestbalkan er afgørende for at styrke sikkerheden i både kandidatlande og potentielle kandidatlande.

EU vil også integrere **naboskabspartnerne** yderligere i EU's sikkerhedsarkitektur. Unionen vil gennem den **nye pagt for Middelhavsområdet** og den kommende **strategiske tilgang til Sortehavet** sigte mod fortsat at opbygge regionalt samarbejde og bilaterale strategiske omfattende partnerskaber med en sikkerhedsdimension, når det er relevant, med regelmæssige sikkerhedsdialoger på højt niveau. Det operationelle samarbejde med Nordafrika, **Mellemøsten og Golfstaterne** vil blive styrket, navnlig inden for bekæmpelse af terrorisme, bekæmpelse af hvidvask af penge, handel med skydevåben og produktion af og handel med narkotika, især captagon.

For at imødegå stigningen i terroraktiviteter og kriminelle aktiviteter og de potentielle afsmittende virkninger heraf i **Afrika syd for Sahara**, **navnlig Sahel, Afrikas Horn og Vestafrika**, vil EU øge støtten til Den Afrikanske Union, de regionale økonomiske fællesskaber og landene i regionen. I overensstemmelse med EU-strategien for maritim sikkerhed[85] vil EU styrke samarbejdet i **Guineabugten, Det Røde Hav og Det Indiske Ocean** for at bekæmpe smugler- og piratvirksomhed ved at støtte samarbejdet internt i Afrika og regionalt og med

[84] Det Globale Forum for Terrorbekæmpelse, den globale koalition mod Da'esh, det globale internetforum til terrorbekæmpelse (GIFCT), Christchurch Call Foundation og Global Coalition to Address Synthetic Drug Threats.
[85] JOIN(2023) 8 final.

støtte fra EU's koordinerede maritime tilstedeværelse og Det Maritime Analyse- og Operationscenter vedrørende Narkotika (MAOC-N).

EU vil sammen med **Latinamerika og Caribien** styrke det operationelle samarbejde for at optrævle og retsforfølge kriminelle højrisikonetværk og sætte en stopper for ulovlige aktiviteter og smuglerruter samt styrke samarbejdsrammer som f.eks. Den Latinamerikanske Komité for Intern Sikkerhed (EU-CLASI) og koordinations- og samarbejdsmekanismen vedrørende narkotika (EU-CELAC). Logistiske knudepunkters modstandsdygtighed og partnerskaber og følg pengene-tilgange vil være blandt prioriteterne. EU vil yderligere støtte udviklingen af politifællesskabet i Nord-, Mellem- og Sydamerika (AMERIPOL) med henblik på at gøre det til den regionale ækvivalent til Europol og styrke det retlige samarbejde mellem medlemsstaterne og regionen. EU vil også samarbejde med **Syd- og Centralasien** i forbindelse med fælles sikkerhedsmæssige udfordringer vedrørende terrorisme, ulovlig handel med varer, herunder narkotika, menneskehandel og smugling af migranter.

Herudover vil EU støtte regionale samarbejdsrammer i tredjelande for yderligere at bistå dem med at sætte en stopper for ulovlig handel ved kilden i overensstemmelse med princippet om fælles ansvar for hele den kriminelle forsyningskæde. Endelig vil EU gøre sin del for at bidrage til at styrke sikkerheden i logistiske knudepunkter i udlandet ved at koordinere **fælles inspektioner i tredjelandshavne**.

Operationelt samarbejde

Global Gateway vil støtte bæredygtige infrastrukturprojekter af høj kvalitet inden for den digitale sektor og sektorerne for klima og energi, transport, sundhed, uddannelse og forskning. Kommissionen vil nu medtage sikkerhedshensyn, hvor det er relevant, i de kommende Global Gateway-investeringer. Dette vil omfatte initiativer, der er afgørende for EU's og partnerlandenes strategiske autonomi, såsom infrastrukturprojekter, der omfatter sikkerhedsvurderinger og risikobegrænsende foranstaltninger.

Kommissionen vil bestræbe sig på at indgå yderligere **aftaler mellem EU og tredjelande om samarbejde med Europol og Eurojust**, navnlig med lande i Latinamerika.

Desuden er tredjelandes proaktive deltagelse i **EMPACT** et af de mest effektive midler til at styrke det operationelle samarbejde. EU vil yderligere opfordre til, at tredjelande, navnlig Vestbalkan, det østlige naboskab, Afrika syd for Sahara, Nordafrika, Mellemøsten, Latinamerika og Caribien, deltager i denne ramme. Et andet værktøj til at intensivere samarbejdet med tredjelande om bekæmpelse af kriminalitet er de af Europol koordinerede operationelle taskforcer mellem medlemsstaterne, som tredjelande kan deltage i. Kommissionen sigter også mod at afslutte forhandlingerne om den internationale aftale mellem **EU og Interpol**[86] for at sikre en mere ensartet tilgang til globale sikkerhedstrusler og bekæmpe grænseoverskridende kriminalitet.

Unionen skal være synlig på stedet inden for rammerne af en Team Europe-tilgang. Specialiseret personale fra Unionen og medlemsstaterne spiller en afgørende rolle, når det gælder om at sikre, at Unionens foranstaltninger udadtil er tilstrækkeligt underbyggede, koordinerede og tilpasningsduelige. For at udvide denne tilgang vil Kommissionen med støtte fra den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik styrke **forbindelsesnetværkene** og lette udsendelsen af regionale **forbindelsesofficerer fra Europol og Eurojust** i overensstemmelse med medlemsstaternes operationelle behov.

EU vil søge et tættere operationelt samarbejde med retshåndhævende og retslige myndigheder og fremme informationsudveksling i realtid og fælles operationer gennem **fælles**

[86] Rådets afgørelse (EU) 2021/1312 af 19. juli 2021 og Rådets afgørelse (EU) 2021/1313 af 19. juli 2021.

efterforskningshold i tredjelande med støtte fra Europol og Eurojust. Kommissionen vil også hjælpe medlemsstaterne med at oprette **fælles fusionscentre**, der samler eksperter og lokale retshåndhævende myndigheder i strategiske tredjelande.

Værktøjer inden for rammerne af den fælles udenrigs- og sikkerhedspolitik (FUSP)

Missioner inden for rammerne af den fælles sikkerheds- og forsvarspolitik (FUSP) vil også blive anvendt fuldt ud for bedre at afdække og håndtere eksterne trusler mod den indre sikkerhed i EU i overensstemmelse med de af Rådet fastsatte mandater. For at opbygge tredjelandes kapacitet vil den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik og Kommissionen støtte FUSP-aktioner med særlige finansieringsinstrumenter og undersøge alle passende finansieringsmuligheder.

EU's restriktive foranstaltninger er et veletableret FUSP-redskab, der også anvendes til at bekæmpe terrorisme. På grundlag af forslag fra den højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, medlemsstaterne eller Kommissionen kan Rådet vurdere, hvordan EU's eksisterende autonome restriktive foranstaltninger (EU's terrorliste) kan gøres mere effektive, operationelle og smidige. Det kan desuden overvejes at undersøge yderligere restriktive foranstaltninger rettet mod kriminelle netværk i overensstemmelse med FUSP-målene.

Visumpolitik og informationsudveksling

EU's visumpolitik er et vigtigt værktøj til at samarbejde med tredjelande og sikre vores grænser ved at kontrollere indrejse i EU og fastsætte betingelserne herfor. Kommissionen vil fuldt ud integrere **sikkerhedshensyn i EU's visumpolitik** gennem en kommende strategi for EU-visumpolitik. Kommissionen vil samarbejde med Europa-Parlamentet og Rådet om at vedtage forslaget om at revidere og strømline mekanismen til suspension af visumfritagelse, navnlig i særlige tilfælde, hvor den visumfri ordning misbruges[87]. Tredjelande vil blive opfordret til at udveksle information om personer, der kan udgøre en sikkerhedstrussel, og som vil blive registreret i EU's informationssystemer og databaser.

For at koordinere politikker og forstærke indsatsen samt opnå et mere effektivt, hurtigt og gnidningsløst samarbejde vil Kommissionen arbejde hen imod oprettelsen af **dataflowordninger** og undersøge måder at **forbedre informationsudvekslingen** med betroede tredjelande på med henblik på retshåndhævelse og grænseforvaltning i overensstemmelse med de grundlæggende rettigheder og databeskyttelsesreglerne.

Vigtige tiltag

Kommissionen vil:

- **indgå internationale aftaler mellem EU og prioriterede tredjelande om samarbejde med Europol og Eurojust**
- **tilskynde partnerlande til at deltage i EMPACT med henblik på at bekæmpe organiseret kriminalitet og terrorisme**
- **støtte EU-agenturer og -organer i forbindelse med oprettelsen og styrkelsen af samarbejdsordninger med partnerlande**
- **yderligere medtage sikkerhedshensyn i EU's visumpolitik gennem den kommende visumstrategi**
- **styrke informationsudvekslingen med betroede tredjelande med henblik på retshåndhævelse og grænseforvaltning**

[87] COM(2023) 642.

Kommissionen vil i samarbejde med den højtstående repræsentant for udenrigsanliggender:

- **gøre fuld brug af civile missioner inden for rammerne af den fælles sikkerheds- og forsvarspolitik (FUSP)**
- **senest i 2027 koordinere fælles inspektioner i tredjelandshavne**

Kommissionen vil i samarbejde med den højtstående repræsentant for udenrigsanliggender og medlemsstaterne:

- **styrke forbindelsesnetværkene og samarbejdet inden for rammerne af en Team Europe-tilgang**
- **fra 2025 oprette fælles operationelle hold og fusionscentre i tredjelande**

Europa-Parlamentet og Rådet opfordres til at:

- **afslutte forhandlingerne om revisionen af mekanismen til suspension af visumfritagelsen**

8. Konklusion

I en usikker verden er det nødvendigt at opgradere Unionens kapacitet til at foregribe, forebygge og reagere på sikkerhedstrusler.

Det er ikke nok kun at reagere på kriser, når de opstår. Vi er nødt til at skærpe vores opmærksomhed ved hjælp af et fuldstændigt billede af truslerne, efterhånden som de udvikler sig, og sikre, at vi med vores værktøjer og kapabiliteter kan løse opgaven.

Det omfattende sæt foranstaltninger, der er beskrevet i nærværende strategi, vil bidrage til at skabe en stærkere Union i verden: en Union, som er i stand til at foregribe, planlægge og imødekomme sine egne sikkerhedsbehov, som kan reagere effektivt på trusler mod dens indre sikkerhed og drage gerningsmænd til ansvar, og som beskytter sine åbne, frie og velstående samfund og demokratier.

Dette kræver, at vi ændrer vores holdning til den indre sikkerhed. Vi vil arbejde på at fremme en ny EU-sikkerhedskultur, hvor sikkerhedshensyn medtages i alle lovgivningsmæssige bestemmelser, politikker og programmer – fra udformning til gennemførelse – og hvor samarbejde på tværs af politikområder kan åbne op for nye perspektiver.

Dette er ikke kun en enkelt institutions, regerings eller aktørs opgave. Det er en opgave, som Europa skal løse i fællesskab.