



Bruxelles, den 9.12.2020
COM(2020) 797 final

**MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG
RÅDET**

Første statusrapport om strategien for EU's sikkerhedsunion

DA

DA

I INDLEDNING

Sikkerhed er noget af det, borgerne lægger størst vægt på, og den seneste tids terrorangreb på europæisk jord har yderligere understreget behovet for en indsats fra EU's side. Den 24. juli 2020 vedtog Kommissionen en **strategi for EU's sikkerhedsunion 2020-2025**¹ for at målrette indsatsen mod prioriterede områder, hvor EU kan tilføre nationale bestræbelser merværdi. Den bygger på de fremskridt, der tidligere er gjort under den europæiske dagsorden om sikkerhed 2015-2020², og skaber et nyt fokus for at sikre, at EU's sikkerhedspolitik afspejler det ændrede trusselsbillede, at den opbygger langsigtet, bæredygtig modstandsdygtighed, at den inddrager EU's institutioner og agenturer, regeringer, den private sektor og enkeltpersoner i en tilgang, der omfatter hele samfundet, og at den samler de mange politikområder med direkte indvirkning på sikkerheden. Det er centralt for indsatsen at sikre fuld overholdelse af de grundlæggende rettigheder, da sikkerheden i EU kun kan garanteres, når alle har tillid til, at deres grundlæggende rettigheder respekteres fuldt ud.

Truslen fra tværnationale terrornetværk er en levende påmindelse om, at der er behov for en koordineret EU-indsats for effektivt at beskytte europæerne og værne om vores fælles værdier og vores europæiske levevis. Dette er et symbol på, at der er opstået mere og mere komplekse grænseoverskridende og tværsektorielle sikkerhedstrusler, hvilket gør et tættere samarbejde om sikkerhed på alle niveauer stadig vigtigere. Dette gælder for organiseret kriminalitet og narkotikahandel — med det gælder også for den digitale verden, hvor cyberangreb og cyberkriminalitet fortsat er i fremmarch. Alle disse udfordringer gælder også uden for vores grænser med en klar sammenhæng mellem den indre og den ydre sikkerhed. Covid-19-krisen har også sat skarpt fokus på europæisk sikkerhed og har udfordret modstandsdygtigheden i Europas kritiske infrastruktur, kriseberejdskab, strategiske værdikæder og krisestyringssystemer samt vores samfunds modstandsdygtighed over for manipulerende indblanding og desinformation.

Strategien for sikkerhedsunionen består af fire strategiske indsatsområder på EU-plan: et fremtidssikret sikkerhedsmiljø, håndtering af foranderlige trusler, beskyttelse af Europa mod terrorisme og organiseret kriminalitet og et stærkt europæisk sikkerhedsøkosystem. Gennemførelsen er et centralt element i strategien, og dette er hovedtemaet for denne rapport: gennemførelse, som kræver, at de nationale myndigheder engagerer sig fuldt ud i frontlinjen for sikkerhed i EU. Denne rapport er den første gennemførelsesrapport under strategien og opfylder Kommissionens tilsagn om regelmæssigt at aflægge rapport om fremskridtene³. Den dækker perioden fra den 31. oktober 2019, hvor den seneste statusrapport om sikkerhedsunionen blev offentliggjort under Kommissionens tidligere mandat⁴.

II ET FREMTIDSSIKRET SIKKERHEDSMILJØ

1. *Beskyttelse af kritisk infrastruktur og modstandsdygtighed*

Borgernes dagligdag afhænger af en stadig mere indbyrdes forbundet og indbyrdes afhængig fysisk og digital infrastruktur. Denne infrastruktur er afgørende for økonomiens

¹ COM(2020) 605 final.

² COM(2016) 230 final.

³ Under høringen af næstformand Schinas i Europa-Parlamentet den 3. oktober 2019.

⁴ COM(2019) 552 final.

og samfundets funktion. Uden en pålidelig energiforsyning, forudsigelig transport, omfattende sundhedssystemer og et digitalt styret finansielt netværk ville vores nuværende levevis ikke være mulig. Covid-19-pandemien har endnu tydeligere vist vigtigheden af at **sikre modstandsdygtigheden i kritiske sektorer og hos kritiske operatører**. EU har anerkendt, at det er en fælles interesse at beskytte kritisk infrastruktur mod trusler, hvad enten der er tale om naturkatastrofer eller menneskeskabte katastrofer eller terrorangreb. Det nuværende trusselsbillede mod kritiske infrastrukturer er vidtgående. Det omfatter: terrorisme, hybride aktioner, cyberangreb, insider-hændelser, trusler i forbindelse med nye og fremspirende teknologier (såsom droner, 5G, kunstig intelligens), udfordringer i forbindelse med klimaændringer, afbrydelse af forsyningskæder og indblanding i valg. Vores nuværende regler skal moderniseres og udvides⁵. Fokus skal flyttes fra beskyttelse til modstandsdygtighed, der skal sikres bedre sammenhæng og konsekvens i den sektormæssige dækning, og der skal fokuseres på kritiske enheder, der leverer væsentlige tjenester.

Dette vil være målet for kommende forslag til fremme af **fysiske og digitale infrastrukturers** modstandsdygtighed. Det overordnede mål er at øge beredskabet på nationalt plan og EU-plan ved at opbygge robust kapacitet til at forebygge, detektere, reagere på og afbøde trusler og være parat til at handle i krisesituationer. Den eksisterende lovgivning har været i stand til at øge og forbedre risikostyringen i kritiske sektorer. Dette skal intensiveres. Et centralt mål for det reviderede direktiv om kritisk infrastruktur vil være at fremme et højt fælles niveau af modstandsdygtighed inden for et tilstrækkeligt antal nøglesektorer. På samme måde vil ajourføringen af direktivet om net- og informationssystemer (NIS) være rettet mod større ensartethed i medlemsstaternes identifikation af "operatører af væsentlige tjenester"⁶. Mere generelt er cybersikkerhedskapaciteten i medlemsstaterne stadig uensartet trods betydelige fremskridt, så revisionen vil søge at fremme mere cybersikkerhed overordnet set⁷. Resultatet bliver en større og mere sammenhængende tilgang til den fysiske og digitale infrastrukturens modstandsdygtighed.

Efterhånden som arbejdet skrider frem i retning af denne mere sammenhængende ramme, suppleres det af **sektorinitiativer**, der er rettet mod specifikke sårbarheder. De specifikke udfordringer i forbindelse med cybersikkerhed for energisektoren tages nu op på grundlag af Kommissionens henstilling fra 2019⁸, hvor der tages hensyn til sektorens karakteristika såsom realtidskrav, risikoen for kaskadevirkninger og kombinationen af nedarvede systemer og nye teknologier. Der arbejdes på en særlig netregel om cybersikkerhed for grænseoverskridende elektricitetsstrømme samt om beskyttelse af kritisk energiinfrastrukturens modstandsdygtighed og cybersikkerhed. Det tematiske netværk for beskyttelse af kritisk energiinfrastruktur blev også relanceret med et fornyet fokus og mål, og det mødtes for første gang i juni 2020 med over 100 onlinedeltagere. Dette netværk udgør en platform til fremme af grænseoverskridende samarbejde mellem operatører og ejere af kritisk energiinfrastruktur i energisektoren.

For at skabe et fælles udgangspunkt for medlemsstaternes samarbejde om **risikoberedskab i elsektoren** opstillede det europæiske net af transmissionssystemoperatører for elektricitet

⁵ Direktiv 2008/114/EF og direktiv (EU) 2016/1148.

⁶ COM(2019) 546 final. Kommissionen gennemførte også en offentlig høring (7. juli-2. oktober 2020) og landebesøg i alle medlemsstater med henblik på at kontrollere overensstemmelsen af direktivets gennemførelse på møder med operatører og nationale myndigheder.

⁷ COM(2019) 546 final.

⁸ C(2019) 2400.

i september 2020 de mest relevante regionale elkrisescenarier som fastsat i forordningen om risikoberedskab⁹. De omfatter cyberangreb samt pandemier og ekstreme vejrforhold. Medlemsstaterne vil udarbejde nationale krisescenarier og risikoberedskabsplaner for at forebygge og afbøde elkriser (de første udkast skal foreligge i april 2021). For at bidrage til denne proces blev der i juni 2020¹⁰ udsendt en række eksempler på god praksis baseret på en nøje overvågning af covid-19's indvirkning på energisektoren gennem koordinationsgrupperne for elektricitet, gas og olie samt Gruppen af Europæiske Nukleare Tilsynsmyndigheder og Den Europæiske Unions Myndighedsgruppe for Offshore Olie- og Gasaktiviteter.

Den stigende og sofistikerede afhængighed af digitale processer til levering af finansielle tjenesteydelser kræver også en styrkelse af cybersikkerheden i **den finansielle sektor**. Selv om IKT-systemernes sikkerhed anerkendes som en integreret del af risikostyringen for finansielle enheder, afspejles dette endnu ikke fuldt ud i EU's lovgivningsmæssige rammer for finansielle tjenesteydelser. Den 24. september 2020 vedtog Kommissionen sin strategipakke for digital finans¹¹ med det klare mål at tackle udfordringer og risici i forbindelse med den digitale omstilling, fremme modstandsdygtighed, databeskyttelse og passende tilsyn. Den omfattede et lovforslag om modstandsdygtighed i digitale operationer¹² for at sikre, at der er indført sikkerhedsforanstaltninger for at afbøde cyberangreb og andre risici¹³. Dette initiativ bidrager til en stærk og dynamisk europæisk digital finanssektor og øger dermed Europas evne til at styrke sin åbne strategiske autonomi inden for finansielle tjenesteydelser og dermed sin evne til at regulere og føre tilsyn med det finansielle system for at beskytte Europas finansielle stabilitet.

I forbindelse med større nødsituationer kræver den store indbyrdes afhængighed mellem sektorer og lande en koordineret indsats for at sikre en hurtig og effektiv indsats samt bedre forebyggelse og beredskab ved lignende situationer i fremtiden. I revisionen af afgørelsen om EU-civilbeskyttelsesmekanismen¹⁴ har Kommissionen foreslået¹⁵, at der opstilles **mål for modstandsdygtighed over for katastrofer** og **planlægning af modstandsdygtighed over for katastrofer** med øget fokus på at opbygge langsigtet tværsektoriel modstandsdygtighed over for grænseoverskridende katastrofer. Den foreslåede nye tilgang til opbygning af modstandsdygtighed supplerer arbejdet med katastroferisikostyring på nationalt plan. Den 26. november nåede Rådet til enighed om et forhandlingsmandat til styrkelse af forebyggelse, beredskab og indsats i tilfælde af katastrofer på grundlag af Kommissionens forslag af 2. juni 2020¹⁶.

Covid-19-pandemien har vist, hvordan en sundhedskrise indvirker på sikkerheden på EU-plan og globalt plan og understreget behovet for at optrappe beredskabs- og indsatsplanlægningen i forbindelse med epidemier og andre alvorlige grænseoverskridende sundhedstrusler. Kommissionens pakke af 11. november 2020 om "**Opbygning af en**

⁹ EUT L 158 af 14.6. 2019, s. 1.

¹⁰ Energy security: good practices to address pandemic risks (SWD(2020) 104).

¹¹ https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

¹² COM(2020) 595 final.

¹³ I forslaget fastlægges et sammenhængende referencepunkt for IKT-risikostyringskravene, indberetning af IKT-hændelser til finansielle tilsynsmyndigheder, digital afprøvning og informationsudveksling. Dertil kommer, at kritiske eksterne udbydere af IKT-tjenester i henhold til forslaget er underlagt en tilsynsramme på europæisk plan.

¹⁴ Afgørelse 1313/2013/EU af 17. december 2013 om en EU-civilbeskyttelsesmekanisme.

¹⁵ COM(2020) 220 final.

¹⁶ Forslag om ændring af afgørelse 1313/2013/EU om en EU-civilbeskyttelsesmekanisme — mandat til forhandlinger med Europa-Parlamentet.

europæisk sundhedsunion: Styrkelse af EU's modstandsdygtighed" fastsætter de næste skridt til at tackle grænseoverskridende sundhedstrusler. Den vil indføre en styrket ramme for grænseoverskridende samarbejde om alle sundhedstrusler og omfatter tre lovforslag: at opgradere lovgivningen om alvorlige grænseoverskridende sundhedstrusler og styrke Det Europæiske Center for Forebyggelse af og Kontrol med Sygdomme (ECDC) og Det Europæiske Lægemiddelagentur (EMA). Disse forslag vil tilsammen udgøre en solid og omkostningseffektiv ramme for at give EU og medlemsstaterne et mere sikkert grundlag, når de skal reagere på fremtidige sundhedskriser.

Et centralt element i beskyttelsen af centrale europæiske og nationale digitale aktiver går ud på at tilbyde kritiske infrastrukturer en kanal til **sikker kommunikation**. Dette understøttes af udviklingen af en netværksinfrastruktur for sikker og modstandsdygtig statslig satellitkommunikation som en del af EU's rumprogram.

2. Cybersikkerhed

Fordelene ved den digitale omstilling er tydelige, men det er også den kendsgerning, at den uundgåeligt ledsages af en stigning i potentielle sårbarheder¹⁷. Kritisk infrastruktur er ofte mål for stadig mere sofistikerede cyberangreb¹⁸. **Cybersikkerhed** skal derfor ikke kun være et anliggende for de politiske beslutningstagere, men for alle, der arbejder eller kommunikerer online.

For at øge tilliden til og sikkerheden ved digitale produkter, processer og tjenester blev der med forordningen om cybersikkerhed fra juni 2019 etableret **en EU-ramme for cybersikkerhedscertificering**.

Kommissionen har anmodet EU's Agentur for Cybersikkerhed, ENISA, om at udarbejde to ordninger for cybersikkerhedscertificering, og agenturet er godt i gang med udarbejdelsen. Dette arbejde omfatter også nationale cybersikkerhedscertificeringsmyndigheder, industrien, forbrugere, akkrediterings-, standardiserings- og certificeringsorganer samt Det Europæiske Databeskyttelsesråd.



¹⁷ ENISA [Threat Landscape 2020](#): Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.

¹⁸ Siden pandemien brød ud, har EU's agenturer og medlemsstaterne konstateret en betydelig stigning i antallet af cyberangreb, herunder mod sundhedssektoren.

En af disse ordninger er en **cloudtjenesteordning** til støtte for et sikkert og pålideligt marked for cloudtjenester. Dette er et centralt element i **EU's datastrategi**, der blev vedtaget i februar 2020¹⁹. Det vil skabe et fælles sikkerhedsgrundlag for cloudtjenester på tværs af sektorer, der bygger på den højeste fællesnævner for eksisterende (europæiske og internationale) standarder, ordninger og praksisser. Dette vil være et centralt element i den frie udveksling af data i hele EU²⁰. Ordningen vil også fremme indførelsen af cloudteknologier ved at give brugerne, navnlig små og mellemstore virksomheder og den offentlige forvaltning, en forståelig forsikring om sikkerhedsniveauet, når de bruger cloudtjenester.

Som fremhævet i strategien for sikkerhedsunionen kan konsekvenserne af systemiske og omfattende forstyrrelser være særligt alvorlige i betragtning af den igangværende udrulning af 5G-infrastrukturen i hele EU og mange kritiske tjenesters potentielle afhængighed af 5G-net. Dette har ført til en fælles indsats fra medlemsstaternes side med at udvikle og indføre passende sikkerhedsforanstaltninger. Efter Kommissionens henstilling om **cybersikkerhed i 5G-net** fra marts 2019²¹ gennemførte medlemsstaterne nationale risikovurderinger, der udmøntede sig i en koordineret EU-risikovurderingsrapport²², hvori man identificerede de sikkerhedsmæssige udfordringer i forbindelse med 5G-net. På grundlag af dette offentliggjorde NIS-samarbejdsgruppen²³ den 29. januar 2020 **EU's værktøjskasse med risikobegrænsende foranstaltninger**²⁴ med de nødvendige strategiske og tekniske foranstaltninger. Værktøjskassen omfatter foranstaltninger, der skal skærpe sikkerhedskravene til mobilnetoperatører, sikre mangfoldigheden af leverandører til individuelle mobilnetoperatører, vurdere leverandørernes risikoprofil og indføre restriktioner for leverandører, der anses for at udgøre en høj risiko. Kommissionen vil støtte indførelsen af værktøjskassen og udnytte de kompetencer og midler, den har til rådighed²⁵, herunder telekommunikations- og cybersikkerhedsregler, fuldt ud koordinering af standardisering og af EU-omfattende certificering og EU's ramme for direkte udenlandske investeringer²⁶.

NIS-samarbejdsgruppen offentliggjorde en statusrapport om gennemførelsen af foranstaltningerne i værktøjskassen i juli 2020²⁷. Heri bemærkede man, at et stort flertal af medlemsstaterne allerede har indført eller er i færd med at gennemføre de foranstaltninger, der anbefales i værktøjskassen. Foranstaltninger, hvor gennemførelsen var mindre fremskreden, omfattede afbødning af risikoen for afhængighed af højrisikoleverandører og udvikling af strategier for flere leverandører på både virksomhedsniveau og på nationalt plan.

¹⁹ COM(2020) 66 final.

²⁰ Forordning (EU) 2018/1807.

²¹ COM(2019) 2335.

²² Rapport om [EU's koordinerede risikovurdering af cybersikkerheden i 5G-net](#).

²³ NIS-samarbejdsgruppen blev oprettet for at sikre strategisk samarbejde og udveksling af oplysninger mellem EU-medlemsstaterne inden for cybersikkerhed.

²⁴ <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures>.

²⁵ COM(2020) 50 final.

²⁶ Forordning (EU) 2019/452. Den indeholder også eksplicite henvisninger til "kritisk infrastruktur" (samt "kritiske teknologier") mere generelt som "faktorer, som medlemsstaterne eller Kommissionen kan tage hensyn til", når de vurderer en investerings potentielle indvirkning.

²⁷ Rapport om [medlemsstaternes fremskridt med gennemførelsen af EU-værktøjskassen](#) om 5G-cybersikkerhed.

I løbet af de seneste måneder har EU-institutionerne og medlemsstaterne reageret på det øgede risikoniveau for cybersikkerhed, der er udløst af **covid-19-krisen**, ved at intensivere udvekslingen af oplysninger og øge beredskabet over for en potentiel cyberkrise. EU-samarbejdet blev intensiveret i vigtige fora (NIS-samarbejdsgruppen og netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)) samt gennem nye former for koordinerings- og informationsudvekslingsværktøjer²⁸. I september 2020 fremkom der endnu en skrivebordsundersøgelse på operationelt plan (Blue OLEx)²⁹, hvor medlemsstaternes forbindelsesnetværk af beredskabsorganisationer til cyberkriser (CyCLONe) også blev lanceret. Det skal stå for den videre gennemførelse af planen for hurtige reaktioner i forbindelse med omfattende grænseoverskridende cyberhændelser eller -kriser³⁰.

I det globale cyberspace stammer cyberangreb og -trusler ofte fra lande uden for EU. For effektivt at imødegå disse udfordringer samarbejder EU og medlemsstaterne om at fremme international sikkerhed og stabilitet i cyberspace, fremme ansvarlig adfærd hos stater, øge den globale modstandsdygtighed og øge bevidstheden om cybertrusler og ondsindede cyberaktiviteter, herunder hos internationale partnere³¹. Den 30. april 2020 offentliggjorde den højtstående repræsentant en erklæring på EU's vegne, hvori man fordømmer ondsindet adfærd i cyberspace og udtrykker solidaritet med ofrene³².

Den 30. juli 2020 vedtog Rådet **EU's første cybersanktioner nogensinde** mod seks enkeltpersoner og tre enheder, der var ansvarlige for eller involveret i cyberangreb. Disse omfatter forsøg på cyberangreb mod OPCW (Organisationen for Forbud mod Kemiske Våben) og cyberangreb, der er almindeligt kendt som "WannaCry", "NotPetya" og "Operation Cloud Hopper". Den 22. oktober 2020 indførte Rådet sanktioner over for yderligere to personer og en enhed, der var ansvarlig for eller involveret i cyberangrebet mod den tyske forbundsdag. Disse beslutninger blev truffet, efter at EU og medlemsstaterne løbende blev gjort opmærksom på behovet for at forebygge, modvirke, afskrække fra og reagere på ondsindede cyberaktiviteter, herunder ved at anvende sin ordning med cybersanktioner som en del af den cyberdiplomatiske værktøjskasse fra 2017³³.

²⁸ EU-institutioner og -organer samledes i en covid-19-cybertaskforce og indførte en ugentlig rapport om sektorspecifik situationsbevidsthed og analyse. ENISA og Europol iværksatte kampagner om, hvordan man kan bevare cybersikkerheden under covid-19. CERT-EU har udsendt en vejledning i, hvordan man opretter sikre VPN'er. I sommeren 2019 oprettede samarbejdsgruppen et nyt arbejdsområde for cybersikkerhed inden for sundhed, og Kommissionen og ENISA etablerede et EU-center for informationsudveksling og analyse på sundhedsområdet.

²⁹ <https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone>.

³⁰ C(2017) 6100.

³¹ EU fremmer den strategiske ramme for konfliktforebyggelse, stabilitet og samarbejde i cyberspace, herunder gennem sin deltagelse i FN's drøftelser om cyberspørgsmål. To vigtige processer er den åbne arbejdsgruppe om udviklingen inden for information og telekommunikation i forbindelse med international sikkerhed og gruppen af regeringseksperter (GGE) til at fremme ansvarlig statslig adfærd i cyberspace. Spørgsmålene omfatter virkningen af folkeretten, gennemførelsen af aftalte frivillige normer for ansvarlig statslig adfærd og tillidsskabende foranstaltninger samt udvikling af gennemførelsen gennem målrettet kapacitetsopbygning.

³² <https://www.consilium.europa.eu/da/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/>.

³³ Rådets afgørelse (FUSP) 2020/1127, 2020/1537 og 2020/651 som en del af 9916/17.

Der er også gjort fremskridt i forhandlingerne mellem medlovgiverne om nye eksportregler, der begrænser salget af cyberovervågningsudstyr til regimer rundt om i verden, der undertrykker menneskerettighederne³⁴. Når disse regler er vedtaget, vil de føre til en mere ansvarlig, konkurrencedygtig og gennemsigtig handel med produkter med dobbelt anvendelse³⁵. De foreslåede ændringer, der er nødvendige som følge af den teknologiske udvikling og de voksende sikkerhedsrisici, omfatter nye kriterier for udstedelse af eller afslag på eksportlicenser til visse produkter.

3. Beskyttelse af det offentlige rum

Som det anerkendes i EU's dagsorden for terrorbekæmpelse³⁶, er beskyttelse af offentlige steder gennem opbygning af modstandsdygtighed over for sikkerhedstrusler fortsat et afgørende element i arbejdet hen imod en effektiv og ægte sikkerhedsunion. Kommissionen arbejder sammen med en bred vifte af offentlige og private interessenter om at udvikle vejledning og yde praktisk støtte og finansiering³⁷ i overensstemmelse med **handlingsplanen fra 2017 til støtte for beskyttelsen af offentlige steder**³⁸ og eksemplerne på god praksis til støtte for beskyttelsen af offentlige steder fra 2019³⁹. Som fastsat i EU's dagsorden for terrorbekæmpelse vil Kommissionen intensivere sin støtte til de lokale og regionale myndigheder, der spiller en central rolle i beskyttelsen af det offentlige rum og i forebyggelsen af radikaliserings. Dette vil omfatte udarbejdelse af en EU-protokol om sikkerhed og modstandsdygtighed for byer, der fastsætter grundlæggende principper og mål for de lokale myndigheder i disse områder.

Eftersom terrorangrebene i stigende grad har været rettet mod **religiøse samlingssteder**, lægges der særlig vægt på samarbejde mellem offentlige myndigheder og ledere af trossamfund og trossamfundene for at øge bevidstheden om sikkerhed og hjælpe med at gennemføre god praksis og uddannelse på religiøse samlingssteder. Enkle foranstaltninger kan betyde forskellen mellem liv og død. I oktober 2019 blev en synagoge i Halle udsat for et terrorangreb. En forstærket dør, en panikknop og sikkerhedskameraer bidrog til at redde liv.

For yderligere at støtte øget sikkerhed i det offentlige rum, navnlig på religiøse samlingssteder, har Kommissionen i 2020 stillet 20 mio. EUR til rådighed for projekter, der ledes af interessenter.

Kommissionen arbejder også på at imødegå **nye risici for det offentlige rum**, herunder **ubemandede luftfartøjssystemer** (UAS). Droner skaber store økonomiske og beskæftigelsesmæssige muligheder, men de udgør også en betydelig risiko for offentlige rum, kritisk infrastruktur og andre følsomme områder såsom fængsler. De seneste EU-regler⁴⁰ på dette område afbøder denne risiko ved at øge sikkerheden i forbindelse med

³⁴ COM(2016) 616 final. Kommissionens forslag tager sigte på at ændre og omarbejde forordning (EF) nr. 428/2009 om en fællesskabsordning for kontrol med udførsel, overførsel, mæglervirksomhed og transit i forbindelse med dobbelt anvendelse.

³⁵ Der er tale om en omfattende gruppe af varer, materialer, software og teknologi, som kan anvendes til både civile og militære formål.

³⁶ COM(2020) 795 final.

³⁷ Indkaldelsen [ISF Protect](#) fra 2019 omfattede "Secu4All" med udvikling af en omfattende uddannelsescyklus for lokale myndigheder for at give borgerne et sikkert bymiljø og "DroneWISE" for at styrke beredskabet hos førsteresponsenheder til at imødegå fjendtlige ubemandede luftfartøjer. I 2020 gennemføres der en ny indkaldelse på 12 mio. EUR vedrørende beskyttelse af offentlige steder.

³⁸ COM(2017) 612 final.

³⁹ SWD(2019) 140 final.

⁴⁰ Kommissionens gennemførelsesforordning (EU) 2019/947.

droneoperationer. Fra januar 2021 vil droneoperatører også skulle lade sig registrere hos de nationale myndigheder. Denne ordning kan suppleres af en **lovramme for U-space**, Europas trafikstyringssystem for ubemandede flyvninger⁴¹, for at garantere mere sikre droneoperationer. Tilsammen vil disse skridt gøre det vanskeligere for enkeltpersoner at flyve med droner i områder med adgangsbegrænsning og bidrage til at identificere og retsforfølge lovovertrædere.

Kommissionen arbejder også på at støtte retshåndhævelse, operatører af kritisk infrastruktur, arrangører af større begivenheder og andre interessenter med henblik på at bekæmpe ikke-samarbejdsbaseret brug af droner, f.eks. ved at samarbejde med Den Europæiske Unions Luftfartssikkerhedsagentur om at udvikle **god praksis for at hjælpe lufthavnenes interessenter** med at reagere på uautoriserede dronehændelser, fremme en mere harmoniseret **indsats for at afprøve modforanstaltninger** i hele EU og udarbejde en praktisk håndbog for interessenter med fokus på bymæssige forhold.

EU's digitale efterårshøjskole for beskyttelse af offentlige steder, der blev afholdt af Kommissionens Fælles Forskningscenter i oktober 2020, samlede mere end 200 byplanlæggere og offentlige og private operatører af offentlige steder. Ved sessionerne behandlede man en lang række emner, f.eks. hvordan man beskytter mod eksplosioner og angreb med køretøjer, afbødning af de trusler, som fjendtlige droner udgør i byområder, og brugen af overvågnings- og detektionsteknologier.

Kommissionen har også fortsat aktivt støttet **partnerskabet for sikkerhed i offentlige rum**, der blev lanceret i januar 2019 som led i EU's dagsorden for byerne, og som har offentliggjort sin nye handlingsplan⁴² til håndtering af sikkerheden i byområder på forskellige forvaltningsniveauer. Tiltagene omfatter etablering af en ramme for et selvevalueringsværktøj, anbefalinger til politikudformning, flerniveaustyring og finansiering, innovation gennem intelligente løsninger og teknologier, herunder begrebet indbygget sikkerhed, forebyggelse og social inklusion. Partnerskabet vil nu gå ind i gennemførelsesfasen.

Der blev også ydet støtte til forbedring af sikkerheden i offentlige rum på lokalt plan gennem den fjerde indkaldelse af nyskabende aktioner i byerne. Tre byer er blevet udvalgt og afprøver nye løsninger på sikkerhedsområdet i byer (Piræus i Grækenland, Tammerfors i Finland og Torino i Italien) ved hjælp af midler fra Den Europæiske Fond for Regionaludvikling.

⁴¹ Kommissionen kan i den forbindelse fremlægge en gennemførelsesforordning, som vil blive vedtaget i henhold til en undersøgelsesprocedure med deltagelse af Udvalget for Luftfartssikkerhed.

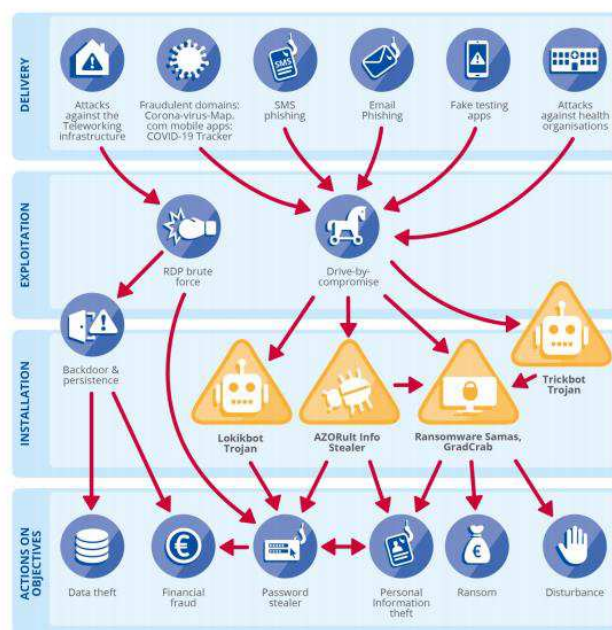
⁴² Handlingsplanen er blevet vedtaget og findes på Futurium: <https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0>.

På indsatssiden har Kommissionen også udviklet en europæisk ramme for at forbedre beredskabet og indsatsen i forbindelse med ulykker med masseforbrændinger, hvor man udnytter den samlede europæiske kapacitet til at behandle patienter gennem samarbejde på EU-plan. EU-civilbeskyttelsesmekanismen kan anvendes til at støtte et stort antal patienter med alvorlige forbrændinger ved at give adgang til senge til brandsårspatienter i specialiserede behandlingscentre, eksperter i vurdering af forbrændinger og medicinsk evakueringskapacitet.

III HÅNTERING AF SKIFTENDE TRUSLER

1. Cyberkriminalitet

Mangler i cybersikkerheden udnyttes ofte af kriminelle. Dette har været tydeligere end nogensinde under covid-19-krisen. Der har været en stigning i "klassisk" cyberkriminalitet ved brug af malware og ransomware (dvs. til at stjæle personoplysninger og betalingsdata eller til afpresning af ofre), og der er dukket mange nye websteder op, der lokker brugerne til at installere malware. Der er forekommet cyberangreb på sundheds- og forskningsinfrastruktur, hvor IKT-systemer er blevet blokeret og kun kan låses op igen mod betaling af løsepenge eller adgang til oplysninger om vaccineudvikling⁴³. Der er også konstateret en betydelig stigning i seksuelt misbrug af børn og materiale med seksuelt misbrug af børn⁴⁴.



En effektiv reaktion på IT-kriminalitet kræver en stærk ramme for strafferetlig efterforskning og retsforfølgning, og et vigtigt første skridt er fuld omsætning og gennemførelse af direktivet om **angreb på informationssystemer**⁴⁵. Kommissionen overvåger Bulgariens, Italiens, Portugals og Sloveniens foranstaltninger efter at have indledt traktatbrudssager i 2019. Der er også behov for fremskridt med hensyn til gennemførelsen af **direktivet fra 2011 om bekæmpelse af seksuelt misbrug af børn**⁴⁶. De områder, hvor der stadig er behov for en indsats, omfatter forebyggelse, materiel

⁴³ Internet Organised Crime Threat Assessment (IOCTA) 2020, oktober 2020.

⁴⁴ Report on Exploiting isolation: [Offenders and victims of online child sexual abuse during the COVID-19 pandemic](#), Europol, 19.06.2020.

⁴⁵ Direktiv 2013/40/EU.

⁴⁶ Direktiv 2011/93/EU.

strafferet, bistand, støtte og beskyttelsesforanstaltninger for børneofre. Siden 2018 har Kommissionen indledt traktatbrudsprocedurer mod 25 medlemsstater⁴⁷.

Den 24. juli 2020 vedtog Kommissionen en **EU-strategi for en mere effektiv bekæmpelse af seksuelt misbrug af børn**⁴⁸, som har til formål at sikre en effektiv EU-indsats mod seksuelt misbrug af børn. Der er også opstået en særlig udfordring, da visse onlinekommunikationstjenester, såsom webmail eller meddelelsetjenester, fra den 21. december 2020 vil være omfattet af e-data-direktivet, og de er omfattet af de reviderede definitioner i den europæiske kodeks for elektronisk kommunikation. Som følge heraf er der en klar risiko for, at udbydere af disse tjenester, der udfører visse vigtige frivillige aktiviteter med henblik på at opdage, tackle og indberette seksuelt misbrug af børn online i dag, vil være nødt til at ophøre med det. Kommissionen har derfor foreslået en **forordning**⁴⁹, der giver mulighed for, at disse frivillige aktiviteter kan fortsætte på visse betingelser, indtil der foreligger en langsigtet lovgivningsmæssig løsning. Kommissionen arbejder på et forslag til en sådan løsning, som forventes vedtaget i 2021.

Det europæiske netværk af cybersikkerhedscentre og kompetencecentre for innovation og operationer har oprettet en **covid-19-cyberforsvarsalliance** for at udvikle innovative tilgange til at bekæmpe covid-19-relateret kriminalitet. I april 2020 blev der oprettet en særlig EIC-COVID-plattform⁵⁰ for at skabe forbindelse mellem civilsamfundet, innovatorer, partnere og investorer i hele Europa med henblik på at udvikle innovative løsninger.

For at sikre en mere effektiv retsforfølgning af forbrydelser og i betragtning af betydningen af elektroniske oplysninger og bevismateriale i strafferetlige efterforskninger bør de retshåndhævende og retslige myndigheder hurtigt få adgang til sådanne oplysninger og beviser med henblik på deres strafferetlige efterforskning. Dette blev anerkendt i den fælles erklæring fra EU's indenrigsministre af 13. november 2020⁵¹. Europol, Eurojust og Det Europæiske Retlige Netværk offentliggjorde den 1. december 2020 deres anden "SIRIUS EU Digital Evidence Situation Report" (SIRIUS-situationsrapport om digitalt bevismateriale i EU). I rapporten fremhæves den øgede relevans af elektronisk bevismateriale i strafferetlige efterforskninger⁵². Med hensyn til Kommissionens forslag om **grænseoverskridende adgang til elektronisk bevismateriale**⁵³ fra april 2018 har Europa-Parlamentet endnu ikke fastlagt sin holdning, og forhandlingerne mellem medlovgiverne er derfor endnu ikke gået i gang. Forsinkelser i vedtagelsen af disse forslag hæmmer de retshåndhævende og retslige myndigheders arbejde og besværliggør de

⁴⁷ Spanien, Portugal, Italien, Nederlandene, Sverige, Malta, Litauen, Slovakiet, Bulgarien, Rumænien, Tyskland, Østrig, Belgien, Tjekkiet, Estland, Grækenland, Finland, Frankrig, Kroatien, Ungarn, Irland, Luxembourg, Letland, Polen, Slovenien.

⁴⁸ COM(2020) 607 final.

⁴⁹ COM(2020) 568 final.

⁵⁰ Kommissionen var sammen med Det Europæiske Innovationsråd og medlemsstaterne vært for et paneuropæisk EUvsVirus Hackathon + Matchathon <https://covid-eic.easme-web.eu/>.

⁵¹ Fælles erklæring fra EU's indenrigsministre om de seneste terrorangreb i Europa, 13.11.2020, 12634/20.

⁵² Ifølge rapporten steg antallet af grænseoverskridende anmodninger, som EU-myndighederne indgav til onlinetjenesteudbydere, betydeligt i 2019, og langt de fleste af dem kom fra Tyskland (37,7 % af anmodningerne), Frankrig (17,9 %) og Det Forenede Kongerige (16,4 %). Antallet af anmodninger om adgang til elektroniske data steg til det dobbelte i Polen og næsten til det tredobbelte i Finland. Desuden steg antallet af anmodninger om oplysninger i nødsituationer med næsten 50 % på et år.

⁵³ COM/2018/226 og COM/2018/225.

igangværende bestræbelser på at fastlægge kompatible regler for grænseoverskridende adgang til elektronisk bevismateriale gennem internationale forhandlinger⁵⁴.

På internationalt plan deltager Kommissionen på EU's vegne i de igangværende forhandlinger om anden tillægsprotokol til Europarådets **Budapestkonvention om IT-kriminalitet**. Denne protokol vil give de kompetente retshåndhævende myndigheder udvidede og vidtrækkende redskaber til grænseoverskridende samarbejde om efterforskning og retsforfølgning af cyberkriminalitet og andre alvorlige former for kriminalitet, herunder direkte samarbejde med tjenesteudbydere. Da de fleste af disse forbedrede og styrkede samarbejdsmetoder vil afhænge af udveksling af personoplysninger, er det afgørende, at den fremtidige protokol indeholder passende databeskyttelsesgarantier, ikke kun ud fra et perspektiv om grundlæggende rettigheder, men også for at garantere retssikkerhed, gensidig tillid og et effektivt operationelt retshåndhævelsessamarbejde.

Forhandlingerne forventes afsluttet i 2021. Sideløbende med det mandat, som RIA-Rådet fik sidste år, forhandler Kommissionen om en **aftale mellem EU og USA om grænseoverskridende adgang til elektronisk bevismateriale**. Den skal supplere de foreslåede interne EU-regler for direkte grænseoverskridende samarbejde med tjenesteudbydere ved at fjerne lovkonflikter og fastsætte fælles regler og garantier. Der blev indledt formelle forhandlinger den 25. september 2019, og der har allerede været afholdt flere forhandlingsrunder. Resultatet af forhandlingerne afhænger imidlertid i høj grad af, hvilke fremskridt der gøres med de interne regler om elektronisk bevismateriale.

Med hensyn til **lagring og anvendelse af data til retshåndhævelsesformål** blev den tidligere Tele2/Watson-dom⁵⁵ fra 2016 fulgt op af Kommissionen gennem eksperthøringer med relevante tjenesteudbydere, politi og retslige myndigheder, civilsamfundet, databeskyttelsesmyndigheder, den akademiske verden og EU-agenturer. Overvejelserne blev også inspireret af en undersøgelse af datalagringspraksis hos udbydere af elektroniske kommunikationstjenester og de retshåndhævende myndigheders behov og praksis med hensyn til adgang til data, identifikation af relevante teknologiske udfordringer og en oversigt over de nationale retlige rammer⁵⁶. Dette arbejde har understreget behovet for, at de retshåndhævende myndigheder får adgang til data for at kunne udføre deres opgaver mere effektivt.

Den 6. oktober 2020 afsagde Domstolen domme⁵⁷ vedrørende Belgiens, Frankrigs og Det Forenede Kongeriges nationale lovgivning om lagring og overførsel af samt adgang til andre kommunikationsdata end indholdsdata med henblik på retshåndhævelse og national sikkerhed. Kommissionen vil vurdere de muligheder, der er til rådighed for at sikre, at terrorister og andre kriminelle kan identificeres og spores, samtidig med at EU-retten som

⁵⁴ F.eks. vedtog FN's Generalforsamling den 27. december 2019 resolution 74/247 om bekæmpelse af brug af informations- og kommunikationsteknologi til kriminelle formål og nedsatte et stående mellemstatsligt ad hoc-ekspertudvalg, der fik til opgave at udarbejde en omfattende international konvention om cyberkriminalitet. EU støtter ikke oprettelsen af et nyt internationalt retligt instrument om cyberkriminalitet, da Budapestkonventionen om IT-kriminalitet allerede indeholder en omfattende multilateral retlig ramme. I juli 2020 blev FN's medlemsstater enige om at udsætte de første skridt: EU bidrog til processen på grundlag af en fælles holdning (doc.7677/2/20).

⁵⁵ Dom af 21. december 2016 i forenede sager C-203/15 og C-698/15, Tele2 Sverige AB og Watson m.fl.

⁵⁶ <https://data.europa.eu/doi10.2837/26288>

⁵⁷ Dom i sag C-623/17, Privacy International, og i forenede sager C-511/18, La Quadrature du Net m.fl., C-512/18, France Data Network m.fl., og C-520/18, Ordre des barreaux francophones et germanophone m.fl.

fortolket af Domstolen overholdes, også under hensyntagen til andre sager, der verserer for Domstolen om dette emne.

Et andet vigtigt element i bekæmpelsen af cyberkriminalitet har været arbejdet med at sikre tilgængeligheden og nøjagtigheden af data fra registrering af domænenavne på internettet ("**WHOIS-oplysninger**") i overensstemmelse med de bestræbelser, som Internet Corporation for Assigned Names and Numbers (ICANN) har udfoldet. Drøftelserne har til formål at sikre, at enheder, der legitimt anmoder om adgang, herunder retshåndhævende myndigheder og cybersikkerhedsoperatører, får effektiv adgang til generiske topdomæneregistreringsdata under fuld overholdelse af gældende databeskyttelsesregler. De endelige anbefalinger til en ny WHOIS-politik blev offentliggjort den 10. august 2020 og er i øjeblikket ved at blive revideret, inden ICANN's bestyrelse træffer afgørelse. Kommissionen vil undersøge konklusionerne af revisionen og overveje, hvorvidt de i tilstrækkelig grad afspejler databeskyttelse og hensynet til offentlighedens interesse med at sikre effektiv adgang for retshåndhævende myndigheder og cybersikkerhedsoperatører.

2. *Moderne retshåndhævelse*

Da teknologien fortsætter med at forandre næsten alle sektorer, herunder sikkerhed, skal de retshåndhævende myndigheder og retsvæsenet være i stand til at holde trit. Det er vigtigt at integrere kunstig intelligens, big data og højtydende databehandling i sikkerhedspolitikken uden at svække den effektive beskyttelse af de grundlæggende rettigheder for at øge sikkerheden.

Kommissionen er aktiv på en række centrale arbejdsområder⁵⁸. Den 25. november 2020 foreslog Kommissionen⁵⁹ forordningen om datastyring, en ramme for lettere udveksling og videreanvendelse af personoplysninger og andre data end personoplysninger til innovations- og udviklingsformål. Dette omfatter industrien og offentlige organer via virtuelle eller fysiske sektorspecifikke dataområder. Det vil give de nationale retshåndhævende myndigheder adgang til data, der befinder sig i andre dataområder, med henblik på deres egne innovationsformål. Samtidig vil det ikke være tilladt at få adgang til oplysninger, som de nationale retshåndhævende myndigheder og sikkerhedsmyndigheder er i besiddelse af, medmindre det er tilladt i henhold til EU-retten eller national ret. De nationale retshåndhævende sikkerhedsmyndigheder kan også drage fordel af, at individuelle registrerede frivilligt stiller deres oplysninger til rådighed for almenvellet udelukkende med henblik på videnskabelig forskning.

Der arbejdes også på udarbejdelsen af et nyt initiativ om **kunstig intelligens** (AI) efter offentliggørelsen af hvidbogen om kunstig intelligens⁶⁰. Samtidig med at hvidbogen anerkender de muligheder, som kunstig intelligens giver for at øge sikkerheden og velfærden for borgerne og samfundet som helhed, identificerer den også en række risici — såsom cybertrusler, personlige sikkerhedsrisici og tab af konnektivitet. I den offentlige høring drejede deltagerens største bekymringer sig om muligheden for, at kunstig intelligens krænker de grundlæggende rettigheder, og risikoen for, at kunstig intelligens kan føre til diskriminerende resultater⁶¹. I meddelelsen om opbygning af tillid til menneskecentreret kunstig intelligens⁶² understregede Kommissionen behovet for at gøre

⁵⁸ Herunder EU's datastrategi (se ovenfor).

⁵⁹ COM(2020) 767 final.

⁶⁰ COM(2020) 65 final.

⁶¹ Henholdsvis 90 % og 87 % af respondenterne mener, at disse bekymringer er vigtige eller meget vigtige.

⁶² COM(2019) 168.

AI-systemer modstandsdygtige over for både åbenlyse angreb og mere subtile forsøg på at manipulere data eller algoritmer og for at tage skridt til at mindske denne risiko.

Kryptering spiller en grundlæggende rolle med hensyn til at garantere en stærk cybersikkerhed og effektiv beskyttelse af grundlæggende rettigheder, såsom privatlivets fred, herunder kommunikationshemmelighed, beskyttelse af personoplysninger og sikring af tillid til tjenester og produkter baseret på krypteringsteknologier, såsom digitale identitetsløsninger. Samtidig kan kryptering også bruges til at skjule kriminalitet fra retshåndhævende og dømmende myndigheder, hvilket gør det vanskeligt at efterforske, afsløre og retsforfølge kriminalitet. Medlemsstaterne i Rådet har opfordret til løsninger, der gør det muligt for de retshåndhævende og retslige myndigheder at få lovlig adgang til digitalt bevismateriale under fuld respekt for privatlivets fred, databeskyttelse og garantier for en retfærdig rettergang⁶³. Kommissionen vil samarbejde med medlemsstaterne om at finde juridiske, operationelle og tekniske løsninger vedrørende lovlig adgang til elektroniske oplysninger i krypterede miljøer, som opretholder kommunikationssikkerheden.

De praktiske skridt, der er på vej, omfatter en **dekrypteringsplatform** i Europol, der skal hjælpe de retshåndhævende myndigheder med at få lovlig adgang til krypterede oplysninger på enheder, der beslaglægges i forbindelse med strafferetlige efterforskninger⁶⁴. Den europæiske uddannelsesgruppe vedrørende IT-kriminalitet har udviklet pilotuddannelsesmoduler, som vil indgå i arbejdet i Agenturet for Uddannelse inden for Retshåndhævelse (CEPOL). Der er oprettet et netværk af medlemsstaternes krypteringsekspertisecentre, der skal udveksle bedste praksis og ekspertise og støtte udviklingen af en værktøjskasse med tekniske og praktiske instrumenter.

Det **digitale udvekslingssystem for elektronisk bevismateriale (eEDES)** vil udgøre et redskab til sikker, hurtig og effektiv grænseoverskridende udveksling af europæiske efterforskningskendelser, anmodninger om gensidig bistand og dokumentation i digitalt format. Det bør gradvist udbygges og udvides til andre instrumenter for retligt samarbejde i straffesager, og dets fremtidige anvendelsesområde vil blive fastlagt i et lovforslag om digitalisering af de retlige samarbejdsprocedurer, der er planlagt til 2021⁶⁵.

3. Bekæmpelse af terrorrelateret indhold på nettet

Radikalisering, der fører til voldelig ekstremisme og terrorisme, er et flerdimensionelt og grænseoverskridende fænomen, der har været i stand til at udnytte internettets hastige vækst. Internettet bruges fortsat til at radikalisere og rekruttere sårbare personer. I juli fjernede Europols internetindberetningsenhed 2 000 links til terrorrelateret indhold — herunder manualer og vejledninger om, hvordan et angreb skal udføres. Dokumentationen for internettets rolle med hensyn til at radikalisere og reklamere for forbrydelser begået af dem, der var involveret i angreb i Frankrig og Østrig, understreger yderligere behovet for en klar juridisk ramme for at forhindre udbredelsen af terrorrelateret onlineindhold, samtidig med at der opretholdes effektive garantier for beskyttelse af de grundlæggende rettigheder. Forhandlingerne mellem Europa-Parlamentet og Rådet om den foreslåede **forordning om terrorrelateret onlineindhold**⁶⁶ er blevet intensiveret i de seneste uger. Afslutningen af disse forhandlinger med oprettelsen af navnlig det nye og effektive

⁶³ ST 13084 2020 — Rådets resolution om kryptering — Sikkerhed ved hjælp af kryptering og på trods heraf.

⁶⁴ Dette projekt til 6 mio. EUR støttes også af Kommissionens Fælles Forskningscenter.

⁶⁵ Meddelelse om digitalisering af retsvæsenet i EU, COM(2020) 710 af 2. december 2020.

⁶⁶ COM(2018) 640 final.

operationelle instrument til påbud om fjernelse på tværs af grænserne af terrorrelateret indhold inden for en time eller mindre fra modtagelsen af disse påbud er afgørende for at kunne håndtere terrorrelateret indhold, herunder indhold, der bidrager til radikaliserings.

I mellemtiden fungerer **EU's internetforum** fortsat som en katalysator for handling og udgør en vigtig platform, der samler medlemsstaterne og erhvervslivet for at forhindre udbredelsen af terrorrelateret onlineindhold og bekæmpe radikaliseringsbudskaber. Forummet arbejder på at udarbejde en referenceliste over forbudte symboler og grupper i medlemsstaterne, som kan udgøre grundlaget for platformens politikker for indholdsmoderation.

EU's internetforum har udvidet sit aktivitetsområde til også at omfatte **seksuelt misbrug af børn på internettet**. Forummet vil skabe et fælles rum til udveksling af bedste praksis og kortlægning af hindringer, som både private og offentlige aktører står over for, for at øge den gensidige forståelse og finde frem til løsninger i fællesskab. Det giver også mulighed for politisk koordinering på højt plan for at maksimere effekten og effektiviteten af indsatsen. Der blev etableret en teknisk ekspertproces under EU's internetforum bestående af eksperter fra den akademiske verden, industrien, offentlige myndigheder og civilsamfundsorganisationer med henblik på at afsløre og foretage en foreløbig vurdering af mulige tekniske løsninger til at opdage og indberette seksuelt misbrug af børn i end-to-end-krypteret elektronisk kommunikation. Sådanne tekniske løsninger bør ikke svække krypteringen. Denne tilgang supplerer andre elementer i bekæmpelsen af seksuelt misbrug af børn, både online og offline, som beskrevet ovenfor.

Kommissionen er også fortsat med at dele EU's ekspertise og erfaringer som en del af det uafhængige rådgivende udvalg under det nyligt oprettede **Global Internet Forum to Counter Terrorism (globalt internetforum til bekæmpelse af terrorisme)** og som en del af ledelsen af arbejdsgruppen for kriseberedskab sammen med Microsoft. Sammen med Europol fortsatte Kommissionen med at støtte medlemsstaterne i gennemførelsen af **EU's kriseprotokol**. EU's internetindberetningsenhed var vært for endnu en skrivebordsøvelse den 23. november 2020 med henblik på at udarbejde retningslinjer for at forbedre de operationelle svar og koordineringen i realtid mellem medlemsstaterne og onlinetjenesteudbydere.

I juni 2020 offentliggjorde Kommissionen resultaterne af den seneste overvågning af gennemførelsen af **adfærdskodeksen for bekæmpelse af ulovlig hadefuld tale på internettet**⁶⁷. Den viste, at IT-virksomheder i gennemsnit vurderer 90 % af det markerede indhold inden for 24 timer og fjerner 71 % af det indhold, der anses for at være ulovlig hadefuld tale. Den identificerede imidlertid også mangler med hensyn til gennemsigtighed og feedback til brugerne. Gennemførelsen af adfærdskodeksen i de seneste fire år har også bidraget til overvejelserne om, hvordan ulovligt indhold på nettet skal bekæmpes, samtidig med at ytringsfriheden beskyttes i det kommende forslag til en retsakt om digitale tjenester. I talen om Unionens tilstand 2020 meddelte Ursula von der Leyen også, at Kommissionen inden udgangen af 2021 vil foreslå en udvidelse af listen over forbrydelser på EU-plan i henhold til artikel 83, stk. 1, i TEUF til også at omfatte hadforbrydelser og hadefuld tale⁶⁸.

4. *Hybride trusler*

⁶⁷ https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

⁶⁸ Også nærmere beskrevet i strategi for ligestilling af LGBTIQ-personer 2020-2025 (COM(2020) 698).

I erkendelse af, at de hybride trusler udvikler sig, nedsatte Rådet i juli 2019 **Den Horisontale Gruppe vedrørende Styrkelse af Modstandsdygtighed og Imødegåelse af Hybride Trusler**. Hovedformålet er at støtte strategisk og horisontal koordinering mellem medlemsstaterne vedrørende statens og samfundets modstandsdygtighed, forbedre den strategiske kommunikation og bekæmpe desinformation. Arbejdet har omfattet opfølgning på undersøgelser af hybride risici⁶⁹ med specifikt fokus på hybride trusler og desinformation i naboskabspartnerlande. Den Horisontale Gruppens aktiviteter er blevet præsenteret i en årsberetning, der blev vedtaget den 14. september 2020.

I december 2019 vedtog Rådet "Konklusioner om supplerende tiltag til at styrke modstandsdygtigheden og imødegå hybride trusler"⁷⁰, hvori det opfordrede til en samlet tilgang til sikkerhed og til imødegåelse af hybride trusler, idet man arbejder på tværs af alle relevante politikområder på en mere strategisk, koordineret og sammenhængende måde. To vigtige opfølgende skridt blev taget i juli 2020. Først udarbejdede Kommissionens tjenestegrene og EU-Udenrigstjenesten en **kortlægning af foranstaltninger og dokumenter vedrørende EU's reaktion på hybride trusler**⁷¹. Kortlægningen giver en samlet oversigt over imødegåelse af hybride trusselsrelaterede foranstaltninger på EU-plan og tilsvarende politikdokumenter. Den tjener som udgangspunkt for at skabe en begrænset onlineplatform som kvikskranke for alle hybride trusselsrelaterede foranstaltninger, politiske og lovgivningsmæssige dokumenter samt relevante undersøgelser. For det andet blev der i den seneste **årsrapport om imødegåelse af hybride trusler**⁷² set på gennemførelsen, der omfatter situationsbevidsthed, opbygning af modstandsdygtighed, beredskab og kriserespons samt internationalt samarbejde og navnlig samarbejdet mellem EU og NATO om imødegåelse af hybride trusler. Selv om der i rapporten gøres opmærksom på visse fremskridt med hensyn til koordinering på EU-plan, kræver det hidtil usete omfang og mangfoldigheden af hybride trusler i dag yderligere skridt på EU-plan for at integrere den eksterne og interne dimension i en uhindret strøm og støtte medlemsstaternes bestræbelser på at imødegå hybride trusler og styrke deres modstandsdygtighed.

Sideløbende hermed arbejdes der på at gennemføre de foranstaltninger, der er fastlagt i den nye sikkerhedsstrategi, med henblik på at integrere hybride overvejelser i politikudformningen, udvikle en onlineplatform med adgangsbegrænsning, etablere sektorspecifikke EU-referencescenarier for modstandsdygtighed samt strømline informationsstrømmene for yderligere at øge situationsbevidstheden⁷³. Dette bygger på **EU's analyseenhed for hybride trusler** (HFC), der er oprettet inden for rammerne af EU's Efterretnings- og Situationscenter (EU INTCEN), som fortsat er EU's vigtigste kontaktpunkt for vurderinger af hybride trusler. Det har nu udarbejdet mere end 180 skriftlige rapporter om hybride trusler og cybertrusler. Et af HFC-projekterne er **analysen**

⁶⁹ Foranstaltning 1 i den fælles ramme for imødegåelse af hybride trusler fra 2016, se JOIN/2016/018.

⁷⁰ Rådets konklusioner 14972/19.

⁷¹ SWD(2020) 152, fælles arbejdsdokument fra Kommissionens tjenestegrene, Kortlægning af foranstaltninger vedrørende styrkelse af modstandsdygtigheden og imødegåelse af hybride trusler.

⁷² SWD(2020) 153, fælles arbejdsdokument fra Kommissionens tjenestegrene, Rapport om gennemførelsen af den fælles meddelelse af 2016 om imødegåelse af hybride trusler fra 2016 og den fælles meddelelse af 2018 om øget modstandsdygtighed og bedre kapacitet til at imødegå hybride trusler.

⁷³ F.eks. foreslog Det Fælles Forskningscenter den 26. november 2020 en ny ramme for at øge bevidstheden om trusler: <https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats>.

af hybride tendenser⁷⁴, der leverer data om emner som f.eks.: tilbagevendende analyser af nye aktørers hybride aktiviteter, udenlandske efterretningsaktiviteter mod EU's medlemsstater, institutioner, partnere og interesser og hybride statslige og ikkestatslige aktører, der udnytter covid-19-pandemien.

Samarbejdet mellem EU og NATO (inden for rammerne af de fælles erklæringer fra Warszawa og Bruxelles fra 2016 og 2018) er blevet yderligere intensiveret som fremhævet i den femte fremskridtsrapport fra juni 2020 med samspil mellem personale og konkrete resultater inden for hybride trusler, cyberforsvar og kapacitetsopbygning⁷⁵. Det er afgørende at udvikle en fælles metode på tværs af sektorer til arbejdet med referencekrav til modstandsdygtighed over for hybride trusler for at imødegå risikoen for fragmenterede og overlappende politikker, værktøjer og tiltag. Det Europæiske Center for Imødegåelse af Hybride Trusler i Helsingfors deltog også i dette samarbejde. Samarbejdet med NATO er blevet intensiveret under covid-19-krisen, herunder vedrørende desinformation om pandemien og håndtering af fjendtlige informationsaktiviteter.

Covid-19-pandemien har generelt fremhævet den hastigt voksende risiko for **desinformation** og den reelle risiko for menneskers liv⁷⁶. Den 10. juni 2020 vedtog Kommissionen og den højtstående repræsentant en **fælles meddelelse om covid-19 og desinformation**⁷⁷, hvori man påpegede de specifikke risici for desinformation om covid-19, og hvilke foranstaltninger der bør træffes. Dette indebærer, at større onlineplatforme skal udvikle politikker til håndtering af truslen og intensiveret overvågning af platformenes indsats samt dedikeret samarbejde gennem det hurtige varslingsystem, der forvaltes af EU-Udenrigstjenesten. Pandemien udløste en større indsats for at bekæmpe desinformation og øget offentlig bevidsthed. I første halvdel af 2020 har **EUvsDisinfo's** offentlige database over desinformationssager tilføjet 1963 nye tilfælde af Kreml-venlig desinformation, hvoraf næsten en tredjedel har været relateret til covid-19-infodemien. Fra midten af marts til udgangen af april 2020 besøgte mere end 10 000 personer webstedet dagligt, og det samlede antal besøgende steg med 400 % sammenlignet med samme periode i 2019. EU's indsats omfattede målrettede kommunikationskampagner⁷⁸ og tilvejebringelse af faktuelle oplysninger om pandemien.

De indhøstede erfaringer har bidraget til udarbejdelsen af den **europæiske handlingsplan for demokrati**, der blev vedtaget den 2. december 2020⁷⁹. Heri fastsættes de vigtigste skridt til at styrke modstandsdygtigheden i EU's demokratiske struktur ved at fremme frie og retfærdige valg, tackle pres rettet mod frie og uafhængige medier og bekæmpe desinformation. Dette sidste aspekt vil bygge på handlingsplanen for bekæmpelse af

⁷⁴ Analysen af hybride tendenser er et værktøj, der skal anvendes sideløbende med nationale systemer til at overvåge omfanget og intensiteten af hybride trusler på områderne politik/diplomati, militær, økonomi, information, efterretninger, cybersikkerhed, sociale anliggender, energi og infrastruktur.

⁷⁵ Samarbejdet mellem medarbejdere inden for cybersikkerhed og -forsvar er blevet yderligere intensiveret gennem arbejdet med konsekvente koncepter og doktriner, øvelser, udveksling af oplysninger og tværgående briefinger.

⁷⁶ De håndgribelige faktiske konsekvenser omfattede afbrænding af telekommunikationsinfrastruktur og vildledende sundhedsoplysninger med direkte følger.

⁷⁷ JOIN(2020) 8, fælles meddelelse om bekæmpelse af desinformation om covid-19 — sådan får vi styr på fakta.

⁷⁸ F.eks. blev kampagnen "Tænk før du deler" lanceret for at rådgive om, hvordan man kan begrænse udbredelsen af desinformation til unge målgrupper og multiplikatorer i EU's østlige partnerskabslande, og den nåede mere end 500 000 visninger på sociale medieplatforme.

⁷⁹ COM(2020) 790.

desinformation fra 2018⁸⁰ som grundlag for en øget EU-indsats for at bekæmpe desinformation og for, hvordan man kan inddrage centrale interessenter i civilsamfundet og den private industri. Det skuer også fremad mod det næste skridt med **adfærdskodeksen om desinformation** efter vurderingen af kodeksens effektivitet i september 2020⁸¹. Kodeksen har været et vigtigt og nødvendigt skridt i retning af at skabe et mere gennemsigtigt og ansvarligt onlineplatformsøkosystem, men den ville være mere effektiv med mere ensartede definitioner, en mere konsekvent gennemførelse og flere foranstaltninger til at håndtere specifikke områder såsom mikromålretning. Et andet vigtigt redskab, som EU nu har til rådighed, er **Det Europæiske Observationscenter for Digitale Medier**, der blev operationelt i juni 2020. Det samler centrale interessenter, der arbejder med desinformation, herunder faktatjekkere og akademiske forskere.

IV BESKYTTELSE AF EUROPÆERNE MOD TERRORISME OG ORGANISERET KRIMINALITET

1. *Terrorisme og radikalisering*

De seneste angreb har endnu engang vist, at terrortruslen i EU fortsat er høj. Mordet på en lærer i Conflans-Sainte-Honorine den 16. oktober 2020 blev efterfulgt af drabet på tre mennesker i Notre Dame-kirken i Nice den 29. oktober. Den 2. november blev fire mennesker dræbt og 23 såret ved et terrorangreb i Wien. Den 13. november vedtog Rådet en fælles erklæring fra EU's indenrigsministre om de seneste terrorangreb i Frankrig og Østrig⁸². Disse nylige jihadist-inspirerede angreb kommer oven i en stigende trussel fra voldelige højreekstremister og andre former for terrorisme.

For yderligere at støtte medlemsstaterne i bekæmpelsen af terrorisme og radikalisering vedtager Kommissionen i dag en **EU-dagsorden for terrorbekæmpelse**⁸³. Denne dagsorden bygger på eksisterende politikker og instrumenter og vil styrke EU's ramme for yderligere at forbedre foregribelse af trusler og risici, forebyggelse af radikalisering og voldelig ekstremisme, beskyttelse af mennesker og infrastrukturer, herunder gennem sikkerhed ved de ydre grænser, og effektiv opfølgning efter angreb. Den skitserer også vejen frem for at forbedre retshåndhævelsen og det retlige samarbejde samt brugen af teknologier og udveksling af relevante oplysninger i hele EU, herunder for dem, der udfører kontrol ved de ydre grænser. Gennemførelse og håndhævelse af lovgivningen er fortsat af afgørende betydning.

Forebyggelse er nøglen til bekæmpelse af terrorisme. EU's indsats inden for **forebyggelse af radikalisering** bygger på de solide erfaringer, der indtil videre er gjort med støtte til fagfolk og beslutningstagere i første linje. Den 24. november vedtog Kommissionen en ny **handlingsplan for integration og inklusion**⁸⁴. I kampen mod radikalisering er det af afgørende betydning at arbejde hårdere for at bringe samfundene sammen. Et mere sammenhængende og inklusivt samfund kan bidrage til at forhindre udbredelsen af ekstremistiske ideologier, der kan føre til terrorisme og voldelig ekstremisme. Støtte til **netværket til bevidstgørelse omkring radikalisering** omfatter en kontrakt på yderligere 30 mio. EUR i januar 2020 for de næste fire år med hjælp til fagfolk på stedet samt ekstra

⁸⁰ JOIN(2018) 36, fælles meddelelse, Handlingsplan for bekæmpelse af desinformation.

⁸¹ SWD(2020) 180 final.

⁸² Fælles erklæring fra EU's indenrigsministre om de seneste terrorangreb i Europa, 13.11.2020, 12634/20.

⁸³ COM(2020) 795 final.

⁸⁴ COM(2020) 758 final.

støtte til politiske beslutningstagere og forskere. Disse og andre instrumenter, såsom **EU's internetforum**, vil gøre det muligt for Kommissionen at tage fat på de prioriterede foranstaltninger, der er fremhævet i de strategiske retningslinjer fra 2021 om en koordineret EU-tilgang til forebyggelse af radikaliserings, som man har udviklet sammen med medlemsstaterne. De suppleres af tiltag i terrorbekæmpelsesdagsordenen for at bekæmpe ekstremistiske ideologier online, optrappe indsatsen i fængsler samt rehabilitering og reintegration, herunder for fremmedkrigere, og for at styrke støtten til lokale aktører og opbygge mere modstandsdygtige samfund.

Direktivet om bekæmpelse af terrorisme⁸⁵, der blev vedtaget i marts 2017, er det vigtigste strafferetlige instrument på EU-plan til bekæmpelse af terrorisme. Det fastsætter minimumsstandarder for definition af terrorhandlinger og terrorrelaterede lovovertrædelser og for sanktioner, samtidig med at ofre for terrorisme får ret til beskyttelse, støtte og bistand. Den 30. september 2020 vedtog Kommissionen en rapport⁸⁶ med en vurdering af de foranstaltninger, som medlemsstaterne har truffet for at efterkomme direktivet. Den konkluderer, at gennemførelsen i national ret har bidraget til at styrke medlemsstaternes strafferetlige tilgang til terrorisme og terrorofrenes rettigheder, men at der stadig er huller. F.eks. kriminaliserer ikke alle medlemsstater i deres nationale lovgivning alle de lovovertrædelser, der er opført i direktivet som terrorhandlinger, samt bestemmelserne om kriminalisering af rejser med terror for øje og finansiering af terrorisme samt støtte til ofre. En evalueringsrapport om direktivet vil blive vedtaget senere i 2021.

EU arbejder fortsat på at støtte medlemsstaterne i at fratage terrorister midlerne til at angribe og i at støtte gennemførelsen af reglerne. Forordningen om markedsføring og anvendelse af **udgangsstoffer til eksplosivstoffer**, der blev vedtaget i juni 2019⁸⁷, træder i kraft den 1. februar 2021. For at hjælpe de nationale myndigheder og den private sektor med at gennemføre forordningen offentliggjorde Kommissionen i juni 2020 et sæt retningslinjer⁸⁸. Desuden udarbejdede Kommissionen i juni 2020⁸⁹ et program til overvågning af forordningens udbytte, resultater og virkninger.

I november 2019 opfordrede Kommissionen medlemsstaterne til at vurdere gennemførelsen af handlingsplanen fra 2017 for at øge beredskabet over for **kemiske, biologiske, radiologiske og nukleare risici (CBRN)**⁹⁰. Den overordnede konklusion var, at de fleste foranstaltninger var blevet gennemført. I begyndelsen af 2020 opstillede Kommissionen i samarbejde med nationale eksperter en liste over problematiske højrisikokemikalier. Den dannede grundlag for et samarbejde med udstyrsfabrikanter med henblik på at forbedre sporingsmulighederne. Kommissionen har for nylig iværksat en undersøgelse af muligheden for at begrænse adgangen til nogle af disse kemikalier. Arbejdet er også i gang som led i EU-civilbeskyttelsesmekanismen, og yderligere CBRN-indsatskapaciteter drøftes med medlemsstaterne inden for områderne dekontaminering, detektion, overvågning og tilsyn samt opbygning af lagre.

Den 12. oktober 2020 besluttede Rådet at forlænge sanktionsordningen mod spredning og brug af kemiske våben med et år⁹¹, således at EU får mulighed for at indføre restriktive

⁸⁵ Direktiv (EU) 2017/541.

⁸⁶ COM(2020) 619 final.

⁸⁷ Forordning (EU) 2019/1148.

⁸⁸ Kommissionens meddelelse — Retningslinjer for gennemførelsen af forordning (EU) 2019/1148 om markedsføring og anvendelse af udgangsstoffer til eksplosivstoffer, EUT C 210 af 24.6.2020, s 1.

⁸⁹ SWD(2020) 114 final.

⁹⁰ COM(2017) 610 final.

⁹¹ Rådets afgørelse (FUSP) 2020/1466 af 12. oktober 2020 om ændring af afgørelse (FUSP) 2018/1544.

foranstaltninger over for personer og enheder, der er involveret i udvikling og anvendelse af kemiske våben. Den 14. oktober 2020 vedtog Rådet restriktive foranstaltninger over for seks personer og en enhed, der var involveret i attentatet på Alexei Navalny, som den 20. august 2020 blev forgiftet med en nervegas fra "Novichok"-gruppen i Rusland⁹².

Finansielle oplysninger er også afgørende for muligheden for at identificere terrornetværk, da terrorister er afhængige af finansiering til rejser, uddannelse og udstyr, og **bekæmpelse af finansiering af terrorisme** er afgørende for terrorbekæmpelseeftersforskninger. Centrale spørgsmål omfatter udnyttelse af det fulde potentiale ved eksisterende værktøjer og efterretninger, korrekt gennemførelse af internationalt vedtagne standarder og håndtering af de udfordringer, der opstår som følge af nye teknologier og sociale medieplatforme⁹³ (se nedenfor).

Transportnettet har været og er fortsat et terrormål. EU's indsats omfatter en risikobaseret tilgang til beskyttelse af luftfartssektoren⁹⁴. Konfliktområder udgør en alvorlig risiko for den civile luftfart, og udveksling af oplysninger og risikovurdering er afgørende for risikoreduktion⁹⁵. EU's varslingsystem for **risikovurdering af konfliktramte områder** anerkendes som bedste praksis, og internationale standarder for informationsudveksling er blevet indarbejdet i EU-lovgivningen⁹⁶. På grundlag af erfaringerne inden for civil luftfart har Kommissionen udvidet den risikovurderingsbaserede tilgang til andre transportformer. Gennemførelsen af EU's **handlingsplan for jernbanesikkerhed**⁹⁷ er godt i gang og udnytter ekspertisen i EU's Rail Passenger Platform (togpassagerplatform), en særlig ekspertgruppe nedsat af Kommissionen. På det maritime område er den risikovurderingsbaserede tilgang velkendt og anvendt, og Kommissionen samarbejder med medlemsstater og interessenter om at styrke passagerernes sikkerhed. Dette er indarbejdet i **EU's strategi for maritim sikkerhed** og dens **handlingsplan**, som blev revideret i 2018, hvor man medtog en sikkerheds- og forsvarsdimension. Dette fremgår af den seneste gennemførelsesrapport, der blev vedtaget og offentliggjort den 23. oktober 2020⁹⁸.

Europol yder støtte til medlemsstaterne ved efterforskning i forbindelse med terrorisme gennem **Det Europæiske Center for Terrorbekæmpelse (ECTC)**. Medlemsstaternes anmodninger om operationel støtte til ECTC blev stadig flere, og ECTC er nu en del af næsten alle større terrorbekæmpelseeftersforskninger. I 2019 støttede Europol i alt 632 forskellige operationer på terrorbekæmpelsesområdet. Medlemsstaternes efterforskere har også vist en stigende påskønnelse af dette arbejde og bevæget sig fra et tilfredshedsniveau på 8/10 i 2018 til 9.1/10 i 2019. ECTC koordinerede i alt 18 aktionsdage i 2019⁹⁹.

⁹² Rådets afgørelse (FUSP) 2020/1482 af 14. oktober 2020 og Rådets gennemførelsesforordning (EU) 2020/1480.

⁹³ Som fremført af EU i november 2019 på ministerkonferencen "No Money For Terror" om finansiering af terrorbekæmpelse, som Australien var vært for.

⁹⁴ Den integrerede EU-proces for risikovurdering af luftfartssikkerheden understøtter beslutningsprocessen inden for luftfragtsikkerhed, normer for luftfartssikkerhed og risici for civil luftfart fra konfliktområder.

⁹⁵ Den tragiske nedskydning af Ukraine International Airlines flynummer 752 den 8. januar 2020 var yderligere et bevis på betydningen af informationsudveksling og risikovurdering for sikkerheden inden for civil luftfart.

⁹⁶ <https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32019R1583>.

⁹⁷ COM(2018) 470 final.

⁹⁸ Rapport fra Kommissionens tjenestegrene, Tjenesten for EU's Optræden Udadtil og Det Europæiske Forsvarsagentur om gennemførelsen af den reviderede handlingsplan for EU's strategi for maritim sikkerhed (SWD(2020) 252).

⁹⁹ 2019 Consolidated annual activity report, Europol, 9.06.2020.

Eurojust støttede også 116 terrorundersøgelser i 2019 og 2020. Det igangværende arbejde vil munde ud i et lovforslag om udvekslinger vedrørende grænseoverskridende digitale terrorsager med henblik på at udvikle det terrorbekæmpelsesregister, der blev lanceret i 2019¹⁰⁰, samt udvide arbejdet om højreekstremistiske og venstreekstremistiske grupper.

Den 30. juli 2020 ajourførte Rådet senest EU's liste over personer, grupper og enheder, der er omfattet af restriktive foranstaltninger med henblik på bekæmpelse af terrorisme. Den seneste liste omfatter 14 personer og 21 enheder. Samme dag indførte Rådet restriktive foranstaltninger over for én person i henhold til sanktionsordningen for terrorbekæmpelse vedrørende ISIL (Da'esh)/al-Qaida. På nuværende tidspunkt er der fem personer, der autonomt er opført på listen under denne ordning, som blev forlænget med et år den 19. oktober 2020¹⁰¹.

Et vigtigt element i terrorbekæmpelsespolitikken vedrører truslerne fra **fremmedkrigere** i øjeblikket i Syrien og Irak. Samtidig med at medlemsstaternes primære ansvar for disse spørgsmål respekteres fuldt ud, hjælper støtte og samarbejde på EU-plan medlemsstaterne med at tackle fælles udfordringer: retsforfølgelse af personer, der har begået terrorhandlinger, forebyggelse af uopdaget indrejse i Schengenområdet samt reintegration og rehabilitering af tilbagesendte fremmedkrigere. Kommissionen arbejder f.eks. tæt sammen med medlemsstaterne og de vigtigste partnerlande for at sikre, at bevismateriale fra slagmarken deles og anvendes effektivt til identifikation, afsløring ved EU's grænser og retsforfølgning. Memorandum on Battlefield Evidence fra 2020¹⁰², som Eurojust har offentliggjort, viser, at selv om der er mange udfordringer med at fremskaffe sådanne oplysninger og sikre, at de opfylder kriterierne for gyldige beviser, kan de bidrage til at få retsforfulgt terrormistænkte.

Kommissionen fremmer også en dialog med medlemsstaterne og humanitære aktører for at levere et samlet og faktisk overblik over situationen i de lejre i det nordøstlige Syrien, hvor europæiske familiemedlemmer til fremmedkrigere befinder sig. Der lægges særlig vægt på børnenes situation i de syriske lejre. Kommissionen hjælper også medlemsstaterne med at udveksle erfaringer om nationale foranstaltninger og mekanismer til bedre at forvalte **rehabilitering og reintegration** af hjemvendte fremmedkrigere og børn. Netværket til bevidstgørelse om radikaliserings gennemfører også studiebesøg og yder skræddersyet rådgivning for bedre at kunne håndtere de udfordringer, som dømte tilbagevendte personer står over for, navnlig efter løsladelse fra fængslet, samt den rolle, som familier og lokalsamfund spiller i reintegrationsbestrebelsene.

Terrorbekæmpelsespartnerskaber og samarbejde med tredjelande og partnere i EU's nabolande er også afgørende for at forbedre sikkerheden i EU og for at sikre en bedre sammenhæng mellem de interne og eksterne dimensioner af EU's sikkerhedspolitik. Rådet har opfordret til en yderligere styrkelse af EU's eksterne engagement i terrorbekæmpelse¹⁰³ med fokus på Vestbalkan, Nordafrika og Mellemøsten, Sahelregionen, Afrikas Horn og Asien. Dette arbejde videreføres ved at udnytte udenrigspolitiske redskaber fuldt ud, herunder dialoger på højt plan om terrorbekæmpelse og netværket af 17

¹⁰⁰ Terrorbekæmpelsesregistret forvaltes af Eurojust 24 timer i døgnet og yder proaktiv støtte til de nationale retlige myndigheder. Disse centraliserede oplysninger bør hjælpe anklagere med at koordinere mere aktivt og identificere mistænkte eller netværk, der efterforskes i specifikke sager med potentielle grænseoverskridende konsekvenser.

¹⁰¹ Rådets afgørelse (FUSP) 2020/1132, 2020/1126 og 2020/1516.

¹⁰² <https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0>.

¹⁰³ Rådets konklusioner (8868/20) om EU's foranstaltninger udadtil vedrørende forebyggelse og bekæmpelse af terrorisme og voldelig ekstremisme (16. juni 2020).

terrorbekæmpelses-/sikkerhedseksperter¹⁰⁴, der er udsendt til EU-delegationerne, og som fortsat yder støtte, letter samarbejdet og fremmer kapacitetsopbygning. Man overvejer i øjeblikket muligheden for at styrke og udvide dette netværk.

Den fælles handlingsplan fra 2018 om terrorbekæmpelse for **Vestbalkan** og de ledsagende bilaterale ordninger, der blev undertegnet i 2019 med hver enkelt partner¹⁰⁵, sætter fokus på en region af central betydning for fælles sikkerhedsmål og for beskyttelsen af mennesker, der bor i EU. På ministerforummet for retlige og indre anliggender mellem EU og Vestbalkan den 22. oktober 2020 bekræftede EU og partnerne på Vestbalkan deres tilsagn om at gennemføre målene i den fælles handlingsplan efter 2020¹⁰⁶. Samarbejdet med Vestbalkan omfatter forvaltning af fremmedkrigernes og deres familiemedlemmers igangværende tilbagevenden samt yderligere integration i aktiviteter til bekæmpelse af radikalisering. EU opretholder også et regelmæssigt engagement i terrorbekæmpelse med **Mellemøsten, Nordafrika og Centralasien**¹⁰⁷. Samarbejdet med **Centralasien** har fokuseret på at tackle kemiske, biologiske, radiologiske og nukleare trusler. Det Blandede Samarbejdsudvalg **EU og Golfstaternes Samarbejdsråd** mødtes den 25. juni 2020 og drøftede spørgsmål som bekæmpelse af radikalisering og finansiering af terrorisme og bekæmpelse af hvidvask af penge samt cybersikkerhed og samarbejde med Europol. EU samarbejdede med NATO om den første revision nogensinde af kemiske, biologiske, radiologiske og nukleare trusler i en af Golfstaterne i slutningen af 2019. Ved udgangen af 2019 var der samlet set afsat omkring 465 mio. EUR til igangværende projekter om terrorbekæmpelse og forebyggelse af voldelig ekstremisme uden for EU, hvilket er en stigning på 15 % i forhold til det foregående år.

EU har også fortsat uddybningen af samarbejdet med **FN** om terrorbekæmpelse¹⁰⁸, navnlig med FN's Kontor for Terrorbekæmpelse og det udøvende direktorat for terrorbekæmpelse, herunder gennem årlige dialoger på højt plan og senest gennem aktiv deltagelse i FN's virtuelle terrorbekæmpelsesuge i sommeren 2020. Kommissionen har også nøje fulgt drøftelserne om en revision af definitionen af terrorhandlinger i **Europarådets** konvention om forebyggelse af terrorisme og tilskyndet til nøje tilpasning til definitionerne i EU-retten. Det gode samarbejde mellem **NATO** og EU fortsatte inden for terrorbekæmpelse og kemiske, biologiske, radiologiske og nukleare materialer, udveksling af oplysninger om kapacitetsopbygning for at undgå overlappning og sikre komplementaritet.

2. Bekæmpelse af organiseret kriminalitet

Den organiserede kriminalitet vokser, bliver stadig mere grænseoverskridende og bevæger sig online.

¹⁰⁴ Algeriet, Bosnien-Hercegovina (regionalt for Vestbalkan), Tchad (regionalt for Sahel), Etiopien (forbindelse til Den Afrikanske Union), Indonesien (regionalt for Sydøstasien og forbindelse til ASEAN-ARF), Irak, Jordan, Kenya (regionalt for Afrikas Horn), Kirgisistan (regionalt for Centralasien), Libanon, Libyen, Marokko, Nigeria, Pakistan, Saudi-Arabien, Tunesien og Tyrkiet.

¹⁰⁵ Serbien, Nordmakedonien, Bosnien-Hercegovina, Kosovo*, Albanien og Montenegro.

¹⁰⁶ Fælles pressemeddelelse: <https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf>.

¹⁰⁷ Terrorbekæmpelsesindsatsen blev f.eks. fremhævet i den nye EU-strategi for Centralasien.

* Denne betegnelse indebærer ingen stillingtagen til Kosovos status, og den er i overensstemmelse med UNSCR 1244(1999) og ICJ's udtalelse om Kosovos uafhængighedserklæring.

¹⁰⁸ I 2019 blev der undertegnet en samarbejdsramme mellem EU og FN om bekæmpelse af terrorisme https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf.



Europol, Serious and Organised Threat Assessment (trusselvurdering af grov og organiseret kriminalitet — SOCTA 2017)

Kommissionens indsats har omfattet bekæmpelse af narkotika, ulovlige skydevåben, økonomisk kriminalitet, ulovlig import af kulturgoder, menneskehandel og miljøkriminalitet, støtte til medlemsstaternes retshåndhævende og retslige myndigheder i medlemsstaterne samt partnere i nabolandsområdet. Samarbejdet med tredjelande, navnlig i nabolandene som det vestlige Balkan, og internationale organisationer, herunder FN's Kontor for Narkotikakontrol og Kriminalitetsbekæmpelse¹⁰⁹, var også af afgørende betydning¹¹⁰.

I 2019 modtog og behandlede **Europols center for grov og organiseret kriminalitet** næsten 55 000 operationelle bidrag, hvilket er en stigning på 12 % i forhold til 2018. Centret støttede operationer i 726 lande¹¹¹. Det er også afgørende, at EU's juridiske ramme for organiseret kriminalitet¹¹², som har til formål at harmonisere medlemsstaternes love om kriminalisering af lovovertrædelser i forbindelse med deltagelse i en kriminel organisation og fastsætter sanktioner for disse lovovertrædelser, gennemføres fuldt ud i alle medlemsstater. Kommissionen har iværksat en undersøgelse for at analysere, hvordan denne lovgivning kan forbedres. Der vil blive taget yderligere skridt til at intensivere bekæmpelsen af organiseret kriminalitet i EU på den EU-dagsorden for bekæmpelse af organiseret kriminalitet, der skal vedtages i første kvartal af 2021.

Indefrysning og konfiskation af udbytte fra strafbart forhold er et af de mest effektive midler til bekæmpelse af organiseret kriminalitet. Det nye europæiske center for finansiell og økonomisk kriminalitet (EFECC), der blev oprettet i juni 2020 i Europol, vil øge den operationelle støtte til medlemsstaterne og EU-organerne inden for finansiell og økonomisk kriminalitet og fremme systematisk brug af finansielle efterforskninger. Til støtte for EU's indsats for mere effektiv identifikation, indefrysning og konfiskation af udbytte fra kriminelle aktiviteter vedtog Rådet i juni 2020 konklusioner om styrkelse af den finansielle efterforskning til bekæmpelse af grov og organiseret kriminalitet¹¹³. I 2021 vil

¹⁰⁹ En dialog på højt plan mellem EU og UNODC fandt sted den 8. december 2020.

¹¹⁰ Ved udgangen af 2019 var der afsat ca. 830 mio. EUR til igangværende aktioner vedrørende organiseret kriminalitet uden for EU.

¹¹¹ 2019 Consolidated Annual Report, Europol, juni 2020.

¹¹² Rameafgørelse 2008/841.

¹¹³ Rådets konklusioner 8927/20.

Kommissionen revidere lovgivningen om indefrysning og konfiskation af udbytte fra strafbart forhold¹¹⁴ og om kontorer for inddrivelse af aktiver¹¹⁵.

Der er behov for sikkerhedsforanstaltninger i kampen mod organiseret kriminalitet for at sikre, at retshåndhævelsesarbejdet kan fungere effektivt inden for væsentlige grænser, såsom beskyttelse af personoplysninger. Direktivet om databeskyttelse på retshåndhævelsesområdet fra 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i forbindelse med strafbare handlinger¹¹⁶ beskytter den grundlæggende ret til databeskyttelse, når retshåndhævende myndigheder på det strafferetlige område anvender personoplysninger til retshåndhævelsesformål. Det sikrer, at personoplysninger om ofre, vidner og personer, der mistænkes for forbrydelser, er behørigt beskyttet, og letter det grænseoverskridende samarbejde i kampen mod kriminalitet og terrorisme. Fristen for gennemførelse af direktivet om databeskyttelse på retshåndhævelsesområdet udløb den 6. maj 2018. I dag har de fleste medlemsstater vedtaget lovgivning til gennemførelse af direktivet. En række traktatbrudsprocedurer er dog endnu ikke afsluttet¹¹⁷. Kommissionen er i øjeblikket i færd med at vurdere, om de nationale gennemførelsesbestemmelser er i overensstemmelse med direktivet.

Kampen mod ulovlig narkotika

Kommissionen vedtog i juli 2020 en ny **EU-narkotikadagsorden og -handlingsplan for 2021-2025**¹¹⁸ i forlængelse af EU's nuværende narkotikastrategier¹¹⁹. Heri fastlægges de politiske rammer og prioriteter for indsatsen i de næste fem år. Dagsordenens hovedfokus er: (1) forstærkede sikkerhedsforanstaltninger over for ulovlig narkotikahandel, fra organiserede kriminelle grupper til forvaltning af EU's ydre grænser og ulovlig distribution og produktion (2) øget forebyggelse, herunder oplysning om stoffers bivirkninger, navnlig i krydsfeltet mellem stofmisbrug, vold og andre former for kriminalitet og (3) mindskning af narkotikarelaterede skader ved hjælp af adgang til behandling, reduktion af risici og skader samt en afbalanceret tilgang til narkotikaproblematikken i fængslerne. Den 30. november 2020 vedtog Kommissionen også en evaluering af EU's politik for narkotikaprækursorer, hvori det konkluderes, at der er behov for yderligere tiltag for at forhindre, at organiserede kriminelle grupper i EU får adgang til de kemikalier, de skal bruge til at fremstille ulovlige syntetiske stoffer¹²⁰.

EU har også finansieret konkrete projekter for at styrke bekæmpelsen af narkotika, såsom civilsamfundsforummet om narkotika. Den Europæiske Narkotikarapport 2020 fra Det Europæiske Overvågningscenter for Narkotika og Narkotikamisbrug, der blev offentliggjort den 22. september 2020¹²¹, viser den seneste udvikling i narkotikamisbrug og -markeder i EU, Tyrkiet og Norge. Den viser en stigning i udbuddet af kokain med beslaglæggelser på et rekordhøjt niveau på 181 tons, en næsten fordobling af

¹¹⁴ Direktiv 2014/42/EU.

¹¹⁵ Rådets afgørelse 2007/845/RIA.

¹¹⁶ Direktiv (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i forbindelse med strafbare handlinger.

¹¹⁷ Tre medlemsstater (Tyskland, Slovenien, Spanien) har endnu ikke givet meddelelse om fuld gennemførelse på trods af traktatbrudsprocedurer. Kommissionen indbragte én sag vedrørende manglende gennemførelse for Domstolen og sendte i maj 2020 supplerende begrundede udtalelser til de to andre medlemsstater for ikke at have gennemført direktivet fuldt ud.

¹¹⁸ COM(2020) 606 final.

¹¹⁹ EU's narkotikastrategi 2013-2020 og EU's narkotikahandlingsplan 2017-2020.

¹²⁰ COM(2020) 768 af 30. november 2020.

¹²¹ European Drug Report (den europæiske narkotikarapport) 2020: Trends and Developments (tendenser og udvikling), EONN, 22.9.2020.

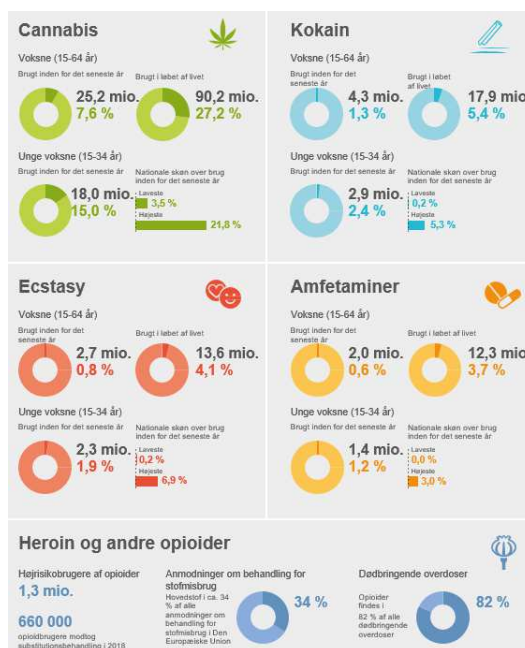
beslaglæggelserne af heroin til 9,7 ton og et stort udbud af narkotika med stor renhed i EU. Den undersøger også fremkomsten af nye syntetiske opioider, der giver anledning til særlige sundhedsproblemer, og tager fat på de udfordringer, der er forårsaget af covid-19-pandemien.

Indsatsen mod narkotika videreføres på flere forskellige niveauer. **Lovpakken om nye psykoaktive stoffer** blev vedtaget i efteråret 2017¹²² og trådte fuldt ud i kraft i november 2018. Fem medlemsstater er stadig genstand for traktatbrudsprocedurer¹²³. Den første delegerede retsakt, der definerer et nyt psykoaktivt stof (isotonitazen) som et narkotikum, er nu blevet vedtaget.¹²⁴

På det **internationale plan** har EU været aktiv i FN's Narkotikakommission¹²⁵, navnlig med hensyn til ajourføring af listerne over nye psykoaktive stoffer¹²⁶ og med henblik på en omregistrering af cannabis og cannabisrelaterede stoffer¹²⁷. Rådet har godkendt to nye dialoger om narkotika med Kina og Iran¹²⁸, og Det Europæiske Overvågningscenter for Narkotika og Narkotikamisbrug er gået videre med samarbejdsordninger med tredjelande¹²⁹.

Bekæmpelse af økonomisk kriminalitet

Der er vedtaget ny lovgivning for at styrke bekæmpelsen af økonomisk kriminalitet og hvidvaskning af penge. Direktivet, der letter anvendelsen af finansielle og andre oplysninger til forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger blev vedtaget i 2019 og gav retshåndhavende myndigheder og kontorer for inddrivelse af aktiver adgang til nationale centrale bankkontoregistre med henblik på bekæmpelse af grov kriminalitet. Direktivet har også til formål at forbedre samarbejdet mellem retshåndhavende myndigheder og finansielle efterretningsenheder (FIU'er) og lette udvekslingen af oplysninger mellem FIU'er. I juni 2020 offentliggjorde Kommissionen en rapport om inddrivelse og konfiskation af aktiver og sikring af, at kriminalitet ikke betaler sig¹³⁰. Heri pegede den på potentialet for øget harmonisering af ordningerne for inddrivelse af aktiver¹³¹ med henblik på at modernisere EU-lovgivningen om inddrivelse af aktiver og styrke de nationale myndigheders kapacitet



¹²² Forordning (EU) 2017/2101 og direktiv 2017/2103/EU,

¹²³ Østrig, Finland, Irland, Portugal og Slovenien.

¹²⁴ C/2020/5897, EUT L 379 af 13.11.2020, s. 55.

¹²⁵ Et styrende organ under FN's Kontor for Narkotikakontrol og Kriminalitetsbekæmpelse (UNODC).

¹²⁶ COM(2019) 631 final.

¹²⁷ COM(2019) 624 og COM(2020) 659.

¹²⁸ Topmødet mellem EU og Kina den 16.-17. juli 2018 i Beijing mandede ud i en aftale om at indlede en årlig narkotikadialog mellem EU og Kina. De nærmere bestemmelser for den fremtidige dialog blev bekræftet af Coreper den 30. oktober 2019. Rådet godkendte indledningen af en ny narkotikadialog mellem EU og Iran den 5. marts 2020.

¹²⁹ Kommissionens udtalelse om udkastet til samarbejdsaftale med Kosovo vedtaget den 14. april 2020 og udtalelsen med Serbien vedtaget den 16. december 2019.

¹³⁰ COM(2020) 2017.

¹³¹ Herunder vurderingen af direktiv 2014/42/EU og Rådets afgørelse 2007/845/RIA.

til at bekæmpe organiseret kriminalitet. Der er iværksat en yderligere analyse af inddrivelsen af aktiver i form af en ekstern undersøgelse. Forordningen om gensidig anerkendelse af afgørelser om indefrysning og konfiskation¹³² vil finde anvendelse fra den 19. december 2020 og vil indebære en betydelig styrkelse af samarbejdet mellem medlemsstaterne.

I maj 2020 vedtog Kommissionen en **handlingsplan for en omfattende EU-politik til forebyggelse af hvidvaskning af penge og finansiering af terrorisme**¹³³ for at forbedre EU-rammen. Den 5. november vedtog Rådet konklusioner om bekæmpelse af hvidvask af penge og finansiering af terrorisme¹³⁴, hvori det navnlig anmodede Kommissionen om at arbejde på vedtagelsen af et fælles regelsæt, oprettelsen af en uafhængig tilsynsmyndighed og koordinering af finansielle efterretningsenheder. I overensstemmelse med Rådets konklusioner om styrkelse af finansielle efterforskninger¹³⁵ vurderer Kommissionen også behovet for at sammenkoble centrale bankkontoregistre, hvilket vil fremskynde adgangen til oplysninger om bankkonti betydeligt for finansielle efterretningsenheder og retshåndhævende myndigheder. Sideløbende hermed fortsætter bestræbelserne på at sikre, at de seneste EU-standarter gennemføres effektivt af medlemsstaterne. Reglerne i det 5. direktiv om bekæmpelse af hvidvaskning af penge har til formål at sikre øget gennemsigtighed i virksomhedernes ejerskabsstrukturer. Gennemførelsesfristen udløb den 1. januar 2020, og Kommissionen indledte traktatbrudsprocedurer mod 16 medlemsstater¹³⁶. En anden vigtig foranstaltning er den nye forordning om kontrol med likvide midler¹³⁷, der blev vedtaget i oktober 2018 og finder anvendelse fra den 3. juni 2021. Den vil forbedre det eksisterende system for kontrol med likvide midler, der føres ind i eller ud af Unionen, og gennemførelsesbestemmelserne er under udarbejdelse.

På den eksterne front fortsætter bestræbelserne på at støtte partnerlandene med at bekæmpe hvidvaskning af penge og finansiering af terrorisme. I den forbindelse spiller EU-Udenrigstjenesten og EU-delegationerne en central rolle med hensyn til at fremme og støtte det politiske engagement med tredjelande og internationale organisationer såsom Den Finansielle Aktionsgruppe (FATF).

Som supplement til dette arbejde har Kommissionen lanceret en global facilitet for at yde støtte til partnerlande uden for EU med henblik på at indføre effektive rammer for bekæmpelse af hvidvaskning af penge og finansiering af terrorisme i henhold til internationale standarder. Foranstaltningen på 20 mio. EUR har også til formål at tilskynde til samarbejde mellem aktører på det finansielle og retlige område på nationalt, regionalt og internationalt plan.

Bekæmpelse af korruption

Korruption er en forbrydelse i sig selv og en vigtig katalysator for organiseret kriminalitet. Som led i forebyggelsen og bekæmpelsen af korruption vil medlemsstaternes retlige rammer blive regelmæssigt overvåget og vurderet i henhold til den nyligt oprettede

¹³² Forordning (EU) 2018/1805.

¹³³ C(2020) 2800 final.

¹³⁴ Rådets konklusioner 12608/20.

¹³⁵ Rådets konklusioner 8927/20.

¹³⁶ Østrig, Belgien, Cypern, Tjekkiet, Grækenland, Ungarn, Estland, Irland, Luxembourg, Nederlandene, Polen, Portugal, Rumænien, Slovakiet, Slovenien, Spanien og Det Forenede Kongerige.

¹³⁷ Forordning (EU) 2018/1672.

retsstatsmekanisme¹³⁸. Den første EU-rapport om retsstatsprincippet blev vedtaget den 30. september 2020¹³⁹. Den viste, at mange medlemsstater har høje retsstatsstandarder, men at der stadig er store udfordringer. Rapporten omfatter alle medlemsstater og indeholder objektive og faktuelle årlige vurderinger med det formål at skabe større bevidsthed om og forståelse af udviklingen i de enkelte medlemsstater, efterhånden som den finder sted, for at kunne identificere risici, udvikle mulige løsninger og målrette støtten på et tidligt tidspunkt. **Den Europæiske Anklagemyndighed (EPPO)** vil bekæmpe kriminalitet, der skader EU-budgettet, på nuværende tidspunkt i de 22 deltagende EU-lande. Den vil have beføjelse til at efterforske, retsforfølge og dømme de ansvarlige for strafbare handlinger, der skader EU-budgettet, såsom svig, korruption eller grov grænseoverskridende momssvig. EPPO skal efter planen være operationel i første kvartal af 2021.¹⁴⁰

Kommissionen er i øjeblikket ved at vurdere gennemførelsen af reglerne i **direktivet om strafferetlig bekæmpelse af svig rettet mod Den Europæiske Unions finansielle interesser**¹⁴¹ i national ret og har indledt traktatbrudsprocedurer mod de medlemsstater, der ikke har givet meddelelse om fuld gennemførelse¹⁴². I 2021 vil Kommissionen vedtage en rapport med en vurdering af, i hvilket omfang medlemsstaterne har truffet de nødvendige foranstaltninger for at efterkomme direktivet.

Bekæmpelse af ulovlig handel med kulturgenstande

Hovedformålet med **forordningen om indførsel og import af kulturgenstande**¹⁴³, der blev vedtaget i juni 2019, er at standse importen til Unionen af kulturgenstande, der er eksporteret ulovligt fra oprindelseslandet. For at sikre korrekt gennemførelse er Kommissionen i øjeblikket ved at forberede vedtagelsen af gennemførelsesbestemmelser, herunder et centraliseret elektronisk system til import af kulturgenstande, som vil muliggøre lagring og udveksling af oplysninger mellem medlemsstaterne og de nødvendige importformaliteter¹⁴⁴. En generel forbudsregel træder i kraft ved udgangen af 2020 og giver medlemsstaternes toldmyndigheder de retlige midler til at kontrollere og reagere på forsendelser, der kan indeholde kulturgenstande, som er eksporteret ulovligt fra deres oprindelsesland.

Bekæmpelse af ulovlig handel med skydevåben

Den 24. juli 2020 offentliggjorde Kommissionen **en ny EU-handlingsplan for 2020-2025 om ulovlig handel med skydevåben**.¹⁴⁵ På en ministerkonference på højt plan mellem EU's og Vestbalkans udenrigs- og indenrigsministerier den 31. januar 2020 blev det

¹³⁸ Den europæiske retsstatsmekanisme omfatter en proces for dialog mellem Kommissionen og medlemsstaterne samt Rådet og Europa-Parlamentet og de nationale parlamenter, civilsamfundet og andre interessenter om retsstatsprincippet. Retsstatsrapporterne er kernen i denne nye proces.

¹³⁹ COM(2020) 580 final.

¹⁴⁰ Rådets gennemførelsesafgørelse om udpegelse af de europæiske anklagere trådte i kraft den 29. juli 2020. De europæiske anklagere udgør kollegiet, der afholdt sit første møde den 28. september 2020. EPPO vil snart indgå samarbejdsaftaler med Europol, Eurojust og OLAF.

¹⁴¹ Direktiv (EU) 2017/1371.

¹⁴² Der er endnu ikke indledt traktatbrudsprocedurer mod Østrig, Irland og Rumænien.

¹⁴³ Forordning (EU) 2019/880.

¹⁴⁴ Systemet til import af kulturgenstande skal være indført senest den 28. juni 2025. Kommissionen har vedtaget en første statusrapport om udviklingen af systemet til import af kulturgenstande. [COM(2020) 342].

¹⁴⁵ COM(2020) 608: Denne nye handlingsplan integrerer det fransk-tyske initiativ for Vestbalkan "Køreplan for en holdbar løsning på ulovlig besiddelse af, misbrug af og ulovlig handel med SALW og ammunition hertil frem til 2024".

understreget, at der er behov for en øget indsats for at bekæmpe ulovlig handel med skydevåben. Handlingsplanen omfatter specifikke foranstaltninger til forbedring af den retlige kontrol med skydevåben, kendskabet til den våbenrelaterede trussel, retshåndhævelsessamarbejde og internationalt samarbejde med fokus på Sydøsteuropa. Kommissionen har taget skridt til at sikre, at direktivet om erhvervelse og besiddelse af våben, der blev vedtaget i maj 2017¹⁴⁶, gennemføres fuldt ud af medlemsstaterne. Ti medlemsstater mangler dog at give meddelelse om fuld gennemførelse af direktivet¹⁴⁷, og et stort flertal af medlemsstaterne har ikke gennemført den efterfølgende gennemførelseslovgivning. Kommissionen har derfor indledt traktatbrudsprocedurer¹⁴⁸. Kommissionen er også i færd med at foretage en detaljeret vurdering af de meddelte gennemførelsesforanstaltninger og vil aflægge rapport om gennemførelsen af direktivet i første halvdel af 2021. Kommissionen er endvidere begyndt at vurdere den mulige modernisering af de retlige rammer for indførsels-, udførsels- og transitforanstaltninger for skydevåben.¹⁴⁹

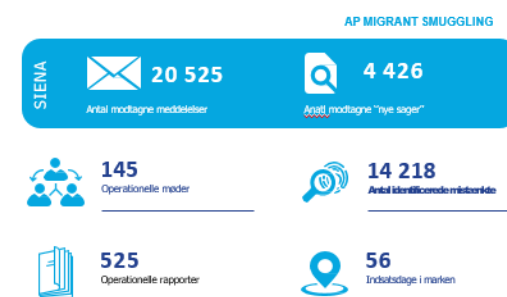
Bekæmpelse af menneskehandel

I strategien for en sikkerhedsunion fremhævede man behovet for at udvikle en ny strategisk tilgang til udryddelse af menneskehandel inden for rammerne af dagsordenen for bekæmpelse af organiseret kriminalitet. Som fastsat i artikel 20 i direktivet om bekæmpelse af menneskehandel¹⁵⁰ offentliggjorde Kommissionen i oktober 2020 sin tredje rapport om de fremskridt, der er gjort i bekæmpelsen af menneskehandel.¹⁵¹

Den viser, at der er gjort fremskridt inden for tværnationalt samarbejde, grænseoverskridende retshåndhævelse og operationelle retlige foranstaltninger, etablering af nationale og tværnationale henvisningsmekanismer for ofre og udvikling af videnbasen om menneskehandel. Medlemsstaterne gør i stigende grad brug af EU-agenturerne til at udveksle oplysninger,

Menneske smugling

Resultatindikatorer - 2019



Menneskehandel

Resultatindikatorer - 2019



¹⁴⁶ Direktiv (EU) 2017/853. Det centrale var også to gennemførelsesdirektiver af 16. januar 2019 om tekniske specifikationer for mærkning og gas- og signalvåben.

¹⁴⁷ Det drejer sig om Tjekkiet, Danmark, Spanien, Cypern, Luxembourg, Ungarn, Polen, Slovenien, Slovakiet og Sverige.

¹⁴⁸ Der er 25 igangværende sager vedrørende dette direktiv (Østrig, Belgien, Bulgarien, Cypern, Tjekkiet, Danmark, Tyskland, Estland, Grækenland, Spanien, Finland, Frankrig, Ungarn, Irland, Litauen, Luxembourg, Letland, Malta, Nederlandene, Polen, Portugal, Rumænien, Sverige, Slovenien og Slovakiet samt Det Forenede Kongerige) og 34 vedrørende gennemførelsesdirektiverne (direktiv 2019/68 — Østrig, Belgien, Bulgarien, Cypern, Tjekkiet, Tyskland, Grækenland, Spanien, Finland, Kroatien, Ungarn, Irland, Italien, Luxembourg, Polen, Rumænien, Sverige, Slovenien samt Det Forenede Kongerige, og direktiv 2019/69 — Bulgarien, Cypern, Tjekkiet, Grækenland, Spanien, Finland, Kroatien, Ungarn, Irland, Italien, Luxembourg, Nederlandene, Polen, Rumænien, Sverige og Slovenien samt Det Forenede Kongerige).

¹⁴⁹ Reguleret ved forordning (EU) nr. 258/2012.

¹⁵⁰ EUT L 101 af 15.04.2011, s. 1.

¹⁵¹ COM(2020) 661 final, suppleret af en undersøgelse om dataindsamling om menneskehandel i EU 2017-2018.

gennemføre fælles aktioner og indsætte fælles efterforskningshold for at bekæmpe menneskehandel både i og uden for EU¹⁵². Det operationelle samarbejde har givet håndgribelige resultater, navnlig inden for rammerne af den europæiske tværfaglige platform mod kriminalitetstrusler: I 2019 har dette arbejde resulteret i 825 anholdelser, 8 824 identificerede mistænkte og 1 307 potentielle ofre, herunder 69 identificerede børn. 94 organiserede kriminelle grupper, der var involveret i disse forbrydelser, blev identificeret eller opløst, og 1,5 mio. EUR på bankkonti, i virksomheder og på webdomæner blev indefrosset. På EU's dag for bekæmpelse af menneskehandel den 18. oktober 2020 offentliggjorde Kommissionen en undersøgelse af omkostningerne ved menneskehandel og en anden om de nationale og tværnationale henvisningsmekanismer¹⁵³.

Smugling af migranter

Det europæiske center for smugling af migranter har rapporteret om en fortsat stigning i omfanget af **migrantsmuglingsaktiviteter**, hovedsagelig på Vestbalkan og i nabolandene, og i sekundære bevægelser i hele EU. I 2019 bidrog Europol til identifikationen af 14 218 mistænkte, der er aktive inden for smugling af migranter¹⁵⁴. I maj 2020 oprettede Eurojust fokusgruppen for anklagere i forbindelse med smugling af migranter som et vigtigt knudepunkt for regelmæssigt at skabe forbindelse mellem de centrale retlige aktører på nationalt plan i EU-medlemsstaterne og støtte deres fælles operationelle indsats¹⁵⁵.

Bekæmpelse af miljøkriminalitet

Miljøkriminalitet omfatter handlinger, der er i strid med miljølovgivningen og forårsager eller kan forårsage betydelig skade på eller risiko for miljøet og menneskers sundhed¹⁵⁶. Blandt de vigtigste områder inden for **miljøkriminalitet** er ulovlige emissioner eller udledning af stoffer til luft, vand eller jord, ulovlig handel med vilde dyr og planter, ulovlig handel med ozonlagnedbrydende stoffer og ulovlig overførsel eller dumpning af affald. Den nylige evaluering af direktivet om miljøkriminalitet¹⁵⁷ viste, at fremskridtene med hensyn til at udvikle en europæisk ramme ikke blev modsvaret af en betydelig virkning i praksis, herunder med hensyn til bedre grænseoverskridende samarbejde og mere lige vilkår med hensyn til sanktioner på tværs af medlemsstaterne. Det havde navnlig ikke ført til flere domfældelser eller til mere afskrækkende sanktioner i medlemsstaterne. Det er derfor blevet besluttet at revidere direktivet inden udgangen af 2021.

Den 29.-30. oktober 2019 afholdt Eurojust sammen med det europæiske netværk af anklagere på miljøområdet (ENPE) en konference om internationalt samarbejde om bekæmpelse af miljøkriminalitet for at øge bevidstheden og fremme grænseoverskridende samarbejde mellem anklagere og andre fagfolk i og uden for EU om miljøkriminalitet.

¹⁵² Eksempelvis samarbejdede Den Europæiske Arbejdsmarkedsmyndighed med Europol om at bekæmpe menneskehandel i EU med henblik på alle former for udnyttelse, herunder seksuel og arbejdsmæssig udnyttelse samt alle former for handel med børn. Dette er også en anerkendelse af Den Internationale Arbejdsorganisations protokol om tvangsarbejde (P29). Denne protokol er en grundlæggende arbejdsstandard, der identificerer tvangsarbejde som en forbrydelse, og som omhandler forebyggelse, beskyttelse af ofre, erstatning og internationalt samarbejde om de nuværende former for tvangsarbejde, herunder i forbindelse med menneskehandel.

¹⁵³ Undersøgelser af de økonomiske, sociale og menneskelige omkostninger ved menneskehandel og gennemgang af, hvordan medlemsstaternes nationale og tværnationale henvisningsmekanismer fungerer, findes på <https://ec.europa.eu/anti-trafficking>.

¹⁵⁴ European migrant smuggling centre, 4. årlige rapport, 15.5.2020.

¹⁵⁵ <http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx>.

¹⁵⁶ Direktiv om strafferetlig beskyttelse af miljøet, 2008/99/EF.

¹⁵⁷ SWD(2020) 259 final.

Handlingsplanen mod ulovlig handel med vilde dyr og planter, der blev vedtaget i 2016, er ved at blive evalueret. En specifik foranstaltning er et projekt, der løber indtil januar 2021, og som er rettet mod ulovlig handel med vilde dyr og planter i og via EU ved hjælp af internettet og pakkeleveringstjenester med det formål at afbryde og optrævre netværk for IT-kriminalitet vedrørende vilde dyr og planter¹⁵⁸.

V. ET STÆRKT EUROPÆISK SIKKERHEDSØKOSYSTEM

Alle dele af samfundet må yde en fælles indsats for at etablere en ægte og effektiv sikkerhedsunion. Forvaltningsmyndigheder, retshåndhævende myndigheder, den private sektor, uddannelsessektoren og borgerne skal inddrages, klædes på og føres sammen for at opbygge et beredskab og skabe modstandsdygtighed for alle, navnlig de mest sårbare, ofre og vidner.

1. Samarbejde og udveksling af oplysninger

Et af de vigtigste bidrag, som EU kan yde for at beskytte borgerne, er at styrke samarbejdet mellem de instanser, der er ansvarlige for sikkerheden. Samarbejde og informationsudveksling er effektive værktøjer til at bekæmpe kriminalitet og terrorisme, håndtere trusler mod cybersikkerheden og opretholde retsordenen. Der er indført en række værktøjer for at støtte informationsudvekslingen mellem retshåndhævende og retslige myndigheder.

I dag vedtager Kommissionen et revideret mandat for **Europol**¹⁵⁹ for at forbedre agenturets arbejde på en række fastlagte områder. Det betyder, at Europol bedre kan håndtere den løbende udvikling inden for internetkriminalitet og økonomisk kriminalitet. Samtidig styrkes samarbejdet med den private sektor, og bestemmelserne for databeskyttelse tilpasses de eksisterende EU-regler.

Europol og andre af EU's agenturer såsom Frontex, CEPOL og Eurojust har med støtte fra Kommissionen fortsat udviklingen af EU's politikcyklus for grov og international organiseret kriminalitet i form af den europæiske tværfaglige platform mod kriminalitetstrusler, "**European Multidisciplinary Platform Against Criminal Threats**" (EMPACT)¹⁶⁰. Samarbejdet under EMPACT har fortsat vist sig at være et effektivt redskab til at bekæmpe organiseret kriminalitet i hele Europa, f.eks. gennem "fælles aktionsdage" i september, oktober og november 2020¹⁶¹. Dette viser tydeligt værdien af at samarbejde. Mindre kvantificerbare mål er også blevet nået, såsom et forbedret efterretningsbillede, uddannelse og kapacitetsopbygning, forebyggelse, samarbejde med partnere uden for EU

¹⁵⁸ <https://wwf.be/fr/wildlife-cybercrime/>.

¹⁵⁹ COM(2020) 796.

¹⁶⁰ EMPACT er EU's redskab til politisamarbejde om bekæmpelse af de største trusler mod EU's sikkerhed og styrker samarbejdet mellem de relevante tjenester i medlemsstaterne, EU-institutionerne og EU-agenturerne samt tredjelande og organisationer. EMPACT inddrager forskellige interessenter (tværfaglig tilgang) for at forbedre og styrke samarbejdet mellem medlemsstaterne, EU-institutionerne og EU-agenturerne samt tredjelande og organisationer, herunder den private sektor.

¹⁶¹ EMPACT's fælles aktionsdage: "operation BOSPHORUS", 1 776 beslaglagte skydevåben (2.-11. november), "[Fællesaktionsdage Mobile 3: over 350 stjålne biler og 1 000 stjålne bildele blev fundet](#)", (12.-13. oktober), "[Fællesaktionsdage mod menneskehandel med henblik på udnyttelse som arbejdskraft](#)", "[politikfolk identificerede 715 potentielle ofre \(14.-20. september\)](#)", "[Fællesaktionsdage mod kriminalitet i Sydøsteuropa](#)", 51 våben af forskellige typer og 47 kg forskellige narkotika beslaglagt (september).

og bekæmpelse af onlinekriminalitet¹⁶². Den uafhængige evaluering af EU-politikcyklussen 2018-2021/EMPACT i 2020¹⁶³ konkluderede, at EMPACT er stadig mere relevant og effektiv med hensyn til at tackle de mest presserende trusler fra organiserede kriminelle grupper. Merværdien opnås ved at skabe en platform for samarbejde, der sætter medlemsstaterne i stand til at opnå bedre resultater i kampen mod grov og organiseret kriminalitet, end hvis de havde håndteret disse spørgsmål alene. Evalueringen påviste også muligheder og indeholdt anbefalinger til videreudvikling af dette meget nyttige samarbejdsredskab for den næste cyklus 2022-2025.

Kommissionen vil i 2021 iværksætte et initiativ til **en EU-kodeks for politisamarbejde** med henblik på at strømline, forbedre, udvikle, modernisere og lette retshåndhævelsessamarbejdet mellem de relevante nationale agenturer. Dette vil være til stor støtte for medlemsstaterne i deres kamp mod grov og organiseret kriminalitet og terrorisme.

Der er også behov for samarbejde mellem **politiet og andre centrale retshåndhævende myndigheder** samt med agenturer som f.eks. toldmyndighederne. EU's **toldmyndigheder** spiller en central rolle med hensyn til at sikre de ydre grænser og forsyningskæden og bidrager dermed til at skabe sikkerhed inden for Den Europæiske Unions grænser. Nye og skiftende trusler berører de vigtigste indbyrdes forbindelser mellem toldmyndigheder og retshåndhævende myndigheder og understreger navnlig toldkontrollens "afslørings-/forebyggelsesværdi" og toldmyndighedernes ledende rolle i forbindelse med varer. Kommissionen har støttet og fremmet samarbejdet mellem toldvæsenet og Europol¹⁶⁴, hvilket har haft en direkte indflydelse på indsatsen på områder som skydevåben, miljøkriminalitet, finansiering af kriminalitet og cybersikkerhed. Toldmyndighederne deltager i øjeblikket i en række EU-ledede aktioner mod alvorlig og international organiseret kriminalitet¹⁶⁵ samt i Ceps uddannelsesaktiviteter. Disse aktiviteter bidrager til at fremme og videreudvikle samarbejdet mellem agenturerne og forbedre samspillet mellem de vigtigste aktører.

Stærke og effektive informationssystemer er uundværlige for en bedre udveksling af oplysninger mellem retslige og retshåndhævende myndigheder i hele EU. **Schengeninformationssystemet (SIS)** er også blevet styrket takket være ajourførte regler, der afhjælper potentielle mangler gennem oprettelsen af yderligere kategorier af indberetninger, udvidelse af listen over genstande, for hvilke der kan indlæses indberetninger, og tilladelse til indlæsning af nye typer oplysninger¹⁶⁶. De nye regler trådte i kraft den 28. december 2018 og skulle være fuldt operationelle senest i december 2021¹⁶⁷.

¹⁶² Alle detaljerede faktablade med resultater og tal for EMPACT's kriminalitetsprioriteter kan ses her: <https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/da/pdf>, Dok. 7623/20 5. maj 2020.

¹⁶³ Rådets konklusioner af 27. marts 2017 omfattede en uafhængig evaluering af videreførelsen af EU-politikcyklussen for organiseret og grov international kriminalitet for perioden 2018-2021 (7704/17).

¹⁶⁴ Se f.eks. handlingsplanen fra Toldsamarbejdsgruppen. Nøgleområderne for 2020-2021 omfatter: øget tilstedeværelse af toldembedsmænd i forbindelseskantorerne i Europol, direkte adgang for toldmyndighederne til Europols netværksprogram for sikker informationsudveksling (SIENA), bedre repræsentation af toldembedsmænd i de nationale Europolenheder og politi- og toldchefers deltagelse i den europæiske politichefkonvention.

¹⁶⁵ Afgiftssvig/momssvig, ulovlig handel med skydevåben, miljøkriminalitet, finansiering af kriminalitet og bekæmpelse af seksuelt misbrug af børn.

¹⁶⁶ Forordning (EU) 2018/1860, forordning (EU) 2018/1861 og forordning (EU) nr. 2018/1862.

¹⁶⁷ SIS vil også blive ajourført i overensstemmelse med de foreslåede ændringer af Europolforordningen (COM (2020) XXX).

Tilsvarende blev **det europæiske informationssystem vedrørende strafferegistre (ECRIS)** i 2019 suppleret med endnu et system, som muliggør effektiv udveksling af strafferegisteroplysninger om tredjelandstatsborgere, der er dømt i EU (ECRIS-TCN). Arbejdet med den tekniske udvikling og gennemførelsen af dette nye centraliserede system er i gang, og systemet forventes at træde i kraft i 2023.

Den 24. juli 2020 vedtog Kommissionen rapporten om gennemgang af direktivet om passagerlisteoplysninger (PNR-oplysninger)¹⁶⁸, der indeholder en gennemgang af PNR-direktivets første to anvendelsesår¹⁶⁹. Dette viser, at udviklingen af PNR-systemet i hele EU er godt i gang. Anvendelsen af PNR-oplysninger er afgørende for bekæmpelsen af terrorisme, grov kriminalitet og organiseret kriminalitet og har allerede givet håndgribelige resultater. Kun én medlemsstat har endnu ikke givet Kommissionen meddelelse om fuld gennemførelse¹⁷⁰. Den 3. december 2020 fremsendte Kommissionen en begrundet udtalelse om manglende meddelelse om fuld gennemførelse af direktivet.

Den 9. september 2020 offentliggjorde Kommissionen evalueringen af **direktivet om forhåndsinformation om passagerer** fra 2004¹⁷¹. Evalueringen fremhæver en række mangler og uoverensstemmelser, som vil indgå i den kommende revision af den nuværende juridiske ramme. Et andet vigtigt instrument, der undersøges nærmere, er **Prümafgørelserne**¹⁷², som vil blive vurderet i lyset af den operationelle, teknologiske, kriminaltekniske og databeskyttelsesmæssige udvikling.

Samarbejdet skal også række ud over EU og inddrage **vigtige tredjelande i bekæmpelsen af terrorisme og organiseret kriminalitet**. Den 13. maj 2020 gav Rådet bemyndigelse til at indlede forhandlinger med New Zealand om udveksling af personoplysninger mellem Europol og New Zealand. Der pågår forhandlinger med Tyrkiet, men der er ikke gjort fremskridt i forhandlingerne med Algeriet, Egypten, Israel, Jordan, Libanon, Marokko og Tunesien om udveksling af personoplysninger med henblik på bekæmpelse af grov kriminalitet og terrorisme. Desuden vedtog Kommissionen den 19. november 2020 en henstilling med henblik på Rådets afgørelse om bemyndigelse til at indlede forhandlinger om en aftale mellem Den Europæiske Union og ti tredjelande om samarbejde mellem Eurojust og de pågældende tredjelande om udveksling af personoplysninger¹⁷³.

Med hensyn til **det internationale samarbejde om udveksling af PNR-oplysninger** med henblik på bekæmpelse af terrorisme og grov kriminalitet gav Rådet bemyndigelse til at indlede forhandlinger med Japan om undertegnelse af en PNR-aftale¹⁷⁴. I mellemtiden er **de fælles evalueringer af de eksisterende aftaler mellem EU og USA og mellem EU og Australien ved at blive afsluttet**. Kommissionen har også iværksat en revision af sin nuværende overordnede tilgang til overførsel af PNR-oplysninger til tredjelande¹⁷⁵.

¹⁶⁸ COM(2020) 305 final.

¹⁶⁹ Direktiv (EU) 2016/681.

¹⁷⁰ Slovenien

¹⁷¹ SWD(2020) 174.

¹⁷² Prümrammen muliggør elektronisk udveksling af DNA-oplysninger, fingeraftryksoplysninger og oplysninger fra køretøjsregistre mellem retshåndhævende myndigheder. En indledende konsekvensanalyse er blevet offentliggjort.

¹⁷³ De foreslåede tredjelande er følgende: Algeriet, Armenien, Bosnien-Hercegovina, Egypten, Israel, Jordan, Libanon, Marokko, Tunesien og Tyrkiet, COM(2020) 743 final.

¹⁷⁴ 18. februar 2020.

¹⁷⁵ Køreplan for den eksterne dimension af EU's politik for passagerlisteoplysninger findes på: <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records->

Kommissionen samarbejder tillige med FN om at øge partnerlandenes kapacitet til at forebygge, afsløre, efterforske og retsforfølge terrorhandlinger og andre alvorlige forbrydelser ved at indsamle og analysere passageroplysninger, både API- og PNR-oplysninger.

Kommissionen indledte processen med at lette overførslen af PNR-oplysninger i overensstemmelse med EU's retlige krav inden for rammerne af de nye PNR-standards¹⁷⁶, der er vedtaget af Organisationen for International Civil Luftfart (ICAO)¹⁷⁷. Den 23. juni 2020 vedtog ICAO-Rådet de nye standarder og den anbefalede praksis (SARP) vedrørende PNR¹⁷⁸, og dets kontraherende parter har indtil den 30. januar 2021 til at underrette ICAO om eventuelle forskelle mellem deres nationale reguleringspraksis og de nye PNR-SARP'er.

2. Bidraget fra stærke ydre grænser

Moderne og effektiv forvaltning af de ydre grænser er nøglen til at garantere EU-borgernes sikkerhed. Inddragelse af alle relevante aktører for at skabe størst mulig sikkerhed ved grænsen og give dem passende redskaber kan have en reel indvirkning på forebyggelsen af grænseoverskridende kriminalitet og terrorisme. I den nye pagt om migration og asyl¹⁷⁹ fremhævede man også behovet for en solid og retfærdig forvaltning af de ydre grænser, herunder identitetskontrol, sundheds- og sikkerhedskontrol. Dette er en del af den samlede tilgang, som viser, hvordan politikken for migration, asyl, integration og grænseforvaltning afhænger af fremskridt på alle fronter.

Den nye pagt understregede, at et effektivt Schengenområde er nødvendigt for migrationspolitikken, og at det også har vidtrækkende sikkerhedsmæssige konsekvenser. Dette blev drøftet på det første Schengenforum den 30. november 2020. Repræsentanter for medlemsstaterne og Europa-Parlamentet var enige om betydningen af et effektivt Schengensamarbejde for borgernes frie bevægelighed og sikkerhed. Denne proces vil indgå i en ny Schengenstrategi, som skal fremlægges i 2021. Schengenevaluerings- og overvågningsmekanismen er et vigtigt redskab til at sikre gensidig tillid og en bedre og sammenhængende gennemførelse af Schengenreglerne, herunder de sikkerhedsmæssige konsekvenser. Dette var et vigtigt emne i statusrapporten, der blev vedtaget den 25. november¹⁸⁰, over gennemførelsen af Schengenreglerne og over, hvordan Schengenevaluerings- og overvågningsmekanismen fungerer.

Interoperabilitetsforordningerne¹⁸¹ er udformet med henblik på at sikre samarbejde mellem eksisterende og nye eller opgraderede EU-informationssystemer, således at sikkerheds-, grænse- og migrationsstyringen foregår på en mere intelligent og effektiv måde. Interoperabilitet mellem EU's informationssystemer vil forbedre effektiviteten af kontrollen ved de ydre grænser, bidrage til at forebygge irregulær indvandring og også til et højt sikkerhedsniveau. Det vil være et værdifuldt ekstra redskab for retshåndhævende

¹⁷⁶ Rådets afgørelse 2019/2107.

¹⁷⁷ Sikkerhedsrådets resolution 2396 (2017).

¹⁷⁸ Benævnt ændring 28 til bilag 9 (Lettelse) til konventionen om international civil luftfart ("Chicagokonventionen").

¹⁷⁹ COM(2020) 609 final.

¹⁸⁰ SWD(2020) 327 final.

¹⁸¹ Forordning (EF) nr. 2019/817 og forordning (EU) 2019/818.

myndigheder og grænsemyndigheder¹⁸². Medlemsstaterne, de associerede Schengenlande og de relevante EU-agenturer (eu-LISA, Det Europæiske Agentur for Grænse- og Kystbevogtning og Europol) skal stå klar, og Kommissionen overvåger forberedelserne og beredvilligheden til at sikre fuld gennemførelse inden udgangen af 2023.

Der blev den 8. december 2020 opnået foreløbig enighed mellem medlovgiverne om forslaget om at **ajourføre visuminformationssystemet**¹⁸³.

En række vigtige retsakter er dog endnu ikke vedtaget. Europa-Parlamentet skal nå til enighed om at ville samarbejde med Rådet om ændringerne¹⁸⁴ af EU-systemet vedrørende rejseinformation og rejsetilladelse (ETIAS)¹⁸⁵.

Forbindelserne mellem relevante informationssystemer til sikkerhedsrisikoanalyse er afgørende for at øge vores sikkerhed. Styrkelse af **samarbejdet mellem told- og grænsekontrolmyndighederne** og synergierne mellem deres **informationssystemer** i overensstemmelse med relevante kontrolforanstaltninger, herunder beskyttelse af personoplysninger og lovgivning om beskyttelse af privatlivets fred, er en prioritet i handlingsplanen om at få toldunionen op på næste niveau den 28. september 2020¹⁸⁶. En foreløbig vurdering foretaget af Kommissionen i samarbejde med politi- og toldeksperter fra medlemsstaterne indeholder navnlig en anbefaling af en sammenkobling mellem Schengeninformationssystemet (SIS) og Europol-data med toldimportkontrollsystemet (ICS2)¹⁸⁷, og der vil nu blive iværksat en feasibilityundersøgelse heraf.

Forordningen om den europæiske grænse- og kystvagt¹⁸⁸ trådte i kraft i december 2019 og er en omfattende ajourføring af EU's kapacitet og redskaber til at styrke EU's ydre grænser. Dette vil gøre det muligt at øge grænsernes bidrag til sikkerheden betydeligt. Det nye mandat styrker Frontex' evne til at støtte medlemsstaterne i forvaltningen af de ydre grænser og tilbagesendelser og udvider mulighederne for samarbejde med tredjelande. Der arbejdes på at sikre, at den europæiske grænse- og kystvagts stående korps er klar til sin første indsættelse den 1. januar 2021.

I juni 2019 indførte EU **strammere sikkerhedsstandarder for ID-kort** for at lette EU-borgernes frie bevægelighed og samtidig mindske identitetssvig¹⁸⁹. Medlemsstaterne skal begynde at udstede identitetskort og opholdsdokumenter med nye sikkerhedsstandarder fra august 2021. De fleste af dem er i øjeblikket i færd med at tilpasse deres dokumentdesign til kravene i forordningen.

3. Styrkelse af forskning og innovation på sikkerhedsområdet

Forskning i sikkerhed og fremme af innovation understøtter en koordineret EU-reaktion på komplekse udfordringer og giver mulighed for konkrete skridt til at afbøde risici.

¹⁸² Eksisterende systemer: Schengeninformationssystemet, (SIS) visuminformationssystemet (VIS) og Eurodac, og fremtidige systemer: ind- og udrejsesystemet, EU-systemet vedrørende rejseinformation og rejsetilladelse (ETIAS) og det europæiske informationssystem vedrørende strafferegistre for tredjelandssstatsborgere (ECRIS-TCN).

¹⁸³ COM(2019) 12

¹⁸⁴ COM(2019) 3 final og COM(2019) 4 final.

¹⁸⁵ Forordning (EU) 2018/1240 og forordning (EU) nr. 2018/1241.

¹⁸⁶ COM(2020) 581 final.

¹⁸⁷ System med forhåndsoplysninger om fragt, der anvendes til tidlig sikkerhedsrisikovurdering af alle varebevægelser, som passerer den ydre grænse.

¹⁸⁸ Forordning (EU) 2019/1896.

¹⁸⁹ Forordning (EU) 2019/1157.

Sikkerhedsunionen er et af fire fokusområder i arbejdsprogrammet for **Horisont 2020 for 2018-2020**¹⁹⁰, som tegner sig for 50 % af den samlede offentlige finansiering af sikkerhedsforskning i EU. Forslagsindkaldelserne vedrørende sikkerhedsforskning under Horisont 2020 i 2019 førte til, at der blev udvalgt 42 projekter, som modtog i alt 253 mio. EUR i EU-støtte. Arbejdet vil omfatte beskyttelse af infrastruktur, øget modstandsdygtighed over for katastrofer, bekæmpelse af kriminalitet og terrorisme og sikring af de ydre grænser samt forbedring af den digitale sikkerhed. Det vejledende budget for projekter i 2020 er på 265 mio. EUR. Dette omfatter en forslagsindkaldelse til 20 mio. EUR om kunstig intelligens, som vil støtte de europæiske retshåndhavende myndigheders opskalering af AI-kapaciteter, øge deres AI-kompetence og styrke samarbejdet. Det arbejde, der forberedes under det nye forskningsrammeprogram Horisont Europa, vil støtte gennemførelsen af EU's strategi for en sikkerhedsunion samt grænseforvaltnings- og sikkerhedsdimensionen i den nye pagt om migration og asyl, EU's politikker for katastrofeforebyggelse og EU-strategien for maritim sikkerhed¹⁹¹.

EU-finansieret sikkerhedsforskning har også vist sig at være effektiv med hensyn til at fremme samarbejde og støtte sikkerhedsaktører under covid-19-pandemien¹⁹². Støtten omfatter værktøjer til fælles epidemiologisk og kriminel risiko- og trusselvurdering og - efterforskning.

For at sikre udbredelsen af **innovative projekter** skal EU-agenturerne integreres i det eksisterende sikkerhedsforsknings- og innovationslandskab. Efter samlingen i Rådet (retlige og indre anliggender) i oktober 2019 er EU-agenturer og Kommissionens Fælles Forskningscenter i øjeblikket ved at oprette **EU's innovationsknudepunkt for indre sikkerhed** på grundlag af de eksisterende retlige mandater, og dette skal fungere som et samarbejdsnetværk for innovationslaboratorierne. Knudepunktet bliver en koordineringsmekanisme til støtte for de deltagende enheder, hvor de kan udveksle oplysninger og viden, oprette fælles projekter og formidle resultater og teknologiske løsninger af relevans for den indre sikkerhed¹⁹³.

Det **europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre** skal støtte innovation og industripolitik inden for cybersikkerhed. De skal styrke den europæiske cybersikkerhedskapacitet, beskytte vores økonomi og samfund mod cyberangreb, fastholde forskningsekspertise og styrke EU's konkurrenceevne. Triloger er i øjeblikket i gang.

4. Færdigheder og bevidsthed

Kendskab til sikkerhedsspørgsmål og tilegnelse af de fornødne færdigheder for at imødegå potentielle trusler er afgørende for at opbygge et mere modstandsdygtigt samfund med bedre rustede virksomheder, forvaltninger og enkeltpersoner. Det er også vigtigt, at ofrene kan udnytte deres rettigheder.

¹⁹⁰ EU har afsat ca. 91 mio. EUR til projekter, der forbedrer beskyttelsen af infrastrukturer, herunder kombinerede cybertrusler og fysiske trusler, forbedret og hurtig reaktion på hændelser og bedre informationsudveksling.

¹⁹¹ Under Horisont Europa vil klynge 3 navnlig støtte Kommissionens politiske prioriteter "Fremme af vores europæiske levevis", "Den europæiske grønne pagt" og "Europa klar til den digitale tidsalder".

¹⁹² Horisont 2020-aktioner til støtte for pandemiindsatsen kan findes på: <https://www.researchgate.net/publication/341287556>.

¹⁹³ Den Stående Komité for det Operationelle Samarbejde om den Indre Sikkerhed bekræftede den 21. februar 2020 kommissorium, hovedtræk og opgaver for samt forvaltning af EU's innovationsknudepunkt for indre sikkerhed.

Fagfolk inden for retshåndhævelse og retsvæsen

De covid-19-relaterede restriktioner påvirkede i høj grad Cepol, som var nødt til at annullere alle planlagte boligaktiviteter fra marts 2020. Disse særlige omstændigheder medførte også en stigende efterspørgsel efter onlinetjenester. I årets første fire måneder registrerede agenturet således en stigning på 30 % i virtuelle aktiviteter og på 100 % i antallet af onlinebrugere. Blandt de prioriterede uddannelsesområder for 2019-2021¹⁹⁴ er bekæmpelse af irregulær indvandring, terrorbekæmpelse, menneskehandel og cyberkriminalitet samt seksuelt misbrug af børn. Kommissionen forbereder i øjeblikket evalueringen af Cepol, som skal være afsluttet i juli 2021.

Den brede offentlighed

Kampagnen **#SaferInternet4EU** blev lanceret på Safer Internet-dagen 2018. Aktiviteterne er nået ud til næsten 63 millioner mennesker i EU i de sidste to år og omfatter priser, støtte til lærere og cyberhygiejne. Netværket af Safer Internet-centre omfatter mere end 1 800 nye fagfolk inden for emner som falske nyheder, cybermobning, bekymringer over privatlivets fred, grooming og cyberhygiejne.

Oktober 2020 var EU's 8. europæiske **måned for cybersikkerhed**, hvor onlinesikkerhed fremmes i EU. Dette års kampagne handlede om at løse sikkerhedsspørgsmål i forbindelse med digitaliseringen af dagligdagen, et behov, som er fremskyndet af covid-19-pandemien. Kampagnen tilskyndede folk til at "Think Before U Click" (tænk, før du klikker) og belyste forskellige cybersikkerhedstemaer for at hjælpe brugerne med at identificere og forberede sig på cybertrusler. Den europæiske cybersikkerhedsudfordring i 2021 i Prag er under forberedelse.

Et vigtigt redskab til at hjælpe ofre for cyberkriminalitet er No More Ransom¹⁹⁵, et gratis dekrypteringsværktøj, der hjælper ofre med at gøre modstand uden at betale hackere. Med støtte fra Europol's Center til Bekæmpelse af IT-Kriminalitet fejrede det sit fireårsjubilæum i juli 2020, og siden oprettelsen har det registreret over 4,2 millioner besøgende fra 188 lande, hvilket har forhindrede, at ca. 632 mio. USD i løsepenge ender i kriminelles lommer.

Den 1. juli 2020 fremlagde Kommissionen den **europæiske dagsorden for færdigheder**¹⁹⁶ til støtte for bæredygtig konkurrenceevne, social retfærdighed og modstandsdygtighed. Den fastsætter ambitiøse, kvantitative mål for forbedring af de eksisterende færdigheder og uddannelse med fokus på nye færdigheder, der skal opnås inden for de næste fem år. Det omfatter særlige tiltag, som skal øge antallet af kandidater inden for naturvidenskab, teknologi, ingeniørvidenskab, humanistiske fag og matematik, som der er behov for inden for avancerede områder såsom cybersikkerhed. Den 10. november 2020 lancerede Kommissionen pagten for færdigheder i forbindelse med den femte udgave af den europæiske uge for erhvervskompetencer 2020. Den fremmer en fælles indsats for at maksimere virkningen af investeringer i forbedring af eksisterende kvalifikationer og uddannelse i nye færdigheder. Sammen med pagten er de første europæiske kvalifikationspartnerskaber blevet bebudet på tre områder: bilindustri, mikroelektronik samt luft-/rumfart og forsvar.

Den 30. september 2020 vedtog Kommissionen en række politiske strategier, som vil få stor betydning for udviklingen af EU's kapacitet til at opnå langsigtede

¹⁹⁴ Vurdering af EU's strategiske uddannelsesbehov 2018-2021, [EU-STNA report](#), CEPOL.

¹⁹⁵ <https://www.nomoreransom.org/>.

¹⁹⁶ COM(2020)274.

sikkerhedsfærdigheder. **Handlingsplanen for digital uddannelse for 2021-2027**¹⁹⁷ vil fremme et højtydende digitalt uddannelsesøkosystem med styrkede kompetencer til den digitale omstilling¹⁹⁸. Samme dag blev der vedtaget en meddelelse om det **europæiske uddannelsesområde** senest i 2025¹⁹⁹ med fokus på grundlæggende og digitale færdigheder. En meddelelse om et nyt **europæisk forskningsrum for forskning og innovation**²⁰⁰ udstikker vejen til at forbedre Europas forsknings- og innovationslandskab og fremskynde EU's overgang til digitalt lederskab samt bekæmpe kønsbaseret vold i alle dens former i forsknings- og innovationsorganisationer.

Programmet Erasmus+ bidrager også til at bekæmpe radikaliserings gennem projekter til bekæmpelse af radikaliserings, voldelig ekstremisme, social udstødelse, misinformation og falske nyheder²⁰¹. Et eksempel herpå er projektet om forebyggelse af radikaliserings i fængsler, der skal styrke frontlinjemedarbejderes kompetence til at identificere, rapportere og fortolke signaler om radikaliserings og reagere hensigtsmæssigt²⁰². Projektet No Hate Bootcamp hjalp ungdomsarbejdere med at blive ambassadører for bekæmpelse af hadefulde tale i deres lokalsamfund.

Kommissionen søger selv at inddrage offentligheden i overvejelserne om EU's sikkerhedspolitik. Tiltag på EU-plan er blevet gjort mere synlige og tilgængelige for borgerne via det nye **websted om EU's sikkerhedsstrategi**²⁰³. Der er iværksat flere **offentlige høringer**, som giver borgerne mulighed for at udøve direkte påvirkning af udformningen af politikker.

Alle ofre for kriminalitet har ret til støtte og beskyttelse, men ofre for de alvorligste forbrydelser såsom terrorisme og seksuel udnyttelse af børn kræver særlig opmærksomhed. Den 24. juni 2020 vedtog Kommissionen sin første **EU-strategi for ofres rettigheder (2020-2025)**²⁰⁴. Dette vedrører ofre for alle forbrydelser, men med særlig vægt på de mest sårbare, herunder ofre for terrorisme, børneofre for seksuel udnyttelse og ofre for menneskehandel. Den 22. september 2020 afholdt Kommissionen en konference på højt plan om ofres rettigheder, hvor den indviede **platformen for ofres rettigheder** for at fremme en mere horisontal tilgang til ofres rettigheder²⁰⁵. Kommissionen har også udpeget sin første **koordinator for ofres rettigheder** for at støtte en sammenhængende og effektiv politik for ofres rettigheder.

Med hensyn til **ofre for terrorisme** blev EU's ekspertisecenter for ofre for terrorisme oprettet i januar 2020. Centret tilbyder ekspertise, vejledning og støtte til nationale

¹⁹⁷ COM(2020) 624.

¹⁹⁸ https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf.

¹⁹⁹ COM(2020) 625 final.

²⁰⁰ COM(2020) 628 final.

²⁰¹ Indtil videre er der finansieret omkring 80 projekter relateret til radikaliserings: over 100 projekter vedrørende forebyggelse og bekæmpelse af cybermobning og mere end 100 om uddannelse i kritisk og etisk anvendelse af internettet med henblik på at bekæmpe desinformation på internettet.

²⁰² <http://www.r2pris.org/>.

²⁰³ https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_da.

²⁰⁴ COM(2020) 258.

²⁰⁵ Platformen samler de vigtigste aktører på EU-plan, herunder det europæiske netværk for ofres rettigheder, EU-netværket af nationale kontaktpunkter for erstatning, EU's antiterrorkoordinatør, relevante agenturer såsom Eurojust, Agenturet for Grundlæggende Rettigheder, Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse, Det Europæiske Institut for Ligestilling mellem Mænd og Kvinder og civilsamfundet.

myndigheder og støtteorganisationer for ofre. Det fremmer udveksling af bedste praksis og ekspertviden mellem fagfolk og specialister på tværs af grænserne. Det skal ikke yde direkte hjælp til bestemte ofre for terrorisme, men støtte nationale strukturer med at yde professionel bistand og støtte, herunder med retningslinjer, der skal offentliggøres i 2020. EU-centret er et pilotprojekt, der løber i to år. Rådets formandskab bakker op om dette med et netværk af fælles nationale kontaktpunkter for ofre for terrorisme.

VI KONKLUSION

Strategien for sikkerhedsunionen blev indført for at skabe en omfattende og dynamisk tilgang. De seneste terrorangreb har igen vist, hvordan EU skal kunne reagere, styrke vores modstandsdygtighed og reaktionsevne gennem modernisering og effektiv anvendelse af de vigtigste værktøjer, vi har til rådighed. De har også vist, at alle aktører skal engagere sig fuldt ud i en fælles tilgang, således at medlemsstaterne, EU-institutionerne, den private sektor, NGO'er og borgerne selv kan spille en rolle i opbygningen af et sikkerhedsgrundlag, der er tilstrækkeligt stærkt og fleksibelt til at kunne levere resultater. Denne sammenhængende, konsekvente tilgang er også den bedste måde til at sikre, at vores grundlæggende rettigheder beskyttes som en del af vores europæiske levevis.

Rapporten viser de mange arbejdsgange, der er undervejs, men også hvordan dynamikken skal opretholdes. Målet med EU's terrorbekæmpelsesdagsorden, der fremlægges i dag, er at styrke den europæiske ramme for terrorbekæmpelse ved at fastlægge de næste nødvendige skridt: at foregribe og forebygge terrorisme, beskytte borgerne og infrastrukturen og være rede til at reagere under hensyntagen til sammenhængen mellem intern og ekstern sikkerhed. Vi har allerede mere samarbejde, der gøres flere bestræbelser på at bekæmpe radikaliserings, og vi har flere redskaber til at fratage terrorister midlerne til at udføre et angreb. Nu skal dette tages et skridt videre. Derfor skal der vedtages nye regler for bekæmpelse af terrorrelateret onlineindhold, hvor det er en vigtig prioritet at nå til enighed i år. Kommissionen opfordrer også indtrængende medlemsstaterne til at fremskynde gennemførelsen af al vedtaget lovgivning. At skabe sikkerhed for EU-borgerne er et fælles ansvar, og en samlet indsats skal være den fælles ambition om et mere sikkert Europa.