EUROPA-
KOMMISSIONEN

Bruxelles, den 24.7.2020
COM(2020) 605 final

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

om strategien for EU's sikkerhedsunion

I. Indledning

Kommissionens politiske retningslinjer gjorde det klart, at vi må vende hver en sten i bestræbelserne på at beskytte vores borgere. Sikkerhed handler ikke alene om personlig sikkerhed, men beskytter ligeledes grundlæggende rettigheder og danner også grundlag for tillid og dynamik i vores økonomi, samfund og demokrati. Europæerne står i vor tid over for et sikkerhedslandskab i stadig forandring, der påvirkes af foranderlige trusler og andre faktorer, herunder klimaændringer, demografiske udviklingstendenser og manglende politisk stabilitet uden for vore grænser. Globalisering, fri bevægelighed og den digitale omstilling skaber fortsat velstand, gør vores liv lettere og fremmer innovation og vækst. Men med disse fordele følger iboende risici og omkostninger. Terrorisme, organiseret kriminalitet, narkotikahandel og menneskehandel kan manipulere med sikkerheden og udgør direkte trusler mod borgerne og vores europæiske levevis. Cyberangreb og cyberkriminalitet forekommer stadig oftere. Sikkerhedstruslerne bliver også mere komplekse: de næres af mulighederne for at arbejde på tværs af grænserne og af den høje grad af sammenkobling. De udnytter udviskningen af grænserne mellem den fysiske og den digitale verden. De udnytter sårbare grupper og sociale og økonomiske forskelle. Angrebene kan udføres med et øjebliks varsel og efterlade få eller ingen spor. Både statslige og ikkestatslige aktører kan benytte en bred vifte af hybride trusler[1], og begivenheder uden for EU kan få kritisk betydning for sikkerheden i EU.

Covid-19-krisen har også ændret vores opfattelse af sikkerhedstrusler og tilknyttede politikker. Krisen har sat fokus på behovet for at garantere sikkerheden i såvel det fysiske som det digitale miljø. Den har understreget betydningen af åben strategisk autonomi for vores forsyningskæder med hensyn til kritiske produkter, tjenester, infrastrukturer og teknologi. Den har styrket behovet for at inddrage alle sektorer og alle enkeltpersoner i en fælles indsats for at sikre, at EU fra første færd er velforberedt, modstandsdygtig og råder over bedre værktøjer til at reagere ved behov.

Borgerne kan ikke beskyttes alene ved, at medlemsstaterne handler på egen hånd. Det har aldrig haft mere afgørende betydning at bygge videre på vores stærke sider med hensyn til at samarbejde, og aldrig har EU haft større potentiale til at gøre en forskel. EU kan foregå med et godt eksempel ved at styrke sit overordnede krisestyringssystem og ved inden for og uden for sine grænser at arbejde for at bidrage til den globale stabilitet. Selv om medlemsstaterne bærer hovedansvaret for sikkerheden, har de seneste år skabt en voksende forståelse af, at sikkerheden i én medlemsstat gavner sikkerheden for alle. EU kan yde en tværfaglig og integreret indsats, der kan bistå medlemsstaternes sikkerhedsaktører med de værktøjer og oplysninger, de har brug for[2].

EU kan også sørge for, at sikkerhedspolitikken fortsat forankres i vores fælles europæiske værdier — respekt for og opretholdelse af retsstatsprincippet, lighed[3] og grundlæggende rettigheder, og at der garanteres gennemsigtighed, ansvarlighed og demokratisk kontrol — for at give politikkerne den rette grobund af tillid. EU kan opbygge en effektiv og ægte

[1] Der findes adskillige definitioner på hybride trusler, men begrebet dækker over en blanding af indgribende og undergravende virksomhed med konventionelle og ukonventionelle midler (dvs. diplomatiske, militære, økonomiske eller teknologiske), som statslige eller ikkestatslige aktører anvender på koordineret vis for at opnå specifikke mål (uden at overskride tærsklen til formel krigsførelse). Jf. JOIN(2016) 18 final.

[2] Eksempelvis gennem de tjenester, der leveres af EU's rumprogram, såsom Copernicus, der leverer jordobservationsdata og programmer til grænseovervågning, maritim sikkerhed, retshåndhævelse, bekæmpelse af pirateri og narkosmugling og desuden katastrofeberedskab.

[3] Et EU med ligestilling: strategi for ligestilling mellem mænd og kvinder 2020-2025 (COM(2020) 152).

sikkerhedsunion, hvori enkeltpersoners rettigheder og frihedsrettigheder beskyttes. Sikkerhed og respekt for de grundlæggende rettigheder er ikke indbyrdes modstridende mål, men hænger sammen og er komplementære. Vores værdier og grundlæggende rettigheder skal danne grundlag for sikkerhedspolitikken og derigennem håndhæve nødvendigheds-, proportionalitets- og legalitetsprincippet og desuden garantere klare ansvarsforhold og mulighed for retlig prøvelse, samtidig med at vi sikrer grundlaget for en effektiv beskyttelse af personer, navnlig de mest sårbare.

Der er allerede indført betydelige retlige og praktiske værktøjer og støtteværktøjer, men der er behov for at styrke disse og gennemføre dem bedre. Der er gjort store fremskridt med at forbedre informationsudvekslingen og efterretningssamarbejdet mellem medlemsstaterne og lukke det rum, hvori terrorister og kriminelle opererer. Men fragmenteringen gør sig stadig gældende.

Arbejdet skal også række ud over EU's grænser. Beskyttelse af Unionen og dens borgere handler ikke længere kun om at sørge for sikkerheden inden for EU's grænser, men også om at tage hånd om den eksterne dimension af sikkerheden. EU's tilgang til ekstern sikkerhed inden for rammerne af den fælles udenrigs- og sikkerhedspolitik (FUSP) og den fælles sikkerheds- og forsvarspolitik (FSFP) vil fortsat være et afgørende element i EU's bestræbelser på at øge sikkerheden i EU. Samarbejde med tredjelande og på globalt plan om at overvinde fælles udfordringer har afgørende betydning for en effektiv og helhedsorienteret reaktion, hvor stabilitet og sikkerhed i EU's nabolande har kritisk betydning for EU's egen sikkerhed.

Med udgangspunkt i Europa-Parlamentets[4], Rådets[5] og Kommissionens[6] hidtidige arbejde viser denne nye strategi, at en ægte og effektiv sikkerhedsunion vil skulle kombinere en solid kerne af instrumenter og politikker for at skabe sikkerhed i praksis, idet det anerkendes, at sikkerhedsaspektet berører alle dele af samfundet og alle offentlige politikker. EU må sørge for et sikkert miljø for alle uanset race eller etnisk oprindelse, religion, tro, køn, alder eller seksuel orientering.

Denne strategi dækker perioden 2020-2025 og fokuserer på at opbygge kompetencer og kapacitet til at sørge for et fremtidssikret sikkerhedsmiljø. Den rummer en sikkerhedstilgang, som inddrager hele samfundet, og som effektivt kan sætte ind over for et trusselsbillede i hastig forandring på en koordineret måde. Den fastlægger de strategiske prioriteter og de tilhørende foranstaltninger til at håndtere digitale og fysiske risici på en integreret måde i hele sikkerhedsunionens økosystem, idet hovedvægten lægges på områder, hvor EU kan tilføre merværdi. Målet er at tilbyde et sikkerhedsudbytte for at beskytte alle i EU.

II. Et europæisk sikkerhedsmæssigt trusselsbillede i hastig forandring

Borgernes sikkerhed, velstand og trivsel afhænger af deres sikkerhed. Truslerne mod denne sikkerhed afhænger af, i hvilket omfang deres liv og eksistensgrundlag er sårbare. Jo større

[4] F.eks. arbejdet i Europa-Parlamentets TERR-udvalg, som aflagde rapport i november 2018.

[5] Rådets konklusioner fra juni 2015 om en "ny strategi for den indre sikkerhed" til Rådets senere konstateringer fra december 2019.

[6] "Gennemførelse af den europæiske dagsorden om sikkerhed for at bekæmpe terrorisme og bane vejen for en effektiv og ægte sikkerhedsunion" (COM(2016) 230 final af 20.4.2016). Jf. den nylige vurdering af gennemførelsen af lovgivningen på området for indre sikkerhed: gennemførelse af lovgivningen vedrørende indre anliggender på området indre sikkerhed — 2017-2020 (SWD(2020) 135).

sårbarheden er, desto større er risikoen for, at den udnyttes. Både sårbarheder og trusler er under stadig forandring, og EU er nødt til at tilpasse sig.

Vores dagligdag afhænger af en lang række forskellige tjenester — f.eks. energi, transport, finansiering og sundhed. Disse afhænger af både fysisk og digital infrastruktur, hvilket øger sårbarheden over for og potentialet for afbrydelser. Under covid-19-pandemien har ny teknologi sikret den fortsatte drift af mange virksomheder og offentlige tjenester både ved at give os netadgang via telearbejde og ved at opretholde forsyningslogistikkæder. Men derved er vejen også banet for en ekstraordinær stigning i ondsindede angreb, hvormed det i kriminelt øjemed forsøges at drage fordel af de ekstraordinære tilstande som følge af pandemien og overgangen til hjemmearbejde via digitale medier[7]. Mangel på varer har skabt nye muligheder for organiseret kriminalitet. Følgerne kunne have været fatale og forstyrret livsvigtige sundhedstjenester på et tidspunkt, hvor de blev udsat for et maksimalt pres.

De stadig flere måder, hvorpå den digitale teknologi letter vores tilværelse, har også gjort **cybersikkerhed** til et spørgsmål af strategisk betydning[8]. Boliger, banker, finansielle tjenesteydelser og virksomheder (især små og mellemstore virksomheder) påvirkes i høj grad af cyberangreb. Den potentielle skade øges mangefold på grund af de fysiske og digitale systemers indbyrdes afhængighed: Enhver fysisk påvirkning vil uvægerligt påvirke de digitale systemer, samtidig med at cyberangreb på informationssystemer og digitale infrastrukturer kan bringe væsentlige tjenester til ophør.[9]. Det fremspirende tingenes internet og den voksende udnyttelse af kunstig intelligens vil udmønte sig i nye fordele såvel som nye risici.

Vores verden er afhængig af digitale infrastrukturer, teknologier og onlinesystemer, som sætter os i stand til at skabe forretningsmuligheder, forbruge produkter og benytte tjenester. Det afhænger alt sammen af kommunikation og interaktion. Afhængigheden af internettet har åbnet døren for en bølge af **cyberkriminalitet**[10]. "Cybercrime as-a-service" og den skjulte cyberkriminelle økonomi giver nem online adgang til cyberkriminelles produkter og tjenester. Kriminelle tilpasser sig hurtigt til at bruge ny teknologi for egen vindings skyld. For eksempel har kopimedicin og forfalskede lægemidler infiltreret den lovlige lægemiddelforsyningskæde.[11]. Den eksponentielle vækst i børnepornografisk materiale på internettet[12] har vist de sociale konsekvenser af kriminelles ændrede adfærdsmønstre. En nylig undersøgelse viste, at størstedelen af EU-befolkningen (55 %) er bekymrede over, hvorvidt kriminelle og svindlere har adgang til deres data[13].

---

7 Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (april 2020).

8 Kommissionens henstilling om cybersikkerheden i forbindelse med 5G-net (C(2019) 2335). Meddelelse om en EU-værktøjskasse til udrulning af sikre 5G-net i EU (COM(2020) 50).

9 I marts 2020 blev Brno University Hospital i Tjekkiet udsat for et cyberangreb, som tvang det til at omdirigere patienter og udsætte operationer (Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis). Kunstig intelligens kan misbruges til digitale, politiske og fysiske angreb foruden overvågning. Indsamlingen af data fra tingenes internet kan anvendes til at overvåge enkeltpersoner (smarture, virtuelle assistenter mv.).

10 Ifølge nogle fremskrivninger vil omkostningerne ved brud på datasikkerheden årligt nå op på 5 bio. USD pr. år senest i 2024, en stigning fra 3 bio. USD pr. år i 2015 (Juniper Research, The Future of Cybercrime & Security).

11 Ifølge en undersøgelse fra 2016 (Legiscript) anslås det, at blot 4 % af internetapotekerne verden over opererer lovligt, og at EU's forbrugere udgør det primære mål for de 30 000-35 000 ulovlige onlineapoteker på nettet.

12 EU-strategi for en mere effektiv bekæmpelse af seksuelt misbrug af børn (COM(2020) 607).

13 Den Europæiske Unions Agentur for Grundlæggende Rettigheder (2020), Your rights matter: Security concerns and experiences, Fundamental Rights Survey, Luxembourg, Publikationskontoret.

Det **globale miljø** forstærker også disse trusler. Tredjelandes assertive industripolitik sammenholdt med et vedvarende cyberbaseret tyveri af intellektuel ejendom ændrer det strategiske paradigme for at beskytte og fremme europæiske interesser. Dette forstærkes af væksten inden for teknologi med dobbelt anvendelse, hvilket gør en stærk civil teknologisektor til et stærkt aktiv for forsvars- og sikkerhedsforanstaltningerne. Industrispionage påvirker i betydelig grad EU's økonomi, beskæftigelse og vækst: cybertyveri af forretningshemmeligheder anslås at koste EU 60 mia. EUR[14]. Derfor må det overvejes grundigt, hvordan afhængighedsforhold og den øgede eksponering for cybertrusler påvirker EU's kapacitet til at beskytte såvel enkeltpersoner som virksomheder.

Covid-19-krisen har også understreget, hvordan sociale kløfter og uvished skaber en sikkerhedssårbarhed. Dette øger potentialet for mere avancerede og **hybride angreb** fra statslige og ikkestatslige aktører, idet sårbarheder udnyttes gennem en blanding af cyberangreb, skade på kritisk infrastruktur[15], desinformationskampagner og radikalisering af den politiske narrativ[16].

Samtidig sker der en løbende videreudvikling af flere traditionelle trusler. **Terrorangreb** udviste en nedadgående tendens i EU i 2019. Truslen om jihadistiske angreb mod EU fra eller inspireret af Da'esh og al-Qaeda og deres sympatisører er dog fortsat høj[17]. Samtidig vokser truslen fra voldelig højreekstremisme også[18]. Racistisk inspirerede angreb giver også anledning til alvorlig bekymring: De dødbringende antisemitiske terrorangreb i Halle var en påmindelse om behovet for at optrappe indsatsen i overensstemmelse med Rådets erklæring af 2018[19]. En ud af fem personer i EU er meget bekymrede for, at et terrorangreb vil finde sted i løbet af de næste 12 måneder[20]. Langt størstedelen af de seneste terrorangreb har været "lavteknologiske" angreb begået af soloaktører mod enkeltpersoner i det offentlige rum, og samtidig fik terrorpropagandaen online et nyt aspekt med den direkte streaming af angrebene i Christchurch[21]. Truslen fra radikaliserede individer er fortsat høj — muligvis støttet af hjemvendte udenlandske terrorkrigere og ekstremister, der løslades fra fængsler[22].

Krisen har også vist, hvordan eksisterende trusler kan udvikle sig under nye omstændigheder. **Organiserede kriminelle grupper** har udnyttet manglen på varer til at skabe nye illegale markeder. Handel med illegale stoffer er fortsat det største kriminelle marked i EU, der anslås at have en minimumsværdi i detailleddet på 30 mia. EUR om året i EU [23]. Menneskehandel finder stadig sted: skønsmæssigt beløber den årlige globale

---

14 The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018.

15 Kritisk infrastruktur er væsentlig for vitale samfundsmæssige funktioner, menneskers sundhed, sikkerhed og økonomisk og social velfærd, og en afbrydelse eller ødelæggelse heraf får væsentlige konsekvenser (Rådets direktiv 2008/114/EF).

16 97 % af EU-borgerne er blevet konfronteret med falske nyheder, 38 % dagligt. Jf. JOIN(2020) 8 final.

17 13 EU-medlemsstater indberettede i alt 119 fuldførte, mislykkede eller afværgede terrorangreb med ti dræbte og 27 tilskadekomne (Europol, European Union Terrorism Situation and Trend Report, 2020).

18 Der blev udført seks højreekstremistiske terrorangreb i tre medlemsstater i 2019 (ét blev fuldført, ét mislykkedes og fire blev afværget) sammenholdt med kun ét i 2018, og der måtte noteres et yderligere antal dræbte i tilfælde, der ikke er klassificeret som terrorisme (Europol, 2020).

19 Se også Rådets erklæring om bekæmpelse af antisemitisme og udvikling af en fælles sikkerhedsstrategi for bedre at beskytte jødiske samfund og institutioner i Europa.

20 EU's Agentur for Grundlæggende Rettigheder: Your rights matter: Security concerns and experiences, 2020.

21 Fra juli 2015 og frem til udgangen af 2019 fandt Europol terrorindhold på 361 platforme (Europol, 2020).

22 Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism, 2019.

23 EMCDDA and Europol EU Drugs Market Report 2019.

fortjeneste ved alle former for udnyttelse sig til næsten 30 mia. EUR[24]. Den internationale handel med forfalskede lægemidler nåede op på 38,9 mia. EUR[25]. Samtidig giver en lav konfiskationsprocent kriminelle mulighed for løbende at udvide deres kriminelle aktiviteter og infiltrere den lovlige økonomi[26]. Kriminelle og terrorister har stadig lettere ved at få adgang til skydevåben fra onlinemarkedet og ved hjælp af ny teknologi som f.eks. tre-d-printning[27]. Kunstig intelligens, ny teknologi og robotteknik vil yderligere øge risikoen for, at kriminelle udnytter fordelene ved innovation til ondsindede formål[28].

Disse trusler går på tværs af kategorier og rammer forskellige dele af samfundet på forskellige måder. De udgør alle en alvorlig trussel mod enkeltpersoner og virksomheder, og der er behov for en fyldestgørende og sammenhængende reaktion på EU-plan. Når sikkerhedssårbarheder kan hidrøre selv fra små, indbyrdes forbundne husholdningsprodukter såsom et internettilsluttet køleskab eller en kaffemaskine, kan vi ikke længere sætte vor lid til de traditionelle statslige aktører alene for at garantere vores sikkerhed. De økonomiske aktører må påtage sig et større ansvar for cybersikkerheden for så vidt angår de produkter og tjenester, de bringer i omsætning. Samtidig må enkeltpersoner have en i det mindste grundlæggende forståelse af cybersikkerhed for at kunne beskytte sig selv.

III. En koordineret EU-reaktion for hele samfundet

EU har allerede vist sig i stand til at tilføre en reel merværdi. Siden 2015 har sikkerhedsunionen skabt nye forbindelsesled i relation til håndteringen af sikkerhedspolitikkerne på EU-plan. Der må imidlertid gøres mere for at inddrage hele samfundet, herunder offentlige myndigheder på alle niveauer, alle erhvervsgrene og enkeltpersoner i alle medlemsstater. Den voksende bevågenhed om risiciene ved afhængighedsforhold[29] og behovet for en stærk europæisk industristrategi[30] er et argument for, at EU må sikre en kritisk masse af industri, teknologiproduktion og modstandsdygtighed i forsyningskæden. Styrke indebærer også fuld respekt for de grundlæggende rettigheder og EU's værdier: de er en forudsætning for legitime, effektive og holdbare sikkerhedspolitikker. I denne strategi for sikkerhedsunionen fastsættes konkrete opgaver, som der må arbejdes videre med. Den har følgende fælles mål som grundlag:

- ***Opbygning af kompetencer og kapacitet til hurtig opdagelse, forebyggelse og hurtig reaktion på kriser:*** EU må styrke sin modstandsdygtighed for at forebygge, afværge og modstå fremtidige chok. Kompetencer og kapacitet må opbygges således, at sikkerhedskriser opdages og afværges hurtigt ved hjælp af en integreret og koordineret

[24] Europols Report on Trafficking in Human Beings, Financial Business Model (2015).

[25] Rapporten fra Den Europæiske Unions Kontor for Intellektuel Ejendomsret og OECD om Trade in counterfeit pharmaceutical products.

[26] Rapport om inddrivelse og konfiskation af aktiver: skabe sikkerhed for, at forbrydelse ikke betaler sig (COM(2020) 217).

[27] I 2017 blev der anvendt skydevåben i 41 % af alle terrorangreb (Europol, 2018).

[28] I juli 2020 forelagde de franske og nederlandske retshåndhævende og retslige myndigheder sammen med Europol og Eurojust den fælles efterforskning med henblik på at gøre en ende på EncroChat; et krypteret telefonnet anvendt af kriminelle netværk, der er involveret i voldelige angreb, korruption, drabsforsøg og storstilede narkotikatransporter.

[29] Risikoen for at være afhængig af tredjelande består i en øget eksponering over for potentielle trusler, f.eks. misbrug af sårbarheder i IT-infrastrukturer, der bringer kritisk infrastruktur i fare (f.eks. energi, transport, bankvæsen og sundhed), kapring af industrielle styringssystemer, eller lettere adgang til at begå datatyveri eller spionage.

[30] Meddelelse fra Kommissionen — En ny industristrategi for Europa (COM(2020) 102).

tilgang, både globalt og gennem sektorspecifikke initiativer (såsom finanssektoren, energisektoren, de retslige og de retshåndhævende myndigheder, sundhedsplejen, den maritime sektor og transportsektoren), idet der tages afsæt i eksisterende værktøjer og initiativer[31]. Kommissionen vil også forelægge forslag om et vidtrækkende krisestyringssystem i EU, der også kan være relevant for sikkerheden.

- ***Fokus på resultater***: En resultatorienteret strategi skal bygge på en omhyggelig trussels- og risikovurdering for at målrette indsatsen bedst muligt. De rette regler og værktøjer vil skulle fastlægges og tages i anvendelse. Der er behov for pålidelige strategiske efterretninger som grundlag for EU's sikkerhedspolitik. Hvis der er behov for EU-lovgivning, skal den følges op, så den gennemføres fuldt ud, for at undgå opsplitning og mangler, der vil kunne udnyttes. En effektiv gennemførelse af denne strategi vil også afhænge af, at en passende finansiering sikres i den næste budgetperiode 2021-2027, herunder for tilknyttede EU-agenturer.
- ***Alle aktører i den offentlige og private sektor føres sammen i en fælles indsats:*** De centrale aktører i både den offentlige og private sektor har været tilbageholdende med at dele sikkerhedsrelevante oplysninger; det være sig af frygt for at bringe den nationale sikkerhed eller konkurrenceevnen i fare.[32]Men effektiviteten er størst, når alle parter støtter hinanden. For det første indebærer dette et mere intensivt samarbejde mellem medlemsstaterne, bl.a. de retshåndhævende og retslige myndigheder og andre offentlige myndigheder, og med EU-institutioner og -agenturer for at opbygge den forståelse og udveksling, der er nødvendig for at finde fælles løsninger. Samarbejde med den private sektor er også afgørende, så meget desto mere som industrien ejer en vigtig del af den digitale og ikkedigitale infrastruktur, der har central betydning for effektivt at kunne bekæmpe kriminalitet og terrorisme. Enkeltpersoner kan også selv bidrage, f.eks. ved at opbygge de færdigheder og den viden, der er nødvendig for at bekæmpe cyberkriminalitet eller desinformation. Endelig skal denne fælles indsats række ud over vores grænser og knytte tættere bånd til ligesindede partnere.

IV. Beskyttelse af alle i EU: Sikkerhedsunionens strategiske prioriteter

EU har enestående forudsætninger for at reagere på disse nye globale trusler og udfordringer. Ovennævnte trusselsanalyse har afdækket fire indbyrdes afhængige strategiske prioriteter, der må fremmes på EU-plan under fuld overholdelse af de grundlæggende rettigheder: i) et fremtidssikret sikkerhedsmiljø, ii) håndtering af foranderlige trusler, iii) beskyttelse af europæerne mod terrorisme og organiseret kriminalitet og iv) et stærkt europæisk sikkerhedsøkosystem.

1. Et fremtidssikret sikkerhedsmiljø

Beskyttelse af kritisk infrastruktur og modstandsdygtighed

Borgerne er afhængige af centrale infrastrukturer i dagligdagen for at kunne rejse, arbejde, drage fordel af vigtige offentlige tjenester som f.eks. hospitaler, transport, energiforsyning

[31] Eksempelvis de integrerede ordninger for politisk kriserespons (IPCR), katastrofeberedskabskoordinationscentret, Kommissionens henstilling om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (C(2017) 6100), EU's operationelle protokol for imødegåelse af hybride trusler (EU-drejebogen) SWD(2016) 227.

[32] Jf. fælles meddelelse om modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU (JOIN(2017) 450 final).

eller udøve deres demokratiske rettigheder. Er disse infrastrukturer ikke tilstrækkeligt beskyttede og robuste, kan angreb forårsage enorme forstyrrelser — såvel fysiske som digitale — både i de enkelte medlemsstater og potentielt i hele EU.

EU's eksisterende rammer for beskyttelse af og modstandsdygtighed for kritisk infrastruktur[33] har ikke holdt trit med den måde, hvorpå risiciene udvikler sig. Den voksende indbyrdes afhængighed indebærer, at forstyrrelser i én sektor umiddelbart kan påvirke driften i andre: et angreb på et elkraftværk kan afbryde telekommunikation, hospitaler, banker eller lufthavne, og et angreb på digital infrastruktur kan føre til forstyrrelser i elnet eller finansieringsnet. Efterhånden som vores økonomis og samfunds transaktioner i stigende grad foregår online, bliver risici i stil med ovennævnte stadig mere akutte. Lovrammen vil skulle tage højde for denne øgede indbyrdes forbundethed og indbyrdes afhængighed med robuste foranstaltninger til at beskytte kritisk infrastruktur og modstandsdygtighed — både i cyberspace og i den fysiske verden. Væsentlige tjenester, herunder tjenester baseret på ruminfrastruktur, må beskyttes tilstrækkeligt mod aktuelle og forventede trusler, men skal også være modstandsdygtige. Dvs. at systemet skal kunne forberede sig på og planlægge efter samt absorbere, genrejse sig efter og bedre tilpasse sig negative hændelser.

Samtidig har medlemsstaterne udøvet deres skønsbeføjelser ved at gennemføre gældende lovgivning på forskellige måder. Den deraf følgende fragmentering kan undergrave det indre marked og gøre det vanskeligere at koordinere på tværs af landegrænser — frem for alt i grænseregioner. Operatører, der leverer væsentlige tjenester i forskellige medlemsstater, skal overholde forskellige rapporteringsordninger. Kommissionen er i færd med at undersøge, om **nye rammer for både fysisk og digital infrastruktur** kan skabe større ensartethed og en mere sammenhængende tilgang til at sikre en pålidelig forsyning af væsentlige tjenester. Denne ramme skal ledsages af **sektorspecifikke initiativer**, hvormed de specifikke risici for kritiske infrastrukturer håndteres, f.eks. i relation til transport, rummet, energi, finans og sundhed[34]. I betragtning af den finansielle sektors betydelige afhængighed af IT-tjenester og dens betydelige sårbarhed over for cyberangreb vil et første skridt være et initiativ vedrørende modstandsdygtighed i de finansielle sektorers digitale operationer. Grundet energisystemets særlige følsomhed og rækkevidde vil et specifikt initiativ medvirke til at styrke modstandsdygtigheden for kritisk energiinfrastruktur mod fysiske trusler, cybertrusler og hybride trusler og dermed sikre lige vilkår for energioperatørerne på tværs af grænserne.

Udenlandske direkte investeringers sikkerhedsrelevante virkninger, der kan påvirke kritiske infrastrukturer eller kritisk teknologi, vil også indgå i EU-medlemsstaternes og Kommissionens vurderinger i relation til den nye europæiske ramme for screening af udenlandske direkte investeringer[35].

---

[33] Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016). Rådets direktiv 2008/114/EF om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre.

[34] I betragtning af det pres, sundhedssektoren har været udsat for, især under covid-19-krisen, vil Kommissionen også overveje initiativer, hvormed EU's rammer for sundhedssikkerhed og de ansvarlige EU-agenturer kan styrkes for at reagere på alvorlige grænseoverskridende sundhedstrusler.

[35] Med ikrafttrædelsen den 11. oktober 2020 af Europa-Parlamentets og Rådets forordning (EU) 2019/452 af 19. marts 2019 om et regelsæt for screening af udenlandske direkte investeringer i Unionen udrustes EU med en ny samarbejdsmekanisme angående tredjelandes direkte investeringer, som vil kunne påvirke sikkerheden eller den offentlige orden. Ifølge forordningen vil medlemsstaterne og Kommissionen vurdere de potentielle risici ved sådanne udenlandske direkte investeringer og, hvis det er hensigtsmæssigt og relevant for mere end én medlemsstat, foreslå tilstrækkelige midler til at afbøde disse risici.

EU kan også opbygge nye værktøjer til støtte for kritiske infrastrukturers modstandsdygtighed. Det globale internet har hidtil udvist en høj grad af modstandsdygtighed, navnlig hvad angår evnen til at støtte øgede datatrafikmængder. Vi er dog nødt til at være forberedt på eventuelle fremtidige kriser, der bringer internettets sikkerhed, stabilitet og modstandsdygtighed i fare. Det må sikres, at internettet til stadighed er fuldt operationelt, hvilket indebærer, at det skal kunne modstå cyberhændelser og ondsindede onlineaktiviteter, og det er vigtigt at begrænse afhængigheden af infrastrukturer og tjenester, som befinder sig uden for EU. Dette vil kræve en kombination af lovgivning og granskning af de eksisterende regler for at sørge for et højt fælles sikkerhedsniveau for nettet og informationssystemer i EU, tillige med øgede investeringer i forskning og innovation og en indsats for at ibrugtage eller befæste centrale internetinfrastrukturer og -ressourcer, navnlig domænenavnesystemet[36].

Et centralt element i beskyttelsen af centrale europæiske og nationale digitale aktiver går ud på at tilbyde kritiske infrastrukturer en kanal til sikker kommunikation. Kommissionen arbejder sammen med medlemsstaterne om at etablere en certificeret sikker ende-til-ende-kvanteinfrastruktur på land og i rummet kombineret med det sikre statslige satellitkommunikationssystem, der er fastlagt ved forordningen om rumprogrammet[37].

Cybersikkerhed

Antallet af cyberangreb stiger fortsat[38]. Disse angreb bliver stadig mere avancerede, de kommer fra en lang række kilder i og uden for EU, og de målrettes de områder, hvor sårbarheden er størst mulig. Statslige eller statsstøttede aktører er ofte involveret, og indsatsen rettes mod centrale digitale infrastrukturer, f.eks. store udbydere af cloudtjenester[39]. Cyberrisici er har også vist sig at udgøre en betydelig trussel mod det finansielle system. Den Internationale Valutafond har anslået det årlige tab som følge af cyberangreb til 9 % af bankernes nettoindtægter globalt set eller ca. 100 mia. USD[40]. Overgangen til internettilkoblet udstyr vil medføre store fordele for brugerne: når en lavere andel af dataene lagres og behandles i datacentre, og en større andel af databehandlingen foregår i nærheden af brugeren via "edge computing"[41], vil cybersikkerhed imidlertid ikke længere kunne fokusere på at beskytte centrale punkter[42].

I 2017 forelagde EU en tilgang til cybersikkerhed med opbygning af modstandsdygtighed, hurtig reaktion og effektiv afskrækkende virkning i centrum[43]. EU må nu sikre, at dets cybersikkerhedskompetencer holder trit med virkeligheden, for at levere både

---

[36] Et domænenavnesystem (DNS) er et hierarkisk opbygget og decentraliseret navnesystem for computere, tjenester eller enhver anden ressource, der er forbundet med internettet eller et privat net. Det omsætter domænenavne til de IP-adresser, der er nødvendige for at lokalisere og identificere computertjenester og -udstyr.

[37] Forslag til forordning om oprettelse af Unionens rumprogram og Den Europæiske Unions Agentur for Rumprogrammet COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] DDoS-angreb udgør fortsat en permanent trussel: Store udbydere måtte i februar 2020 afbøde massive DDoS-angreb, bl.a. et angreb på Amazons webtjenester.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] Edge computing er en distribueret, åben IT-arkitektur med decentral databehandling, og derved skabes det teknologiske grundlag for mobildatabehandling og tingenes internet (IoT). Ved edge computing behandles dataene i selve udstyret eller i en lokal computer eller på en lokal server, i stedet for at de overføres til et datacenter.

[42] Meddelelse om en europæisk strategi for data (COM(2020) 66 final).

[43] Jf. fælles meddelelse om modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU (JOIN(2017) 450 final).

modstandsdygtighed og reaktion. Dette forudsætter en tilgang, som reelt inddrager hele samfundet, hvor EU's institutioner, agenturer og organer, medlemsstaterne, erhvervslivet, den akademiske verden og enkeltpersoner giver cybersikkerhed den fornødne forrang.[44]. Denne horisontale tilgang må suppleres med sektorspecifikke tilgange til cybersikkerhed på områder såsom energi, finansielle tjenesteydelser, transport og sundhed. I den næste fase bør trådene i EU's arbejde samles i en revideret europæisk strategi for cybersikkerhed.

Bestræbelserne på at forbedre cybersikkerheden bør omfatte en undersøgelse af nye og forbedrede former for samarbejde mellem efterretningstjenester, EU INTCEN og andre sikkerhedsorganisationer, samt bekæmpelse af terrorisme, ekstremisme, radikalisme og hybride trusler.

Med baggrund i den igangværende udbredelse af **5G infrastrukturen** i hele EU og mange kritiske tjenesters potentielle afhængighed af 5G-net bliver konsekvenserne af systemiske og udbredte forstyrrelser særligt alvorlige. Den procedure, der er iværksat med Kommissionens henstilling af 2019 om cybersikkerheden i forbindelse med 5G-net[45], har nu udmøntet sig i konkrete tiltag fra medlemsstaternes side angående de centrale foranstaltninger, der blev fastlagt i en 5G-værktøjskasse[46].

Et af de vigtigste behov på lang sigt er at udvikle en kultur, hvor **cybersikkerhed indlejres i designet**, idet sikkerhed indbygges i produkter og tjenester fra første færd. Den nye ramme for cybersikkerhedscertificering, der er fastsat i forordningen om cybersikkerhed udgør et vigtigt bidrag til dette[47]. Rammen er allerede iværksat med to certificeringsordninger, som allerede forberedes, og prioriteter for yderligere ordninger vil blive fastlagt senere i år. Samarbejdet mellem EU's Agentur for Cybersikkerhed (ENISA), databeskyttelsesmyndighederne og Det Europæiske Databeskyttelsesråd[48] har afgørende betydning for dette område.

Kommissionen har allerede konstateret, at der er behov for en **fælles cyberenhed** for at tilvejebringe et struktureret og koordineret operationelt samarbejde. Dette kunne omfatte en mekanisme for gensidig bistand i krisesituationer på EU-plan. Med udgangspunkt i gennemførelsen af henstillingen[49] kan den fælles cyberenhed opbygge tillid mellem det europæiske cybersikkerhedsøkosystems forskellige aktører og tilbyde medlemsstaterne en central tjeneste. Kommissionen vil indlede drøftelser med relevante interessenter (i første omgang medlemsstaterne) og inden udgangen af 2020 fastlægge en klar proces med delmål og en tidsplan.

Fælles regler om informationssikkerhed og cybersikkerhed er også vigtige for alle EU's institutioner, organer og agenturer. Målet bør være at skabe obligatoriske, høje, fælles standarder for sikker informationsudveksling og sikkerhed i digitale infrastrukturer og systemer i alle EU's institutioner, organer og agenturer. Denne nye ramme bør lægge

[44] Det Fælles Forskningscenters rapport "Cybersecurity – our digital Anchor" giver et indblik i forskellige aspekter af udviklingen inden for cybersikkerhed i de sidste 40 år.

[45] Kommissionens henstilling om cybersikkerheden i forbindelse med 5G-net, COM(2019) 2335 final. Ifølge henstillingen skal virkningerne heraf vurderes i sidste kvartal af 2020.

[46] Der henvises til NIS-samarbejdsgruppens rapport af 24. juli 2020 om gennemførelsen af værktøjskassen.

[47] Forordning 2019/881 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi (forordningen om cybersikkerhed).

[48] Meddelelse om databeskyttelse som en hjørnesten i borgernes indflydelse og EU's tilgang til den digitale omstilling — to års anvendelse af den generelle forordning om databeskyttelse (COM(2020) 264).

[49] Kommissionens henstilling (EU) 2017/1584 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser.

grunden til et stærkt og effektivt operationelt samarbejde om cybersikkerhed i alle EU's institutioner, organer og agenturer med fokus på den rolle, som IT-Beredskabsenheden (CERT-EU) spiller for EU's institutioner, organer og agenturer.

I betragtning af problemets globale karakter har opbygningen og opretholdelsen af solide **internationale partnerskaber** afgørende betydning for at forebygge, afværge og reagere på cyberangreb. Rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter ("cyberdiplomatisk værktøjskasse")[50] rummer foranstaltninger inden for rammerne af den fælles udenrigs- og sikkerhedspolitik, herunder restriktive foranstaltninger (sanktioner), som kan tages i anvendelse over for aktiviteter, der skader EU's politiske, sikkerhedsmæssige og økonomiske interesser. Gennem udviklings- og samarbejdsmidler bør EU også udbygge sit arbejde for at bistå partnerlandene med kapacitetsopbygning for at styrke deres digitale økosystemer, vedtage nationale lovgivningsreformer og overholde internationale standarder. Derved øges hele samfundets modstandsdygtighed og dets evne til at imødegå og reagere effektivt på cybertrusler. Dette omfatter specifikt arbejde med henblik på at fremme EU's standarder og relevant lovgivning med henblik på at øge cybersikkerheden hos partnerlandene i naboskabsområdet[51].

Beskyttelse af det offentlige rum

De seneste terrorangreb har været koncentreret om **det offentlige rum**, herunder religiøse samlingssteder og transportknudepunkter, idet disses åbenhed og tilgængelighed udnyttes. Den tiltagende terrorisme, der er udløst af politisk eller ideologisk motiveret ekstremisme, har gjort denne trussel endnu mere akut. Dette stiller krav om såvel en mere omfattende fysisk beskyttelse af sådanne steder som passende detekteringssystemer, uden at det går ud over borgernes friheder[52]. Kommissionen vil forbedre samarbejdet mellem den offentlige og den private sektor om at beskytte det offentlige rum med finansiering, udveksling af erfaringer og god praksis, specifik vejledning[53] og anbefalinger[54]. En del af strategien vil omfatte bevidstgørelse, krav til ydeevne, test af detekteringsudstyr og forbedring af baggrundstjek for at imødegå insidertrusler. Det er vigtigt at bemærke, at mindretal og sårbare personer kan blive uforholdsmæssigt hårdt ramt — dette gælder personer, der udvælges som mål på grund af deres religion eller køn, og dette aspekt kræver særlig opmærksomhed. Regionale og lokale offentlige myndigheder spiller en vigtig rolle i at forbedre sikkerheden i det offentlige rum. Kommissionen bistår også byerne med at fremme innovation inden for sikkerhed i det offentlige rum[55]. Lanceringen af en ny partnerskabsdagsorden for byerne[56] om "sikkerhed i det offentlige rum" i november 2018

---

50 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/da/pdf

51 Jf. retningslinjerne for EU's eksterne cyberkapacitetsopbygning, der blev vedtaget i Rådets konklusioner af 26. juni 2018.

52 Fjernstyrede biometriske identifikationssystemer bør underkastes en særlig kontrol. Der er redegjort for Kommissionens indledende synspunkter i Kommissionens hvidbog af 19. februar 2020 om kunstig intelligens (COM(2020) 65).

53 F.eks. vejledningen om valg af passende sikkerhedsbarriereløsninger til beskyttelse af det offentlige rum (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

54 Retningslinjer for god praksis findes i SWD(2019) 140, herunder et afsnit om offentlig-privat samarbejde. Finansiering inden for rammerne af Fonden for Intern Sikkerhed – Politi har særligt fokus på at styrke offentlig-privat samarbejde.

55 Tre byer (Piræus i Grækenland, Tammerfors i Finland og Torino i Italien) vil som led i de nyskabende foranstaltninger i byerne afprøve nye løsninger, der samfinansieres af Den Europæiske Fond for Regionaludvikling (EFRU).

56 EU's dagsorden for byerne udgør en ny arbejdsmetode, hvor samarbejdet på flere niveauer fremmes mellem medlemsstaterne, byerne, Europa-Kommissionen og andre interessenter med henblik på at stimulere

afspejler, at medlemsstaterne, Kommissionen og byerne er fast besluttet på at tage bedre hånd om trusler mod sikkerheden i byområder.

Markedet for **droner** er fortsat i vækst med mange værdifulde og legitime anvendelser. De har imidlertid også potentiale til at blive misbrugt af kriminelle og terrorister, og det offentlige rum er særligt udsat. Målene kan omfatte enkeltpersoner, personforsamlinger, kritisk infrastruktur, retshåndhævende myndigheder, grænser eller det offentlige rum. Viden om, hvordan droner bruges i konflikter, kan finde vej tilbage til Europa enten direkte (via tilbagevendende udenlandske terrorkrigere) eller online. De regler, Den Europæiske Unions Luftfartssikkerhedsagentur allerede har opstillet, er et vigtigt første skridt på området, bl.a. registrering af droneoperatører og obligatorisk fjernidentifikation af droner. Da droner bliver stadig mere alment tilgængelige, økonomisk overkommelige og ydedygtige, er der behov for yderligere tiltag. Dette kan omfatte informationsdeling, vejledning og god praksis til brug for alle, herunder retshåndhævelse og flere test af dronemodforholdsregler[57]. Desuden bør beskyttelsen af privatlivets fred og databeskyttelse i forbindelse med anvendelse af droner i det offentlige rum analyseres og behandles yderligere.

De vigtigste tiltag
• Lovgivning om beskyttelse og modstandsdygtighed i relation til kritisk infrastruktur • Revision af NIS-direktivet • Et initiativ med henblik på at styrke finanssektorens operationelle modstandsdygtighed • Beskyttelse og cybersikkerhed i relation til kritisk energiinfrastruktur og netregler om cybersikkerhed for grænseoverskridende elektricitetsstrømme • En EU-strategi for cybersikkerhed • De næste skridt hen imod oprettelsen af en fælles cyberenhed • Fælles regler om informationssikkerhed og cybersikkerhed for EU's institutioner, organer og agenturer • Intensiveret samarbejde om beskyttelse af det offentlige rum, herunder religiøse samlingssteder • Udveksling af bedste praksis for at imødegå af misbrug af droner

2. Håndtering af foranderlige trusler

Cyberkriminalitet

Teknologi åbner nye muligheder for samfundet. Den tilvejebringer også nye værktøjer til de retslige og retshåndhævende myndigheder. Men samtidig åbner den døre for kriminelle. Malware, tyveri af personoplysninger eller forretningsoplysninger ved hjælp af hacking og blokering for digital aktivitet, der skader finansielt eller på omdømmet, udgør et voksende problem. Et modstandsdygtigt miljø med rod i en solid cybersikkerhed er det første forsvar. De retshåndhævende myndigheder skal kunne arbejde med digital efterforskning på grundlag af klare regler for efterforskning og retsforfølgning af forbrydelser og yde ofrene den nødvendige beskyttelse. Dette arbejde bør bygge på Europols fælles taskforce vedrørende cyberkriminalitet og beredskabsprotokollen om retshåndhævelsesindsatsen, der er oprettet med henblik på at koordinere reaktionen på storstilede cyberangreb. Effektive

---

væksten, leveforholdene og innovationen i Europas byer samt indkredse og tage hånd om sociale udfordringer.

[57] Der blev for nylig oprettet et flerårigt testprogram, der skal bistå medlemsstaterne med at opstille en fælles metode og en testplatform på området.

mekanismer, der baner vejen for offentlig-private partnerskaber og samarbejde, er også af central betydning.

Sideløbende hermed bør bekæmpelsen af cyberkriminalitet gøres til en strategisk kommunikationsprioritet i hele EU for at advare europæerne om risiciene og oplyse om de forebyggende foranstaltninger, de kan træffe. Dette bør være et led i en proaktiv tilgang. Et afgørende skridt vil også bestå i en fuld gennemførelse af den nuværende retlige ramme[58]: Kommissionen vil være rede til at tage traktatbrudsprocedurer i anvendelse, hvis det er relevant, og holde øje med denne ramme for at sikre, at den fortsat er velegnet til formålet. Sammen med Europol og EU's Agentur for Cybersikkerhed ENISA vil Kommissionen også undersøge gennemførligheden af et hurtigt EU-varslingssystem for cyberkriminalitet, der kan sikre strømmen af oplysninger og en hurtig modreaktion, hvis der sker en voldsom stigning i cyberkriminaliteten.

Cyberkriminalitet udgør en global udfordring, og der er derfor behov for et effektivt internationalt samarbejde. EU støtter Europarådets Budapestkonvention om IT-kriminalitet, som er en effektiv og veletableret ramme, der giver alle lande mulighed for at afdække, hvilke systemer og kommunikationskanaler de vil skulle indføre for at kunne samarbejde effektivt indbyrdes.

Næsten halvdelen af EU-borgerne er bekymrede over datamisbrug[59] og **identitetstyveri**[60]. Den svigagtige udnyttelse af en persons identitet for økonomisk vindings skyld er ét aspekt, men den kan også få en betydelig personlig og psykologisk virkning, hvis identitetstyven laver ulovlige opslag, som vil kunne findes online i årevis. Kommissionen vil granske mulige praktiske foranstaltninger, hvormed ofre kan beskyttes mod alle former for identitetstyveri under hensyntagen til det kommende initiativ om en europæisk digital identitet[61].

For at håndtere cyberkriminalitet må blikket rettes fremad. I takt med at samfundet anvender ny teknologi til at styrke økonomien og samfundet, kan kriminelle også søge at udnytte disse værktøjer til skadelige formål. For eksempel kan kriminelle benytte kunstig intelligens til at afsløre og identificere passwords eller gøre det lettere at skabe malware og misbruge billeder og lyd, der efterfølgende kan benyttes til identitetstyveri eller -svig.

Moderne retshåndhævelse

De retshåndhævende myndigheder og retsvæsenets aktører må tilpasse sig ny teknologi. Den teknologiske udvikling og nye trusler indebærer, at de retshåndhævende myndigheder må have adgang til nye værktøjer, tilegne sig nye færdigheder og udvikle alternative efterforskningsteknikker. For at supplere de lovgivningsmæssige tiltag, der har til formål at forbedre adgangen til elektronisk bevismateriale på tværs af landegrænser med henblik på strafferetlig efterforskning, kan EU bistå de retshåndhævende myndigheder med at udvikle den nødvendige kapacitet til at finde frem til, sikre og læse de data, der er nødvendige for at efterforske forbrydelser, og anvende disse data som bevismateriale i retten. Kommissionen vil undersøge foranstaltninger, som **styrker retshåndhævelseskapaciteten i forbindelse**

[58] Direktiv 2013/40/EU om angreb på informationssystemer.

[59] 46 % (Eurobarometerundersøgelse om europæernes holdninger til cybersikkerhed, januar 2020).

[60] Langt størstedelen af respondenterne i eurobarometerundersøgelsen fra 2018 om "europæernes holdning til internetsikkerhed" (95 %) anser identitetstyveri for en alvorlig forbrydelse, og syv ud af ti giver udtryk for, at det er en meget alvorlig forbrydelse. Eurobarometerundersøgelsen, der blev offentliggjort i januar 2020, bekræftede, at cyberkriminalitet, onlinebedrageri og identitetstyveri er en kilde til bekymring: to tredjedele af de adspurgte gav udtryk for, at de er bekymrede over banksvindel (67 %) eller identitetstyveri (66 %).

[61] Meddelelse af 19. februar 2020 om "Europas digitale fremtid i støbeskeen" (COM(2020) 67).

med digital efterforskning, og fastlægge, hvordan forskning og udvikling bedst kan udnyttes til at skabe nye værktøjer til retshåndhævelse, og hvordan uddannelse kan tilvejebringe de rette færdigheder til de retshåndhævende og retslige myndigheder. Dette vil også omfatte strengt videnskabelige evalueringer og testmetoder foretaget via Kommissionens Fælles Forskningscenter.

Fælles tilgange kan også sikre, at **kunstig intelligens, rumkapacitet, big data** og **højtydende databehandling integreres** i sikkerhedspolitikken på en sådan måde, at effektiviteten sikres både med hensyn til bekæmpelsen af kriminalitet og sikringen af de grundlæggende rettigheder. Kunstig intelligens kan udgøre et effektivt værktøj til at bekæmpe kriminalitet, idet der skabes en enorm efterforskningskapacitet ved at analysere store informationsmængder og udpege mønstre og uregelmæssigheder[62]. Den kan også tilvejebringe konkrete værktøjer, der kan bidrage til at udpege terrorrelateret indhold på internettet, opdage mistænkelige transaktioner i forbindelse med salg af farlige produkter eller tilbyde bistand til borgere i nødsituationer. For at virkeliggøre dette potentiale må man sammenføre forskning og innovation samt brugere af kunstig intelligens med den rette forvaltning og tekniske infrastruktur, samtidig med, at den private sektor og den akademiske verden inddrages aktivt. Det indebærer også, at der skal sikres de højeste standarder for overholdelse af grundlæggende rettigheder, samtidig med at en effektiv beskyttelse af borgerne sikres. Navnlig skal afgørelser, der berører enkeltpersoner, gennemgås af et menneske og være i overensstemmelse med den relevante gældende EU-ret[63].

Der er brug for elektronisk information og bevismateriale i ca. 85 % af de sager, hvor alvorlige forbrydelser efterforskes, og 65 % af det samlede antal anmodninger er rettet til udbydere, som er etableret i en anden jurisdiktion[64]. Den kendsgerning, at traditionelle fysiske spor nu findes online, udvider kløften mellem retshåndhævelseskapaciteten og de kriminelles kapacitet. Det er afgørende, at der indføres klare regler for grænseoverskridende adgang til elektronisk bevismateriale med henblik på strafferetlig efterforskning. Derfor har Europa-Parlamentets og Rådets hurtige vedtagelse af forslagene af forslagene om elektronisk bevismateriale afgørende betydning for at give fagfolk et effektivt værktøj. Grænseoverskridende adgang til elektronisk bevismateriale gennem multilaterale og bilaterale internationale forhandlinger er også af afgørende betydning for at fastlægge indbyrdes forenelige regler på internationalt plan[65].

Adgang til digitalt bevismateriale afhænger også af, at oplysningerne er tilgængelige. Slettes oplysningerne for hurtigt, kan vigtigt bevismateriale gå tabt, således at der ikke længere er mulighed for at identificere og lokalisere mistænkte og kriminelle netværk (samt ofre). På den anden side afføder datalagringsordninger spørgsmål om beskyttelse af privatlivets fred. Afhængigt af udfaldet af de sager, der verserer for EU-Domstolen, vil Kommissionen vurdere vejen frem med hensyn til lagring af data.

---

62 F.eks. i forbindelse med økonomisk kriminalitet.

63 Dette indebærer overholdelse af den eksisterende lovgivning, herunder den generelle forordning (EU) 2016/679 om databeskyttelse og direktiv (EU) 2016/680 om databeskyttelse på retshåndhævelsesområdet, der regulerer myndigheders behandling af personoplysninger med henblik på at afsløre, forebygge, efterforske og retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner.

64 Kommissionens arbejdsdokument SWD(2018) 118 final.

65 Især anden tillægsprotokol til Europarådets Budapestkonvention om IT-kriminalitet og en aftale mellem EU og USA om grænseoverskridende adgang til elektronisk bevismateriale.

Adgang til oplysninger om registrering af internetdomænenavne ("WHOIS-data")[66] er vigtig for strafferetlig efterforskning, cybersikkerhed og forbrugerbeskyttelse. Det bliver imidlertid vanskeligere at få adgang til disse oplysninger i afventning af, at ICANN (Internet Corporation for Assigned Names and Numbers) vedtager en ny WHOIS-politik. Kommissionen vil fortsat samarbejde med ICANN og multiinteressentfællesskabet for at sikre, at enheder, der legitimt anmoder om adgang, herunder retshåndhævende myndigheder, kan få effektiv adgang til WHOIS-data i overensstemmelse med EU's og internationale bestemmelser om databeskyttelse. Dette vil omfatte en vurdering af mulige løsninger, herunder spørgsmålet om, hvorvidt der er behov for at lovgive for at præcisere reglerne for adgang til sådanne oplysninger.

De retshåndhævende og retslige myndigheder har også behov for det rette udstyr til at hente de(t) fornødne data og bevismateriale, når **5G-arkitekturen for mobil telekommunikation** er fuldt indført i EU, på en sådan måde, at kommunikationshemmeligheden respekteres. Kommissionen vil støtte en udvidet og koordineret tilgang ved udarbejdelsen af internationale standarder med en fastlæggelse af bedste praksis, procedurer og teknisk interoperabilitet på centrale teknologiske områder såsom kunstig intelligens, tingenes internet eller blockchainteknologier.

For indeværende udgør **krypterede oplysninger** en væsentlig del af efterforskningen af alle former for kriminalitet og terrorisme. Kryptering har afgørende betydning for den digitale verden ved at sikre digitale systemer og transaktioner og beskytte en række grundlæggende rettigheder, herunder ytringsfrihed, privatlivets fred og databeskyttelse. Anvendes kryptering imidlertid til kriminelle formål, kan det også skjule kriminelles identitet og indholdet af deres kommunikation. Kommissionen vil undersøge og støtte afbalancerede tekniske, operationelle og retlige løsninger på problemerne og fremme en tilgang, som både opretholder krypteringens effektivitet med hensyn til beskyttelsen af privatlivets fred og kommunikationssikkerheden, samtidig med at det gøres muligt på effektiv vis at gribe ind over for kriminalitet og terrorisme.

Bekæmpelse af terrorrelateret indhold på nettet

Hvis onlinemiljøet skal gøres lige så sikkert som fysiske miljøer, vil der skulle tages yderligere skridt til at **bekæmpe ulovligt indhold på nettet**. Væsentlige trusler mod borgerne, f.eks. terrorisme, ekstremisme og seksuelt misbrug af børn, hidrører stadig oftere fra det digitale miljø: disse må afværges med konkrete tiltag og en ramme til sikring af, at de grundlæggende rettigheder respekteres. Et afgørende første skridt er hurtigt at afslutte forhandlingerne om den foreslåede lovgivning om terrorrelateret onlineindhold[67] og sikre dens gennemførelse. En styrkelse af det frivillige samarbejde mellem de retshåndhævende myndigheder og den private sektor i **EU's internetforum** har også central betydning for at bekæmpe terroristers, voldelige ekstremisters og kriminelles misbrug af internettet. EU's internetindberetningsenhed i Europol vil fortsat spille en afgørende rolle i overvågningen af terrorgruppernes aktiviteter på internettet og de foranstaltninger, der træffes af platforme[68], samt i forbindelse med videreudviklingen af **EU's kriseprotokol**[69]. Desuden vil Kommissionen fortsat samarbejde med internationale partnere, herunder ved at deltage i **GIFCT (Global Internet Forum to Counter Terrorism)** for at bekæmpe disse

[66] Lagret i databaser, der administreres af 2 500 register- eller registratoroperatører, der er etableret i hele verden.

[67] Forslag om forebyggelse af udbredelsen af terrorrelateret onlineindhold (COM(2018) 640 af 12. september 2018).

[68] Europol, november 2019.

[69] A Europe that protects - EU Crisis Protocol: responding to terrorist content online. (Oktober 2019).

udfordringer på globalt plan. Arbejdet vil fortsat støtte udviklingen af alternative fortællinger og tage til genmæle via programmet om styrkelse af civilsamfundet[70].

For at forebygge og bekæmpe udbredelsen af ulovlig hadefuld tale på internettet iværksatte Kommissionen i 2016 en adfærdskodeks for bekæmpelse af ulovlig hadefuld tale på internettet med et frivilligt tilsagn fra onlineplatforme om fjernelse af hadefuld tale. Den seneste evaluering viser, at virksomhederne vurderer 90 % af det anmeldte indhold inden for 24 timer og fjerner 71 % af det indhold, der betragtes som ulovlig hadefuld tale. Platformene må dog forbedre gennemskueligheden og tilbagemeldingerne til brugerne yderligere og sikre en konsekvent evaluering af det påklagede indhold[71].

EU's internetforum vil også lette informationsudvekslingen om eksisterende og ny teknologi med henblik på at imødegå de udfordringer, der er forbundet med seksuelt misbrug af børn online. Bekæmpelse af seksuelt misbrug af børn online står i centrum af en ny strategi for at optrappe **bekæmpelsen af seksuelt misbrug af børn**[72], hvormed der gøres optimal brug af de værktøjer, der er til rådighed på EU-plan til at bekæmpe disse forbrydelser. Virksomhederne skal gives mulighed for fortsat at afsløre og fjerne materiale, der viser seksuelt misbrug af børn online, og de skadevirkninger, som dette materiale påfører ofrene, gør det påkrævet med en ramme, hvorved der pålægges klare og permanente forpligtelser til at imødegå problemet. Som led i strategien vil det også blive bebudet, at Kommissionen vil begynde at udarbejde sektorspecifik lovgivning for at effektivisere imødegåelsen af seksuelt misbrug af børn under fuld overholdelse af de grundlæggende rettigheder.

Mere generelt vil den kommende lov om digitale tjenester også præcisere og opgradere ansvarsområder og sikkerhedsregler gældende for digitale tjenester og fjerne de negative incitamenter, som bremser indsatsen for at imødegå ulovligt indhold og ulovlige varer eller tjenester.

Desuden vil Kommissionen fortsat samarbejde med internationale partnere og med **GIFTC (Global Internet Forum to Counter Terrorism)**, bl.a. via det uafhængige rådgivende udvalg, for at drøfte, hvordan disse udfordringer kan imødegås på globalt plan, samtidig med at EU's værdier og grundlæggende rettigheder bevares. Der bør også tages højde for nye emner såsom algoritmer eller onlinespil[73].

Hybride trusler

Omfanget og mangfoldigheden af de aktuelle hybride trusler er uden fortilfælde. Dette kom tydeligt til udtryk under covid-19-krisen, hvor flere statslige og ikkestatslige aktører søgte at udnytte pandemien til at fremme deres dagsorden, navnlig ved at manipulere informationsmiljøet og udfordre centrale infrastrukturer. Dette risikerer at svække den sociale samhørighed og undergrave tilliden til EU-institutionerne og medlemsstaternes regeringer.

EU's tilgang til hybride trusler er fastlagt i den fælles ramme af 2016[74] og den fælles meddelelse af 2018 vedrørende øget modstandsdygtighed over for hybride trusler[75]. Indsatsen på EU-plan understøttes af en anselig værktøjskasse, der dækker sammenhængen

[70] Dette hænger sammen med arbejdet i programmet til bevidstgørelse omkring radikalisering, se også afsnit IV.3 nedenfor.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] EU-strategi for en mere effektiv bekæmpelse af seksuelt misbrug af børn (COM(2020) 607).

[73] Terrorister bruger stadig oftere spilleplatforme til at udveksle beskeder, og unge terrorister gennemspiller voldelige angreb i videospil.

[74] Fælles ramme for imødegåelse af hybride trusler — Den Europæiske Unions indsats (JOIN(2016) 18).

[75] Øget modstandsdygtighed og bedre kapacitet til at imødegå hybride trusler (JOIN(2018) 16).

mellem den indre og ydre sikkerhed baseret på en strategi, som inddrager hele samfundet, og et tæt samarbejde med strategiske partnere, navnlig NATO og G7. Sammen med denne strategi offentliggøres en rapport om gennemførelsen af EU's tilgang til hybride trusler[76]. På grundlag af den kortlægning[77], der foretages sideløbende med denne strategi, vil Kommissionen og EU-Udenrigstjenesten oprette en **onlineplatform med adgangsbegrænsning** som referencegrundlag for medlemsstaternes værktøjer til at imødegå hybride trusler og foranstaltninger på EU-plan.

Ansvaret for at imødegå hybride trusler ligger primært hos medlemsstaterne på grund af den naturlige sammenhæng med den nationale sikkerheds- og forsvarspolitik, men nogle sårbarheder er fælles for alle medlemsstater, og nogle trusler rækker over landegrænserne, f.eks. angreb mod net eller infrastruktur, der krydser landegrænser. Kommissionen og den højtstående repræsentant vil fastlægge en EU-tilgang til hybride trusler, hvormed den eksterne og interne dimension integreres i en uhindret informationsstrøm, og de nationale og EU-dækkende overvejelser føres sammen. Dette skal omfatte hele spektret af tiltag — fra hurtig afsløring, analyse, bevågenhed, opbygning af modstandsdygtighed og forebyggelse til krisestyring og konsekvenshåndtering.

Da de hybride trusler er i konstant forandring, vil der foruden en styrket gennemførelse blive lagt særlig vægt på at **integrere overvejelser angående hybride trusler i politikudformningen**, holde trit med den dynamiske udvikling og sørge for, at intet potentielt relevant initiativ lades ude af betragtning. De nye initiativers virkninger vil også blive vurderet ud fra hybridperspektivet; dette gælder bl.a. initiativer på områder, der ikke hidtil har været genstand for forholdsregler mod hybride trusler, f.eks. uddannelse, teknologi og forskning. Denne tilgang vil drage fordel af arbejdet med at udvikle koncepter for hybride trusler, hvorved der dannes et samlet overblik over de forskellige værktøjer, som modstanderne kan benytte sig af[78]. Sigtet bør være at sørge for, at beslutningsprocessen underbygges af regelmæssige, fyldestgørende, efterretningsbaserede rapporter om udviklingen på området hybride trusler. Dette hviler i høj grad på medlemsstaternes efterretninger og en yderligere styrkelse af efterretningssamarbejdet med medlemsstaternes kompetente tjenester gennem EU INTCEN.

For at udvikle et **situationskendskab** vil Kommissionen og EU-Udenrigstjenesten undersøge mulighederne for at strømline informationsstrømme fra forskellige kilder, herunder medlemsstaterne, samt EU-agenturer som ENISA, Europol og Frontex. EU-enheden for analyse og udveksling af oplysninger om hybride trusler vil fortsat være EU's kontaktpunkt for hybride trusselsvurderinger. **Opbygning af modstandsdygtighed** har central betydning for at forebygge og yde beskyttelse mod hybride trusler. Det er derfor afgørende systematisk at spore og objektivt at måle fremskridt på området. Et første skridt består i at udpege sektorspecifikke referencekrav til medlemsstaternes såvel som EU-institutioners og -organers modstandsdygtighed over for hybride trusler. For at optrappe **kriseberedskabet over for og bekæmpelsen af hybride trusler** bør der endvidere foretages en revision af den eksisterende protokol, jf. EU-drejebogen af 2016[79], så den

[76] SWD(2020) 153. Rapport om gennemførelsen af den fælles meddelelse af 2016 om imødegåelse af hybride trusler og den fælles meddelelse af 2018 om øget modstandsdygtighed og bedre kapacitet til at imødegå hybride trusler.

[77] SWD(2020) 152. Kortlægning af foranstaltninger vedrørende styrkelse af modstandsdygtighed og imødegåelse af hybride trusler.

[78] The Landscape of Hybrid Threats: A conceptual Model, JRC117280, som er udarbejdet i fællesskab af Det Fælles Forskningscenter og Det Europæiske Center for Imødegåelse af Hybride Trusler.

[79] EU's operationelle protokol for imødegåelse af hybride trusler (EU- drejebogen) (SWD(2016) 227).

afspejler den bredt anlagte gennemgang og styrkelse af EU's kriseresponssystem, der overvejes pt.[80]. Formålet er at optimere virkningen af EU's indsats ved hurtigt at sammenføre sektorspecifikke reaktioner og sikre et helstøbt samarbejde med vores partnere, dvs. NATO i første omgang.

De vigtigste tiltag
• Sikring af, at lovgivningen om cyberkriminalitet gennemføres og er velegnet til formålet • En strategi for en mere effektiv bekæmpelse af seksuelt misbrug af børn • Forslag om afsløring og fjernelse af materiale, der viser seksuelt misbrug af børn • En EU-tilgang til at imødegå hybride trusler • Revision af EU's operationelle protokol for imødegåelse af hybride trusler (EU-drejebogen) • Vurdering af, hvordan retshåndhævelseskapaciteten styrkes i forbindelse med digital efterforskning

3. Beskyttelse af europæerne mod terrorisme og organiseret kriminalitet

Terrorisme og radikalisering

Terrortruslen mod EU er fortsat høj. Trods faldet i antallet af angreb generelt kan disse stadig have en ødelæggende virkning. Radikalisering kan også i højere grad polarisere og destabilisere den sociale samhørighed. Medlemsstaterne har det primære ansvar for at bekæmpe terrorisme og radikalisering. Truslens stadigt voksende tværnationale og tværsektorielle dimension taler dog for, at der inden for rammerne af EU-samarbejdet og -koordineringen må træffes yderligere forholdsregler. En effektiv gennemførelse af EU-lovgivningen om bekæmpelse af terrorisme, herunder restriktive foranstaltninger[81], prioriteres højt. Det er stadig målet at udvide Den Europæiske Anklagemyndigheds beføjelser til at omfatte bekæmpelse af grænseoverskridende terrorhandlinger

Bekæmpelse af terrorisme må i første omgang tage fat på de grundlæggende årsager. Polariseringen af samfundet, den reelle eller oplevede forskelsbehandling og andre psykologiske og sociologiske faktorer kan styrke borgernes modtagelighed over for radikale synspunkter. I den forbindelse går bekæmpelsen af **radikalisering** hånd i hånd med fremme af social samhørighed på lokalt, nationalt og europæisk plan. Flere virkningsfulde initiativer og politikker er udviklet i det seneste årti, navnlig gennem netværket til bevidstgørelse omkring radikalisering og EU's byer mod radikalisering[82]. Tiden er nu inde til at overveje tiltag med henblik på at strømline EU's politikker, initiativer og midler til bekæmpelse af radikalisering. Sådanne foranstaltninger kan støtte udviklingen af kompetencer og færdigheder, forbedre samarbejdet, styrke videngrundlaget og bidrage til at evaluere fremskridt, der inddrager alle relevante interessenter, herunder aktører der arbejder med

[80] Efter en videokonference den 26. marts 2020 vedtog medlemmerne af Det Europæiske Råd en erklæring om EU-tiltag som reaktion på covid-19-udbruddet, hvori det opfordrede Kommissionen til at forelægge forslag om et mere ambitiøst og vidtrækkende krisestyringssystem i EU.

[81] Rådet har vedtaget restriktive foranstaltninger mod ISIL (Da'esh) og al-Qaeda samt specifikke restriktive foranstaltninger mod visse personer og enheder med henblik på at bekæmpe terrorisme. EU's sanktionskort (https://www.sanctionsmap.eu/#/main) indeholder en oversigt over alle restriktive foranstaltninger.

[82] Pilotprojektet "EU's byer mod radikalisering" har det dobbelte formål at fremme udvekslingen af ekspertise mellem EU's byer og indsamle feedback om, hvordan lokalsamfundene bedst kan støttes på EU-plan.

området, politiske beslutningstagere og den akademiske verden[83]. Bløde politikker såsom uddannelse, kultur, ungdom og sport kan bidrage til at forebygge radikalisering og skabe muligheder for udsatte unge og samhørighed i EU[84]. De prioriterede områder omfatter arbejde med tidlig afsløring og risikostyring, opbygning af modstandsdygtighed og afradikalisering samt rehabilitering og reintegration i samfundet.

Terroristerne har forsøgt at anskaffe og omdanne **kemiske, biologiske, radiologiske og nukleare** (CBRN)[85] materialer til våben og udvikle deres viden og kapacitet til at bruge dem.[86]. Potentialet ved CBRN-angreb har en fremtrædende plads i terrorpropagandaen. Skadesomfanget er potentielt så betydeligt, at der er behov for at udvise særlig opmærksomhed på området. Med udgangspunkt i den tilgang, der anvendes til at regulere adgangen til udgangsstoffer til eksplosivstoffer, vil Kommissionen se nærmere på muligheden for at begrænse adgangen til visse farlige kemikalier, der kan anvendes til at udføre angreb. Udviklingen af kapaciteten inden for rammerne af EU's civilbeskyttelsesindsats (rescEU) for at imødegå CBRN-angreb vil også få central betydning. Samarbejde med tredjelande er også vigtigt for at fremme en fælles CBRN-sikkerhedskultur med fuld udnyttelse af EU's globale CBRN-ekspertisecentre. Dette samarbejde vil omfatte nationale mangel- og risikovurderinger, bistand til nationale og regionale CBRN-handlingsplaner, udveksling af god praksis og CBRN-kapacitetsopbyggende aktiviteter.

EU har udarbejdet den mest avancerede lovgivning i verden for at begrænse adgangen til **udgangsstoffer til eksplosivstoffer**[87] og afsløre mistænkelige transaktioner, der har til formål at bygge improviserede eksplosive anordninger. Men truslen fra hjemmelavede sprængstoffer er fortsat høj, og de er blevet anvendt i forbindelse med flere angreb i hele EU[88]. I første omgang må reglerne gennemføres, og det må sikres, at onlinemiljøet ikke gør det muligt at omgå kontrolforanstaltningerne.

En effektiv retsforfølgning af gerningsmænd, der har begået terrorhandlinger, herunder **fremmedkrigere**, som pt. befinder sig i Syrien og Irak, er også et vigtigt element i terrorbekæmpelsespolitikken. Selv om disse anliggender primært håndteres af medlemsstaterne, kan EU's koordinering og bistand hjælpe medlemsstaterne med at imødegå fælles udfordringer. De igangværende tiltag med henblik på at gennemføre lovgivningen om sikkerhedsforanstaltninger ved grænserne fuldt ud[89] og gøre fuld brug af alle relevante EU-databaser til at udveksle oplysninger om kendte mistænkte vil være et vigtigt skridt. Foruden at identificere personer med høj risiko er der behov for en reintegrations- og revalideringspolitik. Tværfagligt samarbejde, herunder med fængselspersonale og kriminalforsorgen, vil styrke den retlige forståelse af radikaliseringsprocesser, der munder

[83] Eksempelvis finansiering inden for rammerne af den europæiske sikkerhedsfond og programmet for unionsborgerskab.

[84] EU-aktioner som f.eks. Erasmus+ Virtual Exchange og e-twinning.

[85] I de seneste to år har der eksempelvis været flere sager både i Europa (Frankrig, Tyskland og Italien) og i tredjelande (Tunesien og Indonesien) med biologiske agenser (sædvanligvis plantebaserede toksiner).

[86] Rådet vedtog restriktive foranstaltninger mod spredning og brug af kemiske våben.

[87] Kemikalier, der kan misbruges til at fremstille hjemmelavede eksplosivstoffer. Disse reguleres ved forordning (EU) 2019/1148 om markedsføring og anvendelse af udgangsstoffer til eksplosivstoffer.

[88] Som eksempel på sådanne ødelæggende angreb kan nævnes angrebene i Oslo (2011), Paris (2015), Bruxelles (2016) og Manchester (2017). Ved et angreb med et hjemmelavet sprængstof i Lyon (2019) kom 13 personer til skade.

[89] Herunder de nye beføjelser, der er tildelt Det Europæiske Agentur for Grænse- og Kystbevogtning (Frontex).

ud i voldelig ekstremisme, og de retslige myndigheders tilgang til domfældelse og alternativer til frihedsberøvelse.

Udfordringen ved fremmedkrigere er et symbol på forbindelsen mellem den indre og **ydre sikkerhed**. Samarbejde om terrorbekæmpelse samt forebyggelse og bekæmpelse af radikalisering og voldelig ekstremisme er af central betydning for sikkerheden i EU[90]. Der er behov for at videreudvikle terrorbekæmpelsespartnerskaber og samarbejde med nabolande og andre lande, idet der trækkes på ekspertisen fra EU's Netværk af terrorbekæmpelses- og sikkerhedseksperter. Den fælles handlingsplan om terrorbekæmpelse for Vestbalkan er en god reference for et sådant målrettet samarbejde. Der bør navnlig gøres en indsats for at støtte partnerlandenes kapacitet til at identificere og lokalisere fremmedkrigere. EU vil også fortsat fremme multilateralt samarbejde i samarbejde med de førende globale aktører på området, f.eks. FN, NATO, Europarådet, Interpol og OSCE. Det vil også samarbejde med Det Globale Forum for Terrorbekæmpelse og den globale koalition mod Da'esh samt relevante civilsamfundsaktører. Unionens udenrigspolitiske instrumenter, herunder udvikling og samarbejde, spiller også en vigtig rolle i samarbejdet med tredjelande om at forhindre terrorisme og pirateri. Internationalt samarbejde er også vigtigt for at afskære alle kilder til **finansiering af terrorisme**, f.eks. via Den Finansielle Aktionsgruppe.

Organiseret kriminalitet

Organiseret kriminalitet medfører enorme økonomiske og personlige omkostninger. Det økonomiske tab som følge af organiseret kriminalitet og korruption skønnes at udgøre mellem 218 og 282 mia. EUR om året[91]. Mere end 5 000 organiserede kriminelle grupper blev efterforsket i Europa i 2017 — en stigning på 50 % i forhold til 2013[92]. Organiseret kriminalitet opererer i stigende grad på tværs af landegrænser, herunder fra EU's umiddelbare nabolande, hvilket nødvendiggør et øget operationelt samarbejde og udveksling af oplysninger med partnere i nabolandene.

Nye udfordringer opstår, idet kriminaliteten går online: under covid-19-pandemien skete der en enorm stigning i onlinesvindel, der gik ud over sårbare grupper, og sundheds- og hygiejneartikler blev genstand for målrettet tyveri og indbrudstyveri[93]. EU er nødt til at intensivere sin indsats mod organiseret kriminalitet, også på internationalt plan, med flere værktøjer til at nedbryde den organiserede kriminalitets forretningsmodel. Bekæmpelse af organiseret kriminalitet forudsætter også et nært samarbejde med lokale og regionale myndigheder samt civilsamfundet, som er vigtige partnere inden for såvel kriminalitetsforebyggelse som med hensyn til at yde bistand og støtte til ofre, og behovet er særligt udtalt hos myndigheder i grænseregioner. Dette arbejde vil blive samlet i en **dagsorden for bekæmpelse af organiseret kriminalitet**.

Mere end en tredjedel af de aktive organiserede kriminelle grupper i EU er involveret i produktion af, handel med eller distribution af narkotika. Narkotikaafhængighed medførte, at over 8 000 personer døde som følge af overdosis i EU i 2019. Størstedelen af **narkohandelen** foregår på tværs af landegrænserne, og en stor del af fortjenesten infiltrerer

[90] I Rådets konklusioner af 16. juni 2020 understreges det, at det er nødvendigt at beskytte EU's borgere mod terrorisme og voldelig ekstremisme i alle afskygninger og uanset deres oprindelse og yderligere styrke EU's eksterne terrorbekæmpelsesengagement og -indsats på visse prioriterede geografiske og tematiske områder.

[91] Målt på bruttonationalproduktet (BNP) Europols rapport: "Does crime still pay?" – Criminal asset recovery in the EU, 2016.

[92] Europol, Serious and Organised Threat Assessments (SOCTA), 2013 og 2017.

[93] Europol, 2020.

den lovlige økonomi[94]. En ny EU-narkotikadagsorden[95] vil styrke EU's og medlemsstaternes indsats med hensyn til at begrænse narkotikaefterspørgslen og -udbuddet, fastlægge fælles tiltag til at løse fælles problemer og styrke dialogen og samarbejdet mellem EU og de eksterne partnere om narkotikaspørgsmål. Efter Det Europæiske Overvågningscenter for Narkotika og Narkotikamisbrugs evaluering vil Kommissionen vurdere, om dets mandat skal ajourføres, for at det kan imødegå de nye udfordringer.

Organiserede kriminelle grupper og terrorister er også centrale aktører i handelen med **ulovlige skydevåben**. Mellem 2009 og 2018 fandt 23 massenedskydninger sted i Europa, hvorved mere end 340 menneskeliv gik tabt[96]. Skydevåben føres ofte ind i EU via dets nærmeste nabolande[97]. Dette er tegn på, at koordineringen og samarbejdet må styrkes både inden for EU og med internationale partnere, navnlig Interpol, for at harmonisere indsamlingen af oplysninger og rapporteringen om beslaglæggelse af skydevåben. Det er også vigtigt at forbedre muligheden for at spore våben, også på internettet, og sikre, at oplysninger udveksles mellem våbenlicensudstedende myndigheder og de retshåndhævende myndigheder. Kommissionen forelægger en ny **EU-handlingsplan for bekæmpelse af ulovlig handel med skydevåben**[98] og vil også vurdere, om reglerne om udførselstilladelse og indførsels- og transitforanstaltninger for skydevåben stadig er velegnede til formålet[99].

Kriminelle organisationer behandler migranter og mennesker med behov for international beskyttelse som en handelsvare. 90 % af de irregulære migranter, der ankommer til EU, har benyttet sig af kriminelle netværk.[100] Smugling af migranter er også ofte forbundet med andre former for organiseret kriminalitet, navnlig menneskehandel[101]. Ud over de enorme menneskelige omkostninger ved menneskehandel anslår Europol, at det årlige overskud for alle former for udnyttelse af menneskehandel udgør 29,4 mia. EUR. Denne udnyttelse er en grænseoverskridende forbrydelse, som næres af en ulovlig efterspørgsel i og uden for EU, og som påvirker alle EU-medlemsstater. De ringe resultater med hensyn til at identificere, retsforfølge og dømme personer for disse forbrydelser gør en ny tilgang påkrævet. En ny **omfattende tilgang til menneskehandel** vil samle trådene i indsatsen. Desuden vil Kommissionen forelægge en **ny EU-handlingsplan for bekæmpelse af smugling af migranter** for 2021-2025. Begge indsatsområder vil fokusere på at bekæmpe kriminelle netværk, sætte skub i samarbejdet og støtte retshåndhævelsen.

Organiserede kriminelle grupper søger — i lighed med terrorister — også at udnytte muligheder på andre områder, navnlig områder, der skaber stor fortjeneste, og hvor opdagelsesrisikoen er lav, f.eks. **miljøkriminalitet**. Ulovlig jagt på og handel med vilde dyr, ulovlig minedrift, skovning og ulovlig bortskaffelse og overførsel af affald er blevet verdens fjerdestørste kriminelle virksomhed[102]. Kriminelle har ligeledes misbrugt emissionshandelssystemet, energicertifikatsystemer og midler afsat til

[94] EMCDDA and Europol, EU Drug Markets Report 2019. (November 2019).
[95] EU's narkotikadagsorden og -handlingsplan (2021-2025) (COM(2020) 606).
[96] Flemish Peace Institute, Armed to kill. (Oktober 2019).
[97] EU har finansieret kampen mod spredning af og handel med håndvåben og lette våben i regionen siden 2002. EU har bl.a. finansieret det Regionale Netværk af Våbeneksperter i Sydøsteuropa (SEEFEN). Siden 2019 har partnerne på Vestbalkan været fuldt involveret i skydevåbenprioriteten inden for rammerne af EMPACT (den europæiske tværfaglige platform mod kriminalitetstrusler).
[98] COM(2020) 608.
[99] Forordning (EU) nr. 258/2012 om gennemførelse af artikel 10 i De Forenede Nationers protokol om bekæmpelse af ulovlig fremstilling af og handel med skydevåben.
[100] Kilde: Europol.
[101] Europol, EMSC, 4th Annual Report.
[102] UNEP-INTERPOL Rapid Response Assessment: The Rise of Environmental Crime, juni 2016.

miljømodstandsdygtighed og bæredygtig udvikling. Ud over at fremme EU's, medlemsstaternes og det internationale samfunds tiltag med henblik på at optrappe indsatsen mod miljøkriminalitet[103] er Kommissionen i færd med at vurdere, om direktivet om miljøkriminalitet[104] fortsat er velegnet til formålet. **Ulovlig handel med kulturgoder** er også blevet en af de mest lukrative kriminelle aktiviteter, en kilde til finansiering af terrorister og organiseret kriminalitet, og udviklingstendensen er stigende. Mulighederne for at spore kulturgoder online og offline i det indre marked og samarbejdet med de tredjelande, hvor kulturgoder plyndres, bør søges forbedret, samtidig med at der ydes aktiv støtte til retshåndhævende myndigheder og akademiske samfund.

Økonomiske og finansielle forbrydelser er meget komplekse, men de berører millioner af borgere og tusindvis af virksomheder i EU hvert år. Bekæmpelse af svig har afgørende betydning og kræver handling på EU-plan. Europol bistår sammen med Eurojust og Den Europæiske Anklagemyndighed medlemsstaterne og EU med at beskytte de økonomiske og finansielle markeder og beskytte EU-skatteydernes penge. Den Europæiske Anklagemyndighed bliver fuldt operationel hen mod udgangen 2020 og vil efterforske og retsforfølge forbrydelser til skade for EU-budgettet, f.eks. svig, korruption og hvidvaskning af penge. Det vil også tage hånd om grænseoverskridende momssvig, som koster skatteyderne mindst 50 mia. EUR om året.

Kommissionen vil også støtte udviklingen af ekspertise og lovgivningsmæssige rammer for så vidt angår nye risici såsom kryptoaktiver og nye betalingssystemer. Kommissionen vil navnlig se på et initiativ som reaktion på fremkomsten af kryptoaktiver såsom bitcoin og denne nye teknologis konsekvenser for måden, hvorpå finansielle aktiver udstedes, udveksles, deles og tilgås.

Penge, der ikke hidrører fra lovlige aktiviteter, bør på ingen måde tolereres i Den Europæiske Union. I mere end tredive år har EU udviklet solide lovgivningsmæssige rammer for forebyggelse og bekæmpelse af **hvidvask af penge** og finansiering af terrorisme med fuld respekt for behovet for at beskytte personoplysninger. Ikke desto mindre er der voksende enighed om, at gennemførelsen af den nuværende ramme må forbedres betydeligt. Der skal tages hånd om de væsentlige forskelle i den måde, hvorpå den anvendes, og de alvorlige svagheder i håndhævelsen af reglerne. Som beskrevet i handlingsplanen fra maj 2020[105] arbejdes der på at vurdere mulighederne for at styrke EU's ramme for bekæmpelse af hvidvaskning af penge og bekæmpelse af finansiering af terrorisme. Der må bl.a. foretages en nærmere undersøgelse vedrørende samkøring af nationale centraliserede bankkontoregistre, hvilket i væsentlig grad kan afkorte den tid, det tager finansielle efterretningsenheder og kompetente myndigheder at få adgang til finansielle oplysninger.

Organiserede kriminelle gruppers fortjeneste anslås til 110 mia. EUR om året i EU. Det nuværende indsats omfatter harmoniseret lovgivning om konfiskation og inddrivelse af aktiver[106], for at forbedre indefrysningen og konfiskationen af aktiver fra kriminelle aktiviteter i EU samt fremme den gensidige tillid og et effektivt samarbejde på tværs af landegrænser mellem medlemsstaterne. Imidlertid konfiskeres kun ca. 1 % af denne fortjeneste[107], hvilket giver organiserede kriminelle grupper mulighed for at investere i at udvide deres kriminelle aktiviteter og infiltrere den lovlige økonomi — navnlig små og

[103] Jf. den europæiske grønne pagt (COM (2019) 640 final).
[104] Direktiv 2008/99/EF om strafferetlig beskyttelse af miljøet.
[105] Handlingsplan for forebyggelse af hvidvaskning af penge og finansiering af terrorisme (COM(2020) 2800).
[106] Ifølge EU-retten skal der oprettes kontorer for inddrivelse af aktiver i alle medlemsstaterne.
[107] Rapport om inddrivelse og konfiskation af aktiver: skabe sikkerhed for, at forbrydelse ikke betaler sig (COM(2020) 217).

mellemstore virksomheder, som har svært ved at opnå adgang til kredit, er et vigtigt mål for hvidvask af penge. Kommissionen vil analysere gennemførelsen af lovgivningen[108] og det eventuelle behov for flere fælles regler, herunder om administrativ konfiskation. Kontorerne for inddrivelse af aktiver[109], der er centrale aktører i proceduren for inddrivelse af aktiver, må også udstyres med bedre værktøjer til at identificere og opspore aktiver hurtigere i hele EU med henblik på at optrappe konfiskationssatserne.

Der er en tydelig forbindelse mellem organiseret kriminalitet og **korruption**. Det anslås, at korruption alene koster EU's økonomi 120 mia. EUR om året[110]. Forebyggelse og bekæmpelse af korruption vil fortsat være underlagt regelmæssig overvågning som led i retsstatsmekanismen og det europæiske semester. Det europæiske semester har vurderet udfordringerne ved korruptionsbekæmpelse i forbindelse med bl.a. offentlige indkøb, offentlig forvaltning, erhvervsmiljøet eller sundhedsplejen. Kommissionens årsrapport om retsstatsprincippet vil omfatte korruptionsbekæmpelse og danne grundlag for en forebyggende dialog med de nationale myndigheder og interessenter på EU-plan og nationalt plan. Civilsamfundsorganisationer kan også spille en central rolle ved at støtte de offentlige myndigheders indsats for at forebygge og bekæmpe organiseret kriminalitet og korruption, og disse organisationer kan med fordel føres sammen i et fælles forum. En anden vigtig dimension er samarbejde om og bistand til EU's naboregioners bekæmpelse af organiseret kriminalitet og korruption, som ikke lader sig hindre af landegrænserne.

De vigtigste tiltag
• Dagsorden for bekæmpelse af terrorisme i EU, herunder fornyede tiltag til bekæmpelse af radikalisering i EU • Nyt samarbejde med centrale tredjelande og internationale organisationer om bekæmpelse af terrorisme • Dagsorden for bekæmpelse af organiseret kriminalitet, herunder menneskehandel • EU's narkotikadagsorden og -handlingsplan 2021-2025 • Det Europæiske Overvågningscenter for Narkotika og Narkotikamisbrugs vurdering • EU's handlingsplan for 2020-2025 om ulovlig handel med skydevåben • Revision af lovgivningen om indefrysning og konfiskation og om kontorer for inddrivelse af aktiver • En vurdering af direktivet om miljøkriminalitet • En EU-handlingsplan for bekæmpelse af smugling af migranter, 2021-2025

4. 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 vil skulle engageres, udrustes og føres sammen på

[108] Direktiv 2014/42/EU om indefrysning og konfiskation af værktøjer og udbytte fra strafbart forhold.

[109] Rådets afgørelse 2007/845/RIA om samarbejde mellem medlemsstaternes kontorer for inddrivelse af aktiver om opsporing og identificering af udbyttet fra strafbart forhold eller andre formuegoder forbundet med kriminalitet.

[110] De samlede økonomiske omkostninger ved korruption lader sig vanskeligt vurdere, selv om det er blevet tilstræbt af nogle organer, herunder Det Internationale Handelskammer, Transparency International, FN's Global Compact-initiativ og Det Verdensøkonomiske Forum, og deres overslag tyder på, at korruption beløber sig til 5 % af det globale BNP.

rette vis for at opbygge beredskab og modstandsdygtighed for alle, navnlig de mest sårbare, ofre og vidner.

Sikkerhedsdimensionen må indgå i alle politikker, og EU kan bidrage på alle niveauer. I hjemmet er vold i familien en af de alvorligste sikkerhedsrisici. I EU har 22 % af kvinderne været udsat for vold fra en partners side[111]. EU's tiltrædelse af Istanbulkonventionen om forebyggelse og bekæmpelse af vold mod kvinder og vold i hjemmet prioriteres fortsat højt. Hvis forhandlingerne fortsat blokeres, vil Kommissionen træffe andre foranstaltninger for at nå konventionens mål, herunder et forslag om at tilføje vold mod kvinder til listen over strafbare handlinger i EU, der er defineret i traktaten.

Samarbejde og informationsudveksling

Et af de mest betydelige bidrag, som EU kan yde for at beskytte borgerne, går ud på at styrke samarbejdet mellem de instanser, der er ansvarlige for sikkerheden. Samarbejde og informationsudveksling er de mest effektive værktøjer til bekæmpelse af kriminalitet og terrorisme og til at opretholde retsordenen. Af hensyn til effektiviteten skal dette foregå på en målrettet og rettidig måde. Hvis de implicerede skal have tillid til indsatsen, skal der indføres fælles sikkerhedsforholdsregler og kontrolforanstaltninger.

Der er oprettet en række EU-instrumenter og sektorspecifikke strategier[112] med henblik på at videreudvikle **det operationelle retshåndhævelsessamarbejde** mellem medlemsstaterne. Et af de vigtigste EU-instrumenter til støtte for retshåndhævelsessamarbejdet mellem medlemsstaterne er Schengeninformationssystemet, der anvendes til at udveksle oplysninger om eftersøgte og forsvundne personer og genstande i realtid. Dette har givet resultater i form af arrestation af kriminelle, beslaglæggelse af narkotika og redning af potentielle ofre[113]. Samarbejdsniveauet kan dog stadig forbedres ved at strømline og opgradere de instrumenter, der står til rådighed. Hovedparten af EU's retlige rammer, der ligger til grund for det operationelle retshåndhævelsessamarbejde, blev udformet for 30 år siden. Medlemsstaterne har indgået et komplekst net af bilaterale aftaler, hvoraf mange er forældede eller ikke udnyttes i tilstrækkeligt omfang, hvilket indebærer en risiko for fragmentering. I mindre stater eller indlandsstater skal retshåndhævelsespersonalet, der arbejder på tværs af landegrænserne, udføre deres operationelle foranstaltninger efter op til syv forskellige regelsæt: Resultatet er, at nogle operationer, f.eks. forfølgelse af mistænkte over de indre grænser, ganske enkelt ikke finder sted. Det operationelle samarbejde om ny teknologi såsom droner er heller ikke omfattet af den gældende EU-ramme.

Den operationelle effektivitet kan understøttes af et specifikt retshåndhævelsessamarbejde, som også kan medvirke til at støtte andre politiske mål, f.eks. ved at give sikkerhedsrelateret input til den nye vurdering af udenlandske direkte investeringer. Kommissionen vil se på, hvordan en kodeks for politisamarbejde kan understøtte dette. Medlemsstaternes retshåndhævende myndigheder har i stigende grad gjort brug af støtte og ekspertise på EU-plan, samtidig med at EU INTCEN har spillet en central rolle i at fremme udvekslingen af strategiske efterretninger mellem medlemsstaternes efterretnings- og sikkerhedstjenester, hvormed der tilvejebringes efterretninger og situationskendskab til fordel for EU-institutionerne[114]. **Europol** kan også spille en central rolle i at udvide sit samarbejde med

[111] Et EU med ligestilling: strategi for ligestilling mellem mænd og kvinder 2020-2025 (COM(2020) 152).

[112] Som f.eks. handlingsplanen for EU's maritime sikkerhedsstrategi, der førte til vigtige resultater for så vidt angår de relevante EU-agenturers samarbejde om kystvagtfunktioner.

[113] EU's bekæmpelse af organiseret kriminalitet i 2019 (Rådet, 2020).

[114] EU INTCEN fungerer som den eneste gateway for medlemsstaternes efterretnings- og sikkerhedstjenester med henblik på at forsyne EU med efterretningsbaseret situationskendskab.

tredjelande til at bekæmpe kriminalitet og terrorisme i sammenhæng med EU's øvrige eksterne politikker og værktøjer. Indtil videre står Europol imidlertid over for en række alvorlige begrænsninger — navnlig for så vidt angår direkte udveksling af personoplysninger med private parter — hvilket forhindrer agenturet i effektivt at støtte medlemsstaterne i bekæmpelsen af terrorisme og kriminalitet. Europols mandat vurderes for øjeblikket for at se nærmere på, hvordan det bør forbedres for at sikre, at agenturet kan varetage sine beføjelser fuldt ud. I den forbindelse bør relevante myndigheder på EU-niveau (f.eks. OLAF, Europol, Eurojust og Den Europæiske Anklagemyndighed) samarbejde tættere og forbedre informationsudvekslingen.

En anden central sammenhæng består i den videre udvikling af **Eurojust** med henblik på at maksimere synergien mellem retshåndhævelsessamarbejde og det retlige samarbejde. EU vil også drage fordel af større sammenhæng på strategisk plan: med **EMPACT**[115], EU's politikcyklus for organiseret og grov international kriminalitet, tilvejebringes en kriminalefterretningsbaseret metode, som myndighederne kan bruge til i fællesskab at imødegå de vigtigste kriminalitetstrusler, der berører EU. Den har skabt vigtige operationelle resultater[116] i det seneste årti. Baseret på aktørernes erfaringer bør den eksisterende mekanisme strømlines og forenkles for bedre at kunne imødegå de mest presserende og foranderlige kriminalitetstrusler, og dette bør ske i forbindelse med en ny politikcyklus for 2022-2025.

Rettidig og relevant **information** har afgørende betydning for arbejdet med at bekæmpe kriminalitet. På trods af udviklingen af nye EU-databaser for sikkerhed og grænseforvaltning ligger mange oplysninger stadig i nationale databaser, eller også udveksles de uden for disse værktøjer. Dette fører til en betydelig ekstra arbejdsbyrde, forsinkelser og en øget risiko for, at vigtige oplysninger overses. Bedre resultater kan opnås med bedre, hurtigere og enklere procedurer, der inddrager hele sikkerhedssamfundet. De rette værktøjer er af afgørende betydning, hvis informationsudvekslingen skal kunne opfylde sit potentiale med hensyn til effektivt at forfølge kriminalitet med de nødvendige beskyttelsesforanstaltninger, således at dataudvekslingen overholder databeskyttelseslovgivningen og de grundlæggende rettigheder. I lyset af den teknologiske, kriminaltekniske og databeskyttelsesmæssige udvikling og ændrede operationelle behov kan EU overveje, om der er behov for med henblik på strafferetlig efterforskning at modernisere instrumenter såsom **Prümafgørelserne fra 2008**, etablere automatiseret udveksling af DNA, fingeraftryk og oplysninger fra køretøjsregistre for at muliggøre elektronisk udveksling af yderligere datakategorier, der allerede findes i medlemsstaternes strafferetlige eller andre databaser. Desuden vil Kommissionen undersøge muligheden for at udveksle straffeattester for at hjælpe med at fastslå, om en given enkeltperson har en straffeattest i andre medlemsstater, og lette adgangen til disse attester, når sådanne findes, under opretholdelse af alle de nødvendige beskyttelsesforanstaltninger.

Oplysninger om rejsende har bidraget til at forbedre grænsekontrollen, begrænse den irregulære migration og identificere personer, der udgør en sikkerhedsrisici. Forhåndsoplysninger om passagerer er de biografiske data for hver passager, som luftfartsselskaberne registrerer ved indtjekning, og de sendes på forhånd til grænsekontrolmyndighederne på bestemmelsesstedet. Revisionen af de retlige rammer[117] kan åbne mulighed for at anvende oplysningerne mere effektivt, samtidig med at det sikres,

[115] EMPACT står for Den europæiske tværfaglige platform mod kriminalitetstrusler.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/da/pdf.
[117] Rådets direktiv 2004/82/EF om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer.

at databeskyttelseslovgivningen efterleves, og passagerstrømmen lettes. Passagerlister (PNR) rummer de data, som passagerer afgiver, når de bestiller flybilletter. Gennemførelsen af PNR-direktivet[118] har afgørende betydning, og Kommissionen vil fortsat støtte og håndhæve dette. Desuden vil Kommissionen på mellemlang sigt iværksætte en revision af den nuværende tilgang til **overførsel af PNR-data til tredjelande**.

Det retlige samarbejde er et nødvendigt supplement til politiets indsats for at bekæmpe grænseoverskridende kriminalitet. Det retlige samarbejde har gennemgået en mere dybtgående forandring i de seneste 20 år. Organer såsom **Den Europæiske Anklagemyndighed** og **Eurojust** har behov for midler til at fungere i fuldt omfang eller blive styrket. Samarbejdet mellem de retslige aktører kan også styrkes gennem yderligere tiltag vedrørende gensidig anerkendelse af retsafgørelser, uddannelse af de retslige aktører og informationsudveksling. Målet bør være at styrke den gensidige tillid blandt dommere og anklagere, som har central betydning for, at retstvister på tværs af landegrænserne forløber smidigt. Brugen af **digital teknologi** kan også forbedre effektiviteten af vores retssystemer. Der oprettes et nyt digitalt udvekslingssystem til fremsendelse af europæiske efterforskningskendelser, anmodninger om gensidig retlig bistand og tilhørende meddelelser mellem medlemsstaterne med bistand fra Eurojust. Kommissionen vil samarbejde med medlemsstaterne om at fremskynde indførelsen af de nødvendige IT-systemer på nationalt plan.

Internationalt samarbejde er også af afgørende betydning for en effektiv retshåndhævelse og det retlige samarbejde. Bilaterale aftaler med vigtige partnere spiller en central rolle i at sikre information og bevismateriale fra lande uden for EU. **Interpol**, der er en af de største mellemstatslige kriminalpolitiorganisationer, spiller en vigtig rolle. Kommissionen vil undersøge mulighederne for at styrke samarbejdet med Interpol, herunder om muligt adgang til Interpols databaser, og styrke det operationelle og strategiske samarbejde. De retshåndhævende myndigheder i EU er også afhængige af vigtige partnerlande i bestræbelserne på at afsløre og efterforske kriminelle og terrorister. **Sikkerhedspartnerskaberne mellem EU og tredjelande** kan intensiveres for at styrke samarbejdet om at bekæmpe fælles trusler som f.eks. terrorisme, organiseret kriminalitet, cyberkriminalitet, seksuelt misbrug af børn og menneskehandel. En sådan tilgang vil være baseret på fælles sikkerhedsinteresser og bygge på etablerede samarbejds- og sikkerhedsdialoger.

Foruden informationsudveksling kan udveksling af ekspertise få særlig stor værdi, når det drejer sig om at øge beredskabet i forbindelse med retshåndhævelse over for **ikketraditionelle trusler**. Ud over at tilskynde til udveksling af bedste praksis vil Kommissionen granske mulighederne for at etablere en **koordineringsmekanisme på EU-plan for politistyrker** i tilfælde af force majeure såsom pandemier. Pandemien har ligeledes gjort det klart, at politiarbejdet i det digitale samfund — ledsaget af en retlig ramme for at lette politiarbejdet online — vil få afgørende betydning for bekæmpelsen af kriminalitet og terrorisme. Partnerskaber mellem politi og samfund, offline og online, kan forebygge kriminalitet og afbøde virkningerne af organiseret kriminalitet, radikalisering og terroraktiviteter. Forbindelsen fra lokale til regionale, nationale og EU-dækkende politiløsninger er en central succesfaktor for EU's sikkerhedsunion som helhed.

Bidraget fra solide ydre grænser

[118] Direktiv 2016/681 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet.

En moderne og effektiv forvaltning af de ydre grænser rummer den dobbelte fordel, at Schengenområdets integritet bevares, og der tilvejebringes sikkerhed for vores borgere. Inddrages alle relevante aktører med henblik på at optimere sikkerheden ved den ydre grænse, kan dette få en reel indvirkning på forebyggelsen af grænseoverskridende kriminalitet og terrorisme. De fælles operationelle aktiviteter i den nyligt styrkede europæiske grænse- og kystvagt[119] bidrager til at forebygge og afsløre grænseoverskridende kriminalitet ved de **ydre grænser** og uden for EU. Toldaktiviteter med henblik på at afsløre sikkerhedsrisici ved alle varer, inden de ankommer til EU, og varekontrollen ved ankomsten er afgørende for bekæmpelsen af grænseoverskridende kriminalitet og terrorisme. I den kommende handlingsplan om toldunionen vil der også blive bebudet en indsats for at styrke risikostyringen og øge den indre sikkerhed, navnlig ved at vurdere gennemførligheden af at sammenknytte relevante informationssystemer med henblik på risikoanalyse.

Rammen for **interoperabilitet mellem EU's informationssystemer** på området retlige og indre anliggender blev vedtaget i maj 2019. Denne nye arkitektur har til formål at forbedre effektiviteten af de nye eller opgraderede informationssystemer[120]. Den vil udmønte sig i hurtigere og mere systematisk information til retshåndhævelsespersonale, grænsevagter og migrationsembedsmænd. Det vil lette arbejdet med at foretage en korrekt identifikation og medvirke til at bekæmpe identitetssvig. For at virkeliggøre dette bør gennemførelsen af interoperabilitet prioriteres højt, både på politisk og teknisk plan. Et nært samarbejde mellem EU-agenturer og alle medlemsstaterne vil være af afgørende betydning for at nå målet om fuld interoperabilitet senest i 2023.

Svig med rejsedokumenter anses for en af de hyppigst begåede forbrydelser. Den letter kriminelles og terroristers ulovlige trafik og spiller en central rolle i menneskehandelen og narkotikahandelen[121]. Kommissionen vil undersøge nærmere, hvordan det eksisterende arbejde med sikkerhedsstandarderne for EU's opholds- og rejsedokumenter kan udbygges, bl.a. med digitalisering. Fra august 2021 vil medlemsstaterne begynde at udstede identitetskort og opholdsdokumenter efter harmoniserede sikkerhedsstandarder, herunder en chip med biometriske identifikatorer, der kan kontrolleres af alle EU-grænsemyndigheder. Kommissionen vil overvåge gennemførelsen af disse nye regler, herunder den løbende ombytning af de dokumenter, der i øjeblikket benyttes.

Styrkelse af forskning og innovation på sikkerhedsområdet

Arbejde for at garantere cybersikkerhed og bekæmpe organiseret kriminalitet, cyberkriminalitet og terrorisme afhænger i høj grad af, at der udvikles værktøjer til denne fremtid: der må bidrages til at skabe en mere sikker ny teknologi, udfordringerne ved den nye teknologi må imødegås, og retshåndhævelsen må støttes. Dette afhænger af private partnere og industrier.

Innovation bør anskues som et strategisk værktøj til at imødegå aktuelle trusler og forudse fremtidige risici og muligheder. Innovativ teknologi kan forsyne de retshåndhævende myndigheder og andre sikkerhedsaktører med nye værktøjer. Kunstig intelligens og analyse

[119] Består af Det Europæiske Agentur for Grænse- og Kystbevogtning (Frontex) og medlemsstaternes grænsemyndigheder og kystvagter.

[120] Ind- og udrejsesystemet (EES), det europæiske system vedrørende rejseinformation og rejsetilladelse (ETIAS), det udvidede europæiske informationssystem vedrørende strafferegistre (ECRIS-TCN-systemet), Schengeninformationssystemet, visuminformationssystemet og det fremtidige opdaterede Eurodac.

[121] Forbindelsen mellem dokumentfalsk og menneskehandel omhandles i den anden rapport om de fremskridt, der er gjort i bekæmpelsen af menneskehandel, (COM(2018) 777) og det dertil knyttede SWD(2018) 473 samt Europols situationsrapport om menneskehandel i EU, 2016.

af big data kan udnytte højtydende databehandling til at tilbyde bedre afsløring og hurtig og omfattende analyse[122]. En central forudsætning for at udvikle pålidelige teknologier er datasæt af høj kvalitet, som de kompetente myndigheder skal have til rådighed for at træne, teste og validere algoritmer[123]. Mere overordnet set er risikoen for teknologisk afhængighed betydelig i vores nuværende situation — EU er f.eks. nettoimportør af cybersikkerhedsprodukter og -tjenester med alt, hvad dette indebærer for økonomien og kritiske infrastrukturer. For at beherske teknologien og garantere forsyningssikkerheden selv i tilfælde af utilsigtede hændelser og kriser har Europa brug for at være til stede og råde over kapacitet i de relevante værdikæders kritiske dele.

EU's **forskning, innovation og teknologiske udvikling** giver mulighed for at tage sikkerhedsdimensionen i betragtning, efterhånden som teknologien og anvendelsen heraf udvikles. Den næste generation af EU-finansieringsforslag kan få en væsentlig stimulerende effekt[124]. I initiativer vedrørende europæiske dataområder og cloudinfrastrukturer iagttages sikkerhedsaspektet fra første færd. Det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre[125] har til formål at etablere en effektiv struktur til at samle og dele forskningskapacitet og -resultater angående cybersikkerhed. EU's rumprogram leverer tjenester, der støtter EU's, dets medlemsstaters og enkeltpersoners sikkerhed[126].

Med over 600 iværksatte projekter siden 2007 til en samlet værdi på næsten 3 mia. EUR er EU-finansieret sikkerhedsforskning et centralt instrument, hvormed teknologi og viden fremmes til støtte for sikkerhedsløsninger. Som led i revisionen af Europols beføjelser vil Kommissionen undersøge, om der kan oprettes et **europæisk innovationscenter for indre sikkerhed**[127], som får til opgave levere fælles løsninger på fælles sikkerhedsudfordringer og -muligheder, som medlemsstaterne muligvis ikke kan udnytte på egen hånd. Samarbejdet har grundlæggende betydning for at nyttemaksimere investeringerne og udvikle innovativ teknologi med både sikkerhedsrelaterede og økonomiske fordele.

Færdigheder og bevidstgørelse

Bevågenhed om 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. Udfordringerne for IT-infrastruktur og e-systemer har vist, at det er nødvendigt at forbedre vores menneskelige kapacitet med hensyn til beredskabsplaner på cybersikkerhedsområdet. Pandemien har også understreget betydningen af digitalisering på tværs af alle områder af EU's økonomi og samfund.

[122] I den forbindelse bør der trækkes på Kommissionens strategi for kunstig intelligens.

[123] En europæisk strategi for data (COM(2020) 66 final).

[124] Kommissionens forslag til Horisont Europa, Fonden for Intern Sikkerhed, Fonden for Integreret Grænseforvaltning, EUInvest-programmet, Den Europæiske Fond for Regionaludvikling og programmet for et digitalt Europa støtter udvikling og udbredelse af innovative sikkerhedsteknologier og -løsninger i hele sikkerhedskæden.

[125] Forslag af 12. september 2018 om oprettelse af det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed og netværket af nationale koordinationscentre (COM(2018) 630).

[126] Eksempelvis leverer Copernicus tjenester, der gør det muligt at overvåge EU's ydre grænser og have, hvilket medvirker til at bekæmpe pirateri og smugling samt støtte kritiske infrastrukturer. Når dette program er fuldt operationelt, vil det være en central katalysator for civile og militære missioner og operationer.

[127] Det vil også samarbejde med EBCGA/Frontex, Cepol, eu-LISA og Det Fælles Forskningscenter.

Blot en **grundlæggende viden om sikkerhedstrusler** og om, hvordan de kan bekæmpes, kan få en reel indvirkning på samfundets modstandsdygtighed. Bevidsthed om risiciene ved cyberkriminalitet og nødvendigheden af at beskytte sig selv mod cyberkriminalitet kan gå hånd i hånd med internetudbydernes beskyttelsesforanstaltninger for at imødegå cyberangreb. Oplysninger om farerne og risiciene ved narkotikahandel kan gøre det vanskeligere for kriminelle at lykkes med deres forehavende. EU kan fremme udbredelsen af bedste praksis, f.eks. gennem netværket af centre for sikkert internet[128], og sikre, at sådanne mål indgår i EU's egne programmer.

Den kommende handlingsplan for digital uddannelse bør omfatte målrettede foranstaltninger til at opbygge IT-færdigheder hos hele befolkningen. Med den nyligt vedtagne dagsorden for færdigheder[129] støttes tilegnelsen af færdigheder gennem hele livet. Det omfatter særlige tiltag, der skal øge antallet af kandidater inden for naturvidenskab, teknologi, ingeniørteknik, humanistiske fag og matematik, som er nødvendige inden for avancerede områder såsom cybersikkerhed. Yderligere tiltag, der finansieres af programmet for et digitalt Europa, vil gøre det muligt for fagfolk at holde trit med udviklingen i sikkerhedstruslen og samtidig afhjælpe manglen på arbejdskraft i EU på dette område. Alt i alt vil enkeltpersoner få mulighed for at tilegne sig færdigheder til at håndtere sikkerhedstrusler, og erhvervslivet vil få mulighed for at finde de fagfolk, de har brug for på området. Det kommende europæiske forskningsrum og det europæiske uddannelsesområde vil også opmuntre til at følge karrierer inden for videnskab, teknologi, ingeniørteknik, humanistiske fag og matematik.

Det er også vigtigt, at **ofrene** kan gøre brug af deres rettigheder. De skal ydes den nødvendige bistand og den støtte, de har behov for, i lyset af deres særlige situation. Der er behov for en særlig indsats, når det drejer sig om mindretal og de mest sårbare ofre, f.eks. børn eller kvinder, som er ofre for menneskehandel med henblik på seksuel udnyttelse, eller som udsættes for vold i hjemmet[130].

Styrkede **kompetencer inden for retshåndhævelse** har en særlig rolle at spille. De aktuelle og nye teknologiske trusler gør det påkrævet at investere mere i at opkvalificere retshåndhævelsespersonalet på det tidligst mulige stadium og i deres samlede karriereforløb. Cepol er en vigtig partner, der bistår medlemsstaterne med at løse denne opgave. Uddannelse i retshåndhævelse vedrørende racisme, fremmedhad og borgernes rettigheder generelt skal være en vigtig del af EU-sikkerhedskulturen. De nationale retssystemer og retsvæsenets aktører må også udrustes således, at de kan tilpasse sig og sætte ind over for hidtil usete udfordringer. Uddannelse er vigtig for at sætte myndighederne i marken i stand til at udnytte disse værktøjer i en operationel situation. Desuden bør der gøres alt for at styrke integrationen af kønsaspektet og styrke kvinders deltagelse i retshåndhævelsen.

De vigtigste tiltag
• Styrkelse af Europols beføjelser • Undersøgelse af en EU-kodeks for politisamarbejde og koordinering af politiet i krisesituationer

[128] Jf. www.betterinternetforkids.eu: Den centrale portal og de nationale centre for sikkert internet finansieres i øjeblikket under CEF/Telekommunikation, men der er fremsat forslag om, at programmet for et digitalt Europa varetager finansieringen fremover.

[129] Den europæiske dagsorden for færdigheder med henblik på bæredygtig konkurrenceevne, social retfærdighed og modstandsdygtighed (COM(2020) 274 final).

[130] Jf. strategien for ligestilling mellem mænd og kvinder (COM(2020) 152), EU-strategien for ofres rettigheder (COM(2020) 258) og den europæiske strategi for et bedre internet for børn (COM(2012) 196 final).

- Styrkelse af Eurojust for at skabe forbindelse mellem de retshåndhævende og de retslige myndigheder
- Revision af direktivet om forhåndsoplysninger om passagerer
- Meddelelse om den eksterne dimension af passagerlister
- Styrket samarbejde mellem EU og Interpol
- En ramme for forhandlinger med centrale tredjelande om informationsdeling
- Bedre sikkerhedsstandarder for rejsedokumenter
- Undersøgelse af et europæisk innovationscenter for indre sikkerhed

V. Konklusion

I en stadig mere turbulent verden betragtes Den Europæiske Union endnu generelt som et af de sikreste steder. Dette kan imidlertid ikke tages for givet.

Den nye strategi for EU's sikkerhedsunion danner grundlag for et sikkerhedsøkosystem, der spænder over hele Den Europæiske Union. Den har rod i bevidstheden om, at sikkerhed er et fælles ansvar. Sikkerhed er et emne, der berører alle. Alle organer i den offentlige forvaltning, virksomheder, sociale organisationer, institutioner og borgere må leve op til deres ansvar for at gøre vore samfund mere sikre.

Sikkerhedsspørgsmål må nu ses i et langt bredere perspektiv end førhen. Det kunstige skel mellem det fysiske og det digitale område i henseende til sikkerhed må vi lægge bag os. Strategien for EU's sikkerhedsunion samler hele spektret af sikkerhedsbehov og fokuserer på de områder, der bliver mest kritiske for EU's sikkerhed i de kommende år. Den rummer også en anerkendelse af, at sikkerhedstruslerne ikke respekterer de geografiske grænser, og det faktum, at den indbyrdes forbindelse mellem den indre og ydre sikkerhed bliver stadig mere tydelig[131]. I den forbindelse er det vigtigt for EU at samarbejde med internationale partnere om at beskytte alle EU-borgere og opretholde en tæt koordinering med EU's optræden udadtil ved gennemførelsen af denne strategi.

Vores sikkerhed er knyttet til vores grundlæggende værdier. Alle foreslåede tiltag og initiativer i denne strategi vil fuldt ud respektere de grundlæggende rettigheder og vores europæiske værdier. Disse udgør fundamentet for vores europæiske livsstil og skal forblive centralt placeret i alt vores arbejde.

Endelig er Kommissionen helt på det rene med, at enhver politik eller handling helt og holdent afhænger af gennemførelsen. Der er derfor behov for en løbende indsats for at sikre en korrekt gennemførelse og håndhævelse af eksisterende og fremtidig lovgivning. Dette vil blive overvåget ved hjælp af regelmæssige rapporter om sikkerhedsunionen, og Kommissionen vil holde Europa-Parlamentet, Rådet og interessenter fuldt underrettet om og inddraget i alle relevante tiltag. Desuden er Kommissionen rede til at deltage i og tilrettelægge fælles drøftelser med institutionerne om strategien for sikkerhedsunionen for sammen at gøre status over de opnåede fremskridt og samtidig se på de kommende udfordringer.

Kommissionen opfordrer Europa-Parlamentet og Rådet til at give deres tilslutning til denne strategi for EU's sikkerhedsunion som grundlag for samarbejdet og den fælles indsats sikkerhedsområdet i de næste fem år.

[131] Jf. EU's globale strategi