EUROPA-
KOMMISSIONEN

Bruxelles, den 30.10.2019
COM(2019) 552 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET, DET EUROPÆISKE RÅD OG RÅDET

20. statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion

I. INDLEDNING

Dette er den 20. statusrapport om de yderligere fremskridt, der er gjort med indførelsen af en effektiv og ægte sikkerhedsunion. Rapporten beskriver udviklingen på to hovedområder: bekæmpelse af terrorisme og organiseret kriminalitet og de midler, der støtter dem, samt styrkelse af vores forsvar og opbygning af modstandsdygtighed over for disse trusler.

Juncker-Kommissionen gjorde lige fra begyndelsen sikkerhed til en topprioritet. Med udgangspunkt i den europæiske dagsorden om sikkerhed af april 2015[1] og meddelelsen af april 2016, der baner vejen for en effektiv og ægte sikkerhedsunion[2], har EU reageret koordineret på en række terrorangreb og andre voksende sikkerhedsudfordringer og gjort væsentlige fremskridt med hensyn til at øge vores fælles sikkerhed[3]. Det står stadig mere klart, at de sikkerhedsmæssige udfordringer, vi i dag står over for, er fælles trusler — hvad enten det er terrorisme, organiseret kriminalitet, cyberangreb, desinformation eller andre nye cyberbaserede trusler. Kun ved at arbejde sammen kan vi opnå det niveau af kollektiv sikkerhed, som borgerne med rette kræver og forventer. Denne fælles forståelse har været grundlaget for de fremskridt, der er gjort med at indføre en effektiv og ægte sikkerhedsunion. Baseret på de nationale myndigheders behov for at garantere deres borgeres sikkerhed har støtten på EU-plan været koncentreret om lovgivningsmæssige og operationelle foranstaltninger, hvor en fælles indsats kan øge medlemsstaternes sikkerhed. Indsatsen er foregået i tæt samarbejde med Europa-Parlamentet og Rådet og i fuld åbenhed over for den brede offentlighed. Det har været centralt for indsatsen at sikre fuld overholdelse af de grundlæggende rettigheder, da sikkerheden i EU kun kan garanteres, hvis borgerne har tillid til, at deres grundlæggende rettigheder respekteres fuldt ud.

EU har arbejdet på at **bekæmpe terrorisme** ved at begrænse terroristernes råderum gennem nye regler, der gør det vanskeligere for dem at få adgang til sprængstoffer, skydevåben og finansiering, og ved at begrænse deres bevægelser. EU har intensiveret udvekslingen af oplysninger for at give de politibetjente og grænsevagter, der befinder sig i frontlinjen, effektiv adgang til nøjagtige og fuldstændige oplysninger ved at udnytte de eksisterende oplysninger optimalt, lukke huller og dække blinde vinkler. En stærk beskyttelse af de ydre grænser er en forudsætning for at holde området med fri bevægelighed uden kontrol ved de indre grænser sikkert. I marts 2019 nåede Europa-Parlamentet og Rådet til enighed om en yderligere styrket og fuldt udstyret **europæisk grænse- og kystvagt**, og den nye forordning forventes at træde i kraft i begyndelsen af december 2019. EU har stillet en platform og finansiering til rådighed for folk, som i deres lokalsamfund arbejder på at udveksle god praksis til **bekæmpelse af radikalisering og forebyggelse af voldelig ekstremisme,** og har derudover foreslået nye regler til effektiv fjernelse af terrorrelateret onlineindhold. EU's bistand har været med til at **gøre byer mere modstandsdygtige** over for angreb via handlingsplaner til støtte for beskyttelsen af offentlige steder og til styrkelse af beredskabet over for kemiske, biologiske, radiologiske og nukleare sikkerhedsrisici. EU har taget hånd om **cybersikkerheden og cyberbaserede trusler** ved at indføre en ny EU-strategi for cybersikkerhed og vedtage relevant lovgivning og ved at bekæmpe **desinformation** for bedre at kunne beskytte vores valg. Der arbejdes stadig på at øge sikkerheden i **kritisk digital infrastruktur**, bl.a. ved at styrke samarbejdet om **cybersikkerheden i 5G-net** på tværs af Europa.

Og vi er endnu ikke færdige. Det livestreamede angreb på en synagoge og drabet på to borgere i den tyske by Halle den 9. oktober 2019 var en chokerende påmindelse om den trussel, som voldelig højreekstremisme og antisemitisme udgør. Hermed blev der endnu en gang sat fokus på misbrug af internettet til terrorpropaganda og det deraf følgende **behov for EU-dækkende regler for sletning af terrorrelateret onlineindhold**. Rådet for Retlige og Indre Anliggender drøftede den 7.-8. oktober 2019 voldelig ekstremisme og terrorisme på højrefløjen og understregede behovet for en yderligere indsats, herunder for at bekæmpe udbredelsen af ulovligt højreekstremistisk indhold online og offline.

---

1 COM(2015) 185 final af 28.4.2015.
2 COM(2016) 230 final af 20.4.2016.
3 Se de tidligere statusrapporter om indførelsen af en effektiv og ægte sikkerhedsunion her: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

Samtidig viser drabet på tre politibetjente og en af de øvrige ansatte på politihovedkvarteret i Paris den 3. oktober 2019, at jihadinspireret terror stadig udgør en reel trussel, og at medlemsstaterne fortsat behøver løbende hjælp til at håndtere denne trussel. De fængslede ISIS/Daesh-medlemmers flugt i forbindelse med de nylige begivenheder i det nordlige Syrien kan få alvorlige konsekvenser for Europas sikkerhed. Det er vigtigt, at medlemsstaterne gør fuldt brug af de eksisterende informationssystemer til at opdage og identificere fremmedkrigere, når disse passerer de ydre grænser. Der arbejdes også på at kunne anvende oplysninger fra krigszonerne til at retsforfølge fremmedkrigere.

Denne rapport beskriver de seneste skridt, der er taget hen imod en effektiv og ægte sikkerhedsunion, med fokus på områder, hvor yderligere tiltag er påkrævet. I rapporten gøres der status over gennemførelsen af de vedtagne foranstaltninger angående **cybersikkerheden i 5G-net**, herunder navnlig med hensyn til **EU's risikovurderingsrapport**, der blev offentliggjort den 9. oktober 2019, og over bekæmpelsen **af desinformation**.

Rapporten har særligt fokus på **den eksterne dimension** af samarbejdet i sikkerhedsunionen, bl.a. underskrivelsen af to bilaterale **antiterrorordninger** med Albanien og Republikken Nordmakedonien og de fremskridt, der er sket i samarbejdet med tredjelandspartnere om udveksling af **passagerlisteoplysninger**. Sideløbende med denne rapport har Kommissionen også vedtaget en anmodning om bemyndigelse til at indlede forhandlinger om en aftale mellem EU og **New Zealand** om udveksling af personoplysninger for at bekæmpe grov kriminalitet og terrorisme.

II. REALISERING AF LOVGIVNINGSMÆSSIGE PRIORITETER

1. Forebyggelse af radikalisering online og i samfundet

Forebyggelse af radikalisering er et vigtigt element i Unionens indsats over for terrortruslen. Hvad angår terrorhandlinger i det 21. århundrede, har internettet spillet en vigtig rolle. Et sådant rum, hvor radikaliserede personer kan kommunikere og dele indhold med hinanden, gør det muligt at udvikle og udbygge verdensomspændende netværk af både jihadister og voldelige højreekstremister. Derfor fortsætter Kommissionen sin tostrengede tilgang til bekæmpelse af radikalisering på internettet, hvor de foreslåede regler for fjernelse af terrorrelateret onlineindhold skal styrke det frivillige partnerskab med onlineplatformene.

En væsentlig forudsætning for dette er **lovgivningsforslaget om forebyggelse af udbredelsen af terrorrelateret onlineindhold** med klare regler og garantier, der vil gøre det obligatorisk for internetplatforme at fjerne terrorrelateret indhold inden for en time, når de modtager et påbud fra de kompetente myndigheder, og at træffe proaktive foranstaltninger, der står i et rimeligt forhold til graden af eksponering for terrorrelateret indhold[4]. De interinstitutionelle forhandlinger mellem Europa-Parlamentet og Rådet er i gang, og det første trepartsmøde fandt sted den 17. oktober 2019. I lyset af truslen fra terrorrelateret onlineindhold opfordrer Kommissionen Europa-Parlamentet og Rådet til at nå til enighed om den foreslåede lovgivning inden udgangen af 2019.

Den foreslåede lovgivning supplerer det frivillige partnerskab med internetbranchen og andre interessenter inden for rammerne af **EU's internetforum**. Forummet har siden sin oprettelse i 2015 været en katalysator for internetvirksomhederne til proaktivt at identificere og fjerne terrorrelateret onlineindhold og har dermed banet vejen for det branchestyrede initiativ om en "delt database over hashtags"[5] og for oprettelsen af "Global Internet Forum to Counter Terrorism" (det globale internetforum til terrorbekæmpelse). EU's internetindberetningsenhed har som en del af EU's

[4] COM(2018) 640 final af 12.9.2018.

[5] Et værktøj, som et konsortium af virksomheder har oprettet for at fremme samarbejdet om at hindre spredning af terrorrelateret indhold på tværs af platforme.

retshåndhævende agentur Europol været et afgørende bidrag til det styrkede samarbejde med internetvirksomhederne og til de overordnede mål for EU's internetforum. På det seneste ministermøde i EU's internetforum den 7. oktober 2019 forpligtede EU's medlemsstater og højtstående repræsentanter for internetvirksomhederne sig til at samarbejde inden for rammerne af den såkaldte **EU-kriseprotokol**. I EU-kriseprotokollen defineres tærsklerne for et øget samarbejde, og der udstikkes nye veje til et forbedret kriseberedskab. Dette er en del af den internationale indsats for at gennemføre Christchurch-opfordringen[6] med henblik på at sikre et koordineret og hurtigt beredskab, der kan dæmme op for den virale spredning af terrorrelateret og voldeligt ekstremistisk onlineindhold.

Ud over disse foranstaltninger til bekæmpelse af radikalisering på internettet støtter Kommissionen fortsat nationale og lokale initiativer til **forebyggelse og bekæmpelse af radikalisering i lokalsamfundet**. På grundlag af den store erfaring og ekspertise, der er samlet inden for netværket til bevidstgørelse omkring radikalisering, tilbyder EU målrettet støtte til lokale aktører, herunder byer[7], og mulighed for udveksling mellem fagfolk, forskere og politiske beslutningstagere. Netværket har f.eks. udstedt specifikke retningslinjer og arrangeret workshops, der skal hjælpe de kompetente myndigheder med at tage sig af børn fra konfliktområder[8]. For at sikre kontinuiteten i de aktiviteter, som netværket til bevidstgørelse omkring radikalisering udfører, har Kommissionen indledt proceduren vedrørende en ny rammekontrakt til en anslået værdi af 61 mio. EUR over en periode på fire år med start i 2020[9].

For at imødegå truslen fra terrorrelateret onlineindhold opfordrer Kommissionen Europa-Parlamentet og Rådet til:

- at færdigforhandle lovgivningsforslaget om forebyggelse af udbredelsen af **terrorrelateret onlineindhold** inden årets udgang.

2. Stærkere og mere intelligente informationssystemer i forbindelse med sikkerhed og grænse- og migrationsforvaltning

EU har intensiveret udvekslingen af oplysninger og derved gjort det lettere at bekæmpe identitetssvig[10], styrke ind- og udrejsekontrol[11], modernisere databaser på retshåndhævelsesområdet[12],

---

6 Som reaktion på angrebene i Christchurch i New Zealand den 15. marts 2019 inviterede den franske præsident Emmanuel Macron og New Zealands premierminister Jacinda Ardern ledere og onlineplatforme til Paris den 15. maj 2019 for at lancere Christchurch-opfordringen ("Christchurch Call to Action"). Kommissionsformand Jean-Claude Juncker støttede opfordringen og meddelte, at der ville blive udviklet en EU-kriseprotokol.

7 Se mere angående samarbejdet med byerne om sikkerhedsspørgsmål i afsnit V.2 om beredskab og beskyttelse, herunder navnlig beskyttelse af offentlige steder.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf.

9 Rammekontrakten er opdelt i to delkontrakter: 29 000 000 EUR i støtte til de kommende fire års aktiviteter i netværket til bevidstgørelse omkring radikalisering og 32 000 000 EUR til at styrke evnen hos medlemsstaterne, de nationale, regionale og lokale myndigheder og prioriterede tredjelande til effektivt at kunne håndtere radikalisering ved navnlig at tilbyde netværksmuligheder, målrettede og behovsbaserede tjenester samt forskning og analyser.

10 Forordning (EU) 2019/1157 af 20. juni 2019 om styrkelse af sikkerheden af unionsborgeres identitetskort og af opholdsdokumenter, der udstedes til unionsborgere og deres familiemedlemmer, som udøver deres ret til fri bevægelighed.

11 Indførelse af systematisk kontrol, der gennemføres ved de ydre grænser af alle borgere, der benytter sig af Schengeninformationssystemet. Alle Schengenstater samt Rumænien, Bulgarien, Kroatien og Cypern anvender de regler, som blev indført i april 2017, om systematisk kontrol i relevante databaser. I overensstemmelse med disse regler er det muligt at tillade midlertidige fravigelser ved land- og søgrænser,

lukke informationshuller[13] og styrke EU's retshåndhævende agentur Europol[14]. En vigtig del af denne indsats er **interoperabiliteten mellem EU's informationssystemer**[15], dvs. at man udnytter de eksisterende oplysninger optimalt og dækker blinde vinkler. Interoperabilitet opfylder behovene hos dem, der befinder sig i frontlinjen, ved at give retshåndhævelsespersonale, grænsevagter og migrationsmedarbejdere hurtigere og mere systematisk adgang til oplysninger, hvorved den bidrager til bedre grænseforvaltning og øget intern sikkerhed.

Interoperabilitet og den deraf medfølgende innovation vil imidlertid kun få betydning for sikkerheden og grænse- og migrationsforvaltningen, hvis hver enkelt medlemsstat gennemfører den tilknyttede lovgivning. Det er derfor på både politisk og teknisk plan en af sikkerhedsunionens øverste prioriteter at **sikre** interoperabilitet. Kommissionen og Det Europæiske Agentur for den Operationelle Forvaltning af Store IT-Systemer inden for Området med Frihed, Sikkerhed og Retfærdighed (eu-LISA) bistår medlemsstaterne med ekspertise og udveksling af bedste praksis gennem et netværk af nationale koordinatorer og gennem udvikling af en resultattavle til effektive overvågnings- og koordineringsordninger. Et tæt samarbejde mellem EU-agenturerne, alle medlemsstaterne og de associerede Schengenlande vil have afgørende betydning for realiseringen af det ambitiøse mål om at opnå fuld interoperabilitet mellem EU's informationssystemer for sikkerhed og grænse- og migrationsforvaltning fra 2020.

Samtidig mangler Europa-Parlamentet og Rådet stadig at **afslutte deres lovgivningsarbejde** på dette område. Hvis det skal sikres, at interoperabiliteten gennemføres fuldstændigt og rettidigt, er det vigtigt, at der snarest opnås enighed om alle de lovgivningsforslag, der endnu ikke er færdigbehandlede. For det første er det som led i den tekniske gennemførelse af **det europæiske system vedrørende rejseinformation og rejsetilladelse** nødvendigt med tekniske ændringer af de dertil knyttede forordninger[16] for at kunne indføre systemet fuldt ud. Kommissionen opfordrer Europa-Parlamentet til at fremskynde sit arbejde med disse tekniske ændringer med henblik på hurtigst muligt at kunne indlede de interinstitutionelle forhandlinger. For det andet pågår der stadig interinstitutionelle forhandlinger om forslaget fra maj 2018 om at styrke og opgradere det eksisterende **visuminformationssystem**[17]. På grundlag af det første trepartsmøde, der fandt sted den 22. oktober 2019, opfordrer Kommissionen Europa-Parlamentet og Rådet til hurtigt at afslutte forhandlingerne. For det tredje er der endnu ikke opnået enighed om Kommissionens forslag fra maj 2016 om at udvide **Eurodacs** anvendelsesområde[18], således at der ikke kun lagres fingeraftryk og relevante oplysninger i forbindelse med asylansøgere og personer, der pågribes i forbindelse med ulovlig passage af de ydre

---

men kun for EU-borgere, for at undgå en uforholdsmæssig stor indvirkning på trafikstrømmen. På nuværende tidspunkt har seks medlemsstater/associerede Schengenlande (Kroatien, Finland, Ungarn, Letland, Norge og Slovenien) givet meddelelse om sådanne fravigelser. Ved luftgrænser udløb muligheden for at fravige reglerne om systematisk kontrol i april 2019.

12 Det styrkede Schengeninformationssystem (forordning (EU) 2018/1860 af 28.11.2018, forordning (EU) 2018/1861 af 28.11.2018, forordning (EU) 2018/1862 af 28.11.2018) og udvidelsen af det europæiske informationssystem vedrørende strafferegistre til at omfatte tredjelandsstatsborgere (forordning (EU) 2019/816 af 17.4.2019). Styrkelsen af Schengeninformationssystemet omfatter en generel pligt til at foretage terrorrelaterede indberetninger i systemet.

13 EU's ind- og udrejsesystem (forordning (EU) 2017/2226 af 30.11.2017) og det europæiske system vedrørende rejseinformation og rejsetilladelse (forordning (EU) 2018/1240 af 12.9.2018 og forordning (EU) 2018/1241 af 12.9.2018).

14 Europols rolle er i både omfang og dybde blevet væsentligt styrket inden for de seneste år. Agenturet er blevet styrket med vedtagelsen af Europolforordningen i 2016 (forordning (EU) 2016/794 af 11.5.2016). Den mængde af oplysninger, som medlemsstaterne deler med og via Europol, er steget betydeligt. Oprettelsen af Europols Europæiske Center for Terrorbekæmpelse (ECTC) har styrket Europols analytiske kapacitet i sager om terrorisme. Europols budget er i de seneste år steget støt fra 82 mio. EUR i 2014 til 138 mio. EUR i 2019. Der forhandles fortsat om budgettet for 2020.

15 Forordning (EU) 2019/817 af 20. maj 2019 og forordning (EU) 2019/818 af 20. maj 2019.

16 Forordning (EU) 2018/1240 af 12.9.2018 og forordning (EU) 2018/1241 af 12.9.2018.

17 COM(2018) 302 final af 16.5.2018.

18 COM(2016) 272 final af 4.5.2016.

grænser, men også i forbindelse med tredjelandsstatsborgere med ulovligt ophold. De foreslåede ændringer vil også medføre en forlængelse af den periode, hvor man lagrer fingeraftryk og relevante oplysninger i forbindelse med personer, der rejser ind i EU på irregulær vis. Kommissionen opfordrer Europa-Parlamentet og Rådet til at vedtage forslaget.

For at styrke EU's informationssystemer for sikkerhed og grænse- og migrationsforvaltning opfordrer Kommissionen Europa-Parlamentet og Rådet til:

- at fremskynde deres arbejde med henblik på at nå til hurtig enighed om de foreslåede tekniske ændringer, der kræves at oprette **det europæiske system vedrørende rejseinformation og rejsetilladelse**
- hurtigst muligt at gennemføre og afslutte forhandlingerne vedrørende forslaget om en styrkelse af det eksisterende **visuminformationssystem**
- at vedtage lovgivningsforslaget om **Eurodac** *(prioritet i den fælles erklæring)*.

3. Begrænsning af terroristernes råderum

EU har truffet håndfaste foranstaltninger til begrænsning af terroristernes råderum gennem nye regler, der gør det vanskeligere for terrorister og andre kriminelle at få adgang til sprængstoffer[19], skydevåben og finansiering[20], og ved at begrænse deres bevægelighed[21].

Med henblik på at styrke den retlige indsats over for terrorisme oprettede EU's Agentur for Strafferetligt Samarbejde (Eurojust) den 1. september 2019 et **europæisk retligt terrorbekæmpelsesregister**. I registeret vil der blive indsamlet retlige oplysninger med det formål at påvise forbindelser i straffesager mod terrormistænkte personer og dermed styrke koordineringen blandt anklagerne i efterforskningsager om terrorisme med mulige grænseoverskridende virkninger.

Der skal imidlertid gøres en større indsats for at støtte og lette efterforskningen i grænseoverskridende sager, navnlig hvad angår de retshåndhævende myndigheders **adgang til elektronisk bevismateriale**. For så vidt angår lovgivningsforslagene fra april 2018 om at forbedre den grænseoverskridende adgang til elektronisk bevismateriale i strafferetlige efterforskninger[22] mangler Europa-Parlamentet stadig at vedtage sin forhandlingsposition, før det kan indlede forhandlinger med Rådet. Kommissionen opfordrer indtrængende Europa-Parlamentet til at fremskynde sit arbejde med dette lovgivningsforslag, således at Parlamentet og Rådet kan arbejde hen imod en hurtig vedtagelse. Kommissionen indleder på baggrund af sit forslag om EU-interne regler også **internationale forhandlinger** om at forbedre den grænseoverskridende adgang til elektronisk bevismateriale. Den 25. september 2019 indledte Kommissionen og de amerikanske myndigheder den første formelle forhandlingsrunde vedrørende **en aftale mellem EU og USA om grænseoverskridende adgang til elektronisk bevismateriale**. Den næste runde fandt ifølge planen sted den 6. november 2019. Som led i de igangværende forhandlinger om en **anden tillægsprotokol til Europarådets Budapestkonvention om IT-kriminalitet** deltog Kommissionen på Unionens vegne i tre forhandlingsmøder i hhv. juli, september og oktober 2019. Selv om der under disse forhandlinger blev gjort pæne fremskridt, mangler man endnu at behandle en række vigtige emner af væsentlig interesse for Unionen som f.eks. databeskyttelsesforanstaltninger. Forhandlingerne om en anden tillægsprotokol vil fortsætte i november 2019 og i løbet af hele 2020. Det er vigtigt at komme hurtigt videre med begge forhandlinger med henblik på at fremme det internationale samarbejde om udveksling af

[19] Forordning (EU) 2019/1148 af 20. juni 2019 om markedsføring og anvendelse af udgangsstoffer til eksplosivstoffer. Forordningen trådte i kraft den 31. juli 2019 og finder anvendelse 18 måneder efter ikrafttrædelsen.

[20] Direktiv (EU) 2019/1153 af 11. juli 2019 om regler, der letter brugen af finansielle og andre oplysninger med henblik på forebyggelse, afsløring, efterforskning eller retsforfølgning af visse strafbare handlinger.

[21] Indførelse af systematisk kontrol, der gennemføres ved de ydre grænser af alle borgere, der benytter sig af Schengeninformationssystemet.

[22] COM(2018) 225 final af 17.4.2018 og COM(2018) 226 final af 17.4.2018.

elektronisk bevismateriale, samtidig med at der sikres overensstemmelse med EU-retten og medlemsstaternes forpligtelser i den forbindelse og under hensyntagen til EU-rettens udviklingsperspektiver.

Som følge af vedvarende bekymringer angående hvidvask af penge har Europa-Parlamentet den 19. september 2019 vedtaget en **beslutning om status for gennemførelsen af Unionens lovgivning om bekæmpelse af hvidvaskning af penge**[23] som reaktion på den pakke med fire rapporter om bekæmpelse af hvidvask af penge, som Kommissionen vedtog den 24. juli 2019[24]. Europa-Parlamentet har opfordret medlemsstaterne til at sikre, at hvidvaskdirektiverne gennemføres hurtigst muligt og på behørig vis. Europa-Parlamentet har derudover opfordret Kommissionen til at vurdere, hvorvidt det vil være mere hensigtsmæssigt med en forordning end et direktiv, hvad angår bekæmpelse af hvidvask af penge, og til at vurdere behovet for en koordinerings- og støttemekanisme for finansielle efterretningsenheder.

For at forbedre de retshåndhævende myndigheders adgang til elektronisk bevismateriale opfordrer Kommissionen Europa-Parlamentet og Rådet til:
• hurtigt at nå til enighed om lovgivningsforslagene om **elektronisk bevismateriale** *(prioritet i den fælles erklæring).*

4. Forbedring af cybersikkerheden

Forbedring af cybersikkerheden er fortsat et centralt aspekt af arbejdet med at indføre en ægte og effektiv sikkerhedsunion. Unionen har med gennemførelsen af EU-strategien for cybersikkerhed fra 2017[25] øget både sin modstandsdygtighed, idet den har vanskeliggjort angreb udefra og gjort det lettere at komme sig over angreb, og den afskrækkende virkning, idet den har skabt bedre muligheder for at fange og straffe personerne bag et angreb, bl.a. via rammen for EU's fælles diplomatiske reaktion på ondsindede cyberaktiviteter. Unionen understøtter også medlemsstaternes cyberforsvar med gennemførelsen af rammen for EU's cyberforsvarspolitik.[26]

Med ikrafttrædelsen af forordningen om cybersikkerhed[27] i juni 2019 er en **EU-ramme for cybersikkerhedcertificering** ved at tage form. Certificering er et afgørende skridt for at øge tilliden til og sikkerheden ved produkter og tjenester, som er vigtige for det digitale indre marked. Certificeringsrammen vil danne grundlag for EU-dækkende certificeringsordninger i form af et sammenhængende sæt regler, tekniske krav, standarder og procedurer. Rammen omfatter to ekspertgrupper, nemlig Den Europæiske Cybersikkerhedscertificeringsgruppe, der repræsenterer medlemsstaternes myndigheder, og Cybersikkerhedscertificeringsgruppen for Interessenter, der repræsenterer branchen. Sidstnævnte samler både efterspørgsels- og udbudssiden inden for kommunikations- og informationsteknologiske produkter og tjenester, herunder små og mellemstore virksomheder, udbydere af digitale tjenester, europæiske og internationale standardiseringsorganer, nationale akkrediteringsorganer, databeskyttelsestilsynsmyndigheder og overensstemmelsesvurderingsorganer.

---

23 https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_DA.html.

24 Rapporten om vurdering af de risici for hvidvask af penge og finansiering af terrorisme, der påvirker det indre marked, og vedrørende grænseoverskridende aktiviteter (COM(2019) 370 af 24.7.2019), rapporten om sammenkobling af medlemsstaternes nationale centrale automatiske mekanismer (centrale registre eller centrale elektroniske systemer for dataudtræk) vedrørende bankkonti (COM(2019) 372 final af 24.7.2019), rapporten om vurdering af de seneste sager om hvidvask af penge, der involverer kreditinstitutter i EU (COM(2019) 373 final af 24.7.2019) samt rapporten om vurdering af samarbejdet mellem finansielle efterretningsenheder (COM(2019) 371 final af 24.7.2019).

25 JOIN(2017) 450 final af 13.9.2017.

26 Rammen for EU's cyberforsvarspolitik (2018-ajourføringen) som vedtaget af Rådet den 19. november 2018 (14413/18).

27 Forordning (EU) 2019/881 af 17.4.2019.

I mellemtiden er Europa-Parlamentet og Rådet endnu ikke nået til enighed om lovgivningsinitiativet[28] om oprettelse af **Det Europæiske Industri-, Teknologi- og Forskningscenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre**. Forslaget tager sigte på at styrke Unionens cybersikkerhedskapacitet ved at stimulere Europas teknologiske og industrielle økosystem inden for cybersikkerhed samt koordinere og sammenlægge de dertil knyttede ressourcer. Kommissionen opfordrer Europa-Parlamentet og Rådet til at genoptage og hurtigt afslutte de interinstitutionelle forhandlinger om dette prioriterede initiativ for at forbedre cybersikkerheden.

Indsatsen for bedre cybersikkerhed omfatter støtte på både nationalt og regionalt plan[29].

Ud over cybertrusler, der er rettet mod systemer og data, håndterer EU fortsat de komplekse og mangesidede udfordringer i forbindelse med **hybride trusler**. I Rådet er der blevet nedsat en horisontal gruppe vedrørende imødegåelse af hybride trusler for at gøre EU og medlemsstaterne mere modstandsdygtige over for hybride trusler og støtte indsatsen for at gøre samfund mere modstandsdygtige over for kriser. Kommissionen og EU-Udenrigstjenesten bakker op om dette arbejde inden for den fælles ramme for imødegåelse af hybride trusler[30] fra 2016 og den fælles meddelelse[31] om øget modstandsdygtighed og forbedrede kapaciteter til håndtering af hybride trusler fra 2018. Derudover er Det Fælles Forskningscenter ved at udarbejde en ramme for en "konceptuel model" til at karakterisere hybride trusler, således at medlemsstaterne og deres kompetente myndigheder bedre kan identificere, hvilken type hybridangreb de kan blive udsat for. I modellen undersøges det, hvordan en (statslig eller ikkestatslig) aktør anvender en række værktøjer (fra desinformation til spionage eller fysiske operationer) inden for forskellige områder (det økonomiske, militære, sociale eller politiske) med henblik på at angribe et mål for at opnå en række ting.

For at styrke cybersikkerheden opfordrer Kommissionen Europa-Parlamentet og Rådet til:
• hurtigt at nå til enighed om lovgivningsforslaget om **Det Europæiske Industri-, Teknologi- og Forskningscenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre**.

III. FORBEDRING AF SIKKERHEDEN I DEN DIGITALE INFRASTRUKTUR

Femtegenerationsnet (5G) vil udgøre den fremtidige rygrad i vores stadig mere digitaliserede økonomi og samfund. Der er tale om milliarder af objekter og systemer, herunder i vigtige sektorer som energi, transport, bank- og sundhedsvæsen, samt industrielle kontrolsystemer, der indeholder følsomme oplysninger, og som understøtter sikkerhedssystemer. Det er derfor vigtigt at sikre, at 5G-nettet er cybersikkert og robust.

Som led i en koordineret tilgang fremlagde medlemsstaterne den 9. oktober 2019 en rapport om **EU's koordinerede risikovurdering af cybersikkerheden i 5G-net** med støtte fra Kommissionen og Det Europæiske Agentur for Cybersikkerhed[32]. Dette vigtige skridt er et led i gennemførelsen af Kommissionens henstilling fra marts 2019 med henblik på at sikre et højt cybersikkerhedsniveau for 5G-net i hele EU[33]. Rapporten er baseret på resultaterne af de nationale

[28] COM(2018) 630 final af 12.9.2018.

[29] Kommissionen støtter bl.a. et interregionalt innovationspartnerskab om cybersikkerhed, der omfatter Bretagne, Castilla y León, Nordrhein-Westfalen, det centrale Finland og Estland, med det formål at udvikle en europæisk cybersikkerhedsværdikæde med fokus på kommercialisering og opskalering.

[30] JOIN(2016)18 final af 6.4.2016.

[31] JOIN(2018) 16 final af 13.6.2018.

[32] EU's koordinerede risikovurdering af cybersikkerheden i 5G-net blev færdiggjort af samarbejdsgruppen af kompetente myndigheder som fastsat i direktivet om sikkerhed i net- og informationssystemer (direktiv (EU) 2016/1148 af 6.7.2016) med støtte fra Kommissionen og Det Europæiske Agentur for Cybersikkerhed: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019) 2355 final af 26.3.2019.

cybersikkerhedsrisikovurderinger i alle medlemsstaterne. Den kortlægger de vigtigste trusler og trusselsaktører, de mest følsomme aktiver, de primære sårbarheder (herunder tekniske og andre typer sårbarheder) og en række strategiske risici. Ud fra denne vurdering fastlægges der afbødende foranstaltninger, som kan anvendes på nationalt og europæisk plan.

Rapporten peger på en række vigtige **cybersikkerhedsmæssige udfordringer**, som sandsynligvis vil opstå eller blive mere fremtrædende i 5G-net. Disse sikkerhedsmæssige udfordringer er hovedsagelig knyttet til centrale *nyskabelser* inden for 5G-teknologien, navnlig den vigtige software og det store udbud af tjenester og applikationer, der muliggøres af 5G, samt *leverandørernes* rolle i forbindelse med opbygning og drift af 5G-net og graden af afhængighed af de enkelte leverandører. Det betyder, at leverandørernes produkter, tjenester og aktiviteter i stigende grad indgår i 5G-nettets "angrebsflade". Desuden vil den enkelte leverandørs risikoprofil få særlig stor betydning, herunder sandsynligheden for, at leverandøren udsættes for indgriben fra et tredjeland.

I overensstemmelse med den proces, der er fastsat i Kommissionens henstilling fra marts 2019 bør medlemsstaterne senest den 31. december 2019 nå til enighed om en **værktøjskasse med afbødningsforanstaltninger** til at håndtere de udpegede cybersikkerhedsrisici på nationalt og EU-plan. Kommissionen og EU-Udenrigstjenesten vil også fortsætte deres udveksling af oplysninger med ligesindede partnere vedrørende 5G-nettets cybersikkerhed og modstandsdygtighed. Kommissionen er i den henseende i kontakt med NATO vedrørende EU's koordinerede risikovurdering af cybersikkerheden i 5G-net.

IV. BEKÆMPELSE AF DESINFORMATION OG BESKYTTELSE AF VALG MOD ANDRE CYBERBASEREDE TRUSLER

EU har opstillet en **ramme for en koordineret indsats for bekæmpelse af desinformation** i fuld overensstemmelse med de europæiske værdier og grundlæggende rettigheder[34]. Inden for rammerne af handlingsplanen for bekæmpelse af desinformation[35] arbejdes der fortsat på at indskrænke mulighederne for at sprede desinformation, herunder med henblik på at værne om valgintegriteten.

En vigtig del af denne indsats er samarbejdet med erhvervslivet gennem den selvregulerende **EU-kodeks om desinformation** for onlineplatforme og reklamebranchen, som trådte i kraft i oktober 2018[36]. Et år efter kodeksens ikrafttrædelse har Kommissionen vurderet dens effektivitet på grundlag af de årlige selvevalueringsrapporter, som onlineplatformene og de andre underskrivere af kodeksen har indsendt og offentliggjort den 29. oktober 2019 sammen med en erklæring fra Kommissionen[37]. Overordnet set fremgår det af rapporterne, at underskriverne gør en stor indsats for at indfri deres løfter.

Der er forskel på, hvor hurtigt og hvor omfattende de underskrivende platforme har truffet foranstaltninger på tværs af kodeksens fem tilsagnsområder. Generelt sker der størst fremskridt vedrørende de løfter, der blev afgivet i forbindelse med valget til Europa-Parlamentet i 2019, nemlig med hensyn til at modvirke reklamer og økonomiske incitamenter til desinformation (område 1), sikre gennemsigtighed i forbindelse med politisk og emnebaseret reklame (område 2) og sikre tjenesteydelsernes integritet imod falske konti og uautentisk adfærd (område 3). I modsætning hertil ses der mindre eller ingen fremskridt, hvad angår løfterne om at forbedre forbrugernes stilling (område 4) og forskersamfundets stilling, herunder at platformene giver adgang til datasæt med henblik på forskning, hvis det er relevant og under hensyntagen til beskyttelse af personoplysninger (område 5). Desuden varierer omfanget af de foranstaltninger, som de enkelte platforme har truffet for at opfylde deres løfter, og der er ligeledes forskel på medlemsstaternes gennemførelse af de enkelte politikker. Kommissionen fortsætter samarbejdet med underskriverne af kodeksen samt andre interessenter om at intensivere indsatsen mod desinformation.

Inden for rammerne af handlingsplanen for bekæmpelse af desinformation har Kommissionen og den højtstående repræsentant i samarbejde med medlemsstaterne etableret et **hurtigt varslingssystem** til imødegåelse af desinformationskampagner. Takket være det hurtige varslingssystem var EU-institutionerne og medlemsstaterne i stand til at koordinere deres indsats og udveksle oplysninger og analyser forud for valget til Europa-Parlamentet i 2019. Denne indsats blev intensiveret yderligere efter valget med løbende daglige arbejdsudvekslinger og tre møder, som blev afholdt af forskellige medlemsstater, for det hurtige varslingssystems kontaktpunkter.

Med de **strategiske kommunikationshold** ("StratCom"-hold), herunder navnlig East StratCom-taskforcen, som har stået for projektet "EUvsDisinfo" med det formål at overvåge, analysere og reagere på ruslandvenlig desinformation, er der taget endnu et praktisk skridt i retning af at identificere

---

34 Jf. handlingsplanen for bekæmpelse af desinformation (JOIN(2018) 36 final af 5.12.2018).

35 JOIN(2019) 12 final af 14.6.2019.

36 I forbindelse med kodeksen har onlineplatformene Google, Facebook, Twitter og Microsoft forpligtet sig til at forebygge, at platformenes tjenester bliver brugt til manipulation af ondsindede aktører, garantere gennemsigtighed i og offentliggørelse af politiske reklamer samt træffe yderligere foranstaltninger for at sikre øget gennemsigtighed, ansvarlighed og troværdighed i onlineøkosystemet. Brancheorganisationer fra reklamebranchen har ligeledes forpligtet sig til at samarbejde med platformene om at forbedre deres granskning af reklamers placering og udvikle varemærkesikkerhedsværktøjer, der skal begrænse placering af reklamer på websteder, der sprede desinformation.

37 https://ec.europa.eu/commission/presscorner/detail/da/statement_19_6166. Ud over Google, Facebook, Twitter og Microsoft omfatter de øvrige underskrivere af kodeksen Mozilla, syv EU-dækkende eller nationale organisationer, der repræsenterer reklamebranchen, samt EDiMA, en europæisk organisation, der repræsenterer platforme og andre teknologivirksomheder, der er aktive inden for onlinesektoren.

desinformation[38]. Siden begyndelsen af 2019 har det første øremærkede budget på 3 mio. EUR gjort det muligt at intensivere og udvide denne indsats til at omfatte overvågning og analyse af ruslandvenlig desinformation, der spredes på webmedier, i radio og TV og på sociale medier, på 19 forskellige sprog lige fra engelsk til serbisk og arabisk. Mængden af afdækkede desinformationsaktiviteter steg til mere end det dobbelte takket være en forbedret overvågningskapacitet, idet der indtil videre i 2019 har været 2000 sager om desinformation sammenlignet med 765 sager i samme periode i 2018. East StratCom-taskforcen spillede en afgørende rolle med hensyn til at overvåge og afdække ruslandvenlig desinformation rettet mod valget til Europa-Parlamentet i 2019. Efterforskningen blev suppleret af en oplysningskampagne vedrørende forsøg på indblanding i valgprocesser rundt om i verden. Oplysningsaktiviteterne, som foregik i tæt samarbejde med Europa-Parlamentet og Kommissionen, resulterede i over 20 medieinterviews, og flere end 300 journalister deltog i kampagnen.

Kommissionen har også gjort en indsats for at **begrænse spredningen af desinformation og myter om EU's institutioner og politikker**. Den har oprettet et netværk af kommunikationseksperter, der via en onlineportal tilbyder interaktivt informationsmateriale om EU-politikker og om udfordringen med desinformation og dens indvirkning på samfundet. Den har derudover på de sociale medier iværksat en række kampagner med fokus på bekæmpelse af desinformation[39] i samarbejde med Europa-Parlamentet og EU-Udenrigstjenesten.

V. GENNEMFØRELSE AF ANDRE PRIORITEREDE SIKKERHEDSFORANSTALTNINGER

1. Gennemførelse af lovgivningsmæssige foranstaltninger i sikkerhedsunionen

Forudsætningen for at drage fuld fordel af de vedtagne foranstaltninger i sikkerhedsunionen er, at alle medlemsstater sikrer en hurtig og fuldstændig gennemførelse af dem. I den henseende støtter Kommissionen aktivt medlemsstaterne i at gennemføre EU-lovgivningen, bl.a. gennem finansiering og ved at fremme udveksling af bedste praksis. Kommissionen vil gøre fuld brug af sine traktatmæssige beføjelser til at håndhæve EU-lovgivningen, herunder eventuelt indlede traktatbrudssager.

Fristen for gennemførelse af **EU-direktivet om passagerlisteoplysninger**[40] udløb den 25. maj 2018. 25 medlemsstater har på nuværende tidspunkt givet meddelelse om fuldstændig gennemførelse[41], hvilket er et betydeligt fremskridt siden juli 2018, hvor Kommissionen indledte traktatbrudssager mod 14 medlemsstater[42]. 2 medlemsstater har endnu ikke meddelt fuldstændig gennemførelse på trods af verserende traktatbrudssager, der blev indledt den 19. juli 2018[43]. Sideløbende hermed bistår Kommissionen fortsat alle medlemsstaterne i arbejdet med at færdigudvikle deres systemer vedrørende passagerlisteoplysninger, bl.a. ved at fremme udveksling af information og bedste praksis.

Fristen for gennemførelse af **direktivet om bekæmpelse af terrorisme**[44] udløb den 8. september 2018. På nuværende tidspunkt har 22 medlemsstater givet meddelelse om fuldstændig gennemførelse, hvilket er et betydeligt fremskridt siden november 2018, hvor Kommissionen indledte

---

38 www.euvsdisinfo.eu.

39 https://europa.eu/euprotects/content/homepage_da.

40 Direktiv (EU) 2016/681 af 27. april 2016. Danmark deltog ikke i vedtagelsen af dette direktiv, som ikke er bindende for og ikke finder anvendelse i Danmark.

41 Henvisningerne til meddelelsen om fuldstændig gennemførelse tager højde for medlemsstaternes erklæringer og berører ikke Kommissionens tjenestegrenes gennemførelseskontrol (status pr. 17.10.2019).

42 Jf. den sekstende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2018) 690 final af 10.10.2018).

43 Slovenien har givet meddelelse om delvis gennemførelse. Spanien har ikke givet meddelelse om gennemførelse (status pr. 17.10.2019).

44 Direktiv (EU) 2017/541 af 15. marts 2017. Direktivet finder ikke anvendelse i Det Forenede Kongerige, Irland og Danmark.

traktatbrudssager mod 16 medlemsstater[45]. 3 medlemsstater har endnu ikke meddelt fuldstændig gennemførelse på trods af verserende traktatbrudssager[46]. Den 25. juli 2019 sendte Kommissionen begrundede udtalelser til 2 medlemsstater for manglende meddelelse om fuldstændig gennemførelse af direktivet[47]. Begge medlemsstater svarede, at lovgivningsarbejdet vil blive afsluttet inden årets udgang.

Fristen for gennemførelse af **direktivet om erhvervelse og besiddelse af våben**[48] udløb den 14. september 2018. På nuværende tidspunkt har 13 medlemsstater givet meddelelse om fuldstændig gennemførelse. 15 medlemsstater har endnu ikke meddelt fuldstændig gennemførelse på trods af verserende traktatbrudssager, der blev indledt den 22. november 2018[49]. Den 25. juli 2019 sendte Kommissionen begrundede udtalelser til 20 medlemsstater for manglende meddelelse om fuldstændig gennemførelse af direktivet. Som følge heraf har 5 medlemsstater givet meddelelse om fuldstændig gennemførelse af direktivet[50].

Fristen for gennemførelse af **direktivet om databeskyttelse på retshåndhævelsesområdet**[51] udløb den 6. maj 2018. På nuværende tidspunkt har 25 medlemsstater givet meddelelse om fuldstændig gennemførelse, hvilket er et betydeligt fremskridt siden juli 2018, hvor Kommissionen indledte traktatbrudssager mod 19 medlemsstater[52]. 3 medlemsstater har endnu ikke meddelt fuldstændig gennemførelse på trods af verserende traktatbrudssager[53]. Den 25. juli 2019 besluttede Kommissionen at indbringe 2 medlemsstater[54] for Den Europæiske Unions Domstol for manglende gennemførelse af direktivet og sendte en åbningsskrivelse til 1 medlemsstat[55] for manglende fuldstændig gennemførelse af direktivet[56].

Kommissionen er ved at vurdere gennemførelsen af det **fjerde direktiv om bekæmpelse af hvidvask af penge**[57] og arbejder samtidig på at kontrollere, om medlemsstaterne gennemfører reglerne. De skulle have gennemført direktivet i deres nationale lovgivning senest den 26. juni 2018. Kommissionen opretholder traktatbrudsprocedurer mod 21 medlemsstater, da den vurderer, at de meddelelser, den har modtaget fra medlemsstaterne, ikke udgør en fuldstændig gennemførelse af dette direktiv[58].

---

45 Jf. den syttende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2018) 845 final af 11.12.2018).

46 Grækenland og Luxembourg har ikke anmeldt nogen nationale gennemførelsesforanstaltninger. Polen har anmeldt nationale foranstaltninger, der svarer til en delvis gennemførelse (status pr. 17.10.2019).

47 Grækenland og Luxembourg.

48 Direktiv (EU) 2017/853 af 17. oktober 2019.

49 Belgien, Det Forenede Kongerige, Estland, Tjekkiet, Polen, Slovakiet og Sverige har anmeldt gennemførelsesforanstaltninger for en del af de nye bestemmelser. Cypern, Grækenland, Luxembourg, Rumænien, Slovenien, Spanien, Tyskland og Ungarn har ikke anmeldt nogen gennemførelsesforanstaltninger (status pr. 17.10.2019).

50 Finland, Irland, Litauen, Nederlandene og Portugal (status pr. 17.10.2019).

51 Direktiv (EU) 2016/680 af 27. april 2016.

52 Jf. den sekstende statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2018) 690 final af 10.10.2018).

53 Slovenien har givet meddelelse om delvis gennemførelse. Spanien har ikke givet meddelelse om gennemførelse. Selv om Tyskland har givet meddelelse om fuldstændig gennemførelse, anser Kommissionen ikke denne gennemførelse for at være fuldstændig (status pr. 17.10.2019).

54 Grækenland og Spanien.

55 Tyskland.

56 Grækenland har givet meddelelse om fuldstændig gennemførelse, hvilket Kommissionen er i færd med at vurdere.

57 Direktiv (EU) 2015/849 af 20. maj 2015.

58 Belgien, Bulgarien, Cypern, Danmark, Det Forenede Kongerige, Estland, Finland, Frankrig, Irland, Italien, Letland, Litauen, Nederlandene, Polen, Rumænien, Slovakiet, Sverige, Tjekkiet, Tyskland, Ungarn og Østrig (status pr. 17.10.2019). Syv traktatbrudssager vedrørende direktivet er tidligere blevet afsluttet.

Kommissionen har vurderet, hvorvidt gennemførelsen er i overensstemmelse med **direktiverne vedrørende cyberkriminalitet**. Kommissionen har i juli og oktober 2019 indledt traktatbrudssager mod 23 medlemsstater[59], idet den ikke anser den nationale gennemførelseslovgivning, som blev meddelt af disse medlemsstater, for at være en korrekt gennemførelse af **direktivet om bekæmpelse af seksuelt misbrug af børn**[60]. Ligeledes har Kommissionen i juli og oktober 2019 indledt traktatbrudssager mod fire medlemsstater[61], idet den ikke anser den nationale gennemførelseslovgivning, som blev meddelt af disse medlemsstater, for at være en korrekt gennemførelse af **direktivet om angreb på informationssystemer**[62].

Kommissionen opfordrer medlemsstaterne til hurtigst muligt at træffe de nødvendige foranstaltninger til fuldt ud at gennemføre følgende direktiver i den nationale lovgivning og anmelde dem til Kommissionen:

- **EU-direktivet om passagerlisteoplysninger**, hvor 1 medlemsstat endnu ikke har givet meddelelse om gennemførelse i national ret, og hvor 1 medlemsstat mangler at give endelig meddelelse om gennemførelse[63]
- **direktivet om bekæmpelse af terrorisme**, hvor 2 medlemsstater stadig mangler at give meddelelse om gennemførelse i national ret, og hvor 1 medlemsstat stadig mangler at give endelig meddelelse om gennemførelse[64]
- **direktivet om erhvervelse og besiddelse af våben**, hvor 8 medlemsstater stadig ikke har givet meddelelse om gennemførelse i national ret, og hvor 7 medlemsstater mangler at give endelig meddelelse om gennemførelse[65]
- **direktivet om databeskyttelse på retshåndhævelsesområdet**, hvor 1 medlemsstat stadig mangler at give meddelelse om gennemførelse i national ret, og hvor 2 medlemsstater mangler at give endelig meddelelse om gennemførelse[66]
- **det fjerde direktiv om bekæmpelse af hvidvask af penge**, hvor 21 medlemsstater stadig mangler at give endelig meddelelse om gennemførelse[67]
- **direktivet om bekæmpelse af seksuelt misbrug af børn**, hvor der er indledt traktatbrudssager for ukorrekt gennemførelse over for 23 medlemsstater[68]
- **direktivet om angreb på informationssystemer**, hvor der er indledt traktatbrudssager for ukorrekt gennemførelse over for 4 medlemsstater[69].

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

60 Direktiv 2011/93/EU af 13. december 2011.

61 Bulgarien, Italien, Portugal og Slovenien.

62 Direktiv 2013/40/EU af 12. august 2013.

63 Slovenien har givet meddelelse om delvis gennemførelse. Spanien har ikke givet meddelelse om gennemførelse (status pr. 17.10.2019).

64 Grækenland og Luxembourg har ikke givet meddelelse om gennemførelse. Polen har givet meddelelse om delvis gennemførelse (status pr. 17.10.2019).

65 Belgien, Det Forenede Kongerige, Estland, Tjekkiet, Polen, Slovakiet og Sverige har anmeldt gennemførelsesforanstaltninger for en del af de nye bestemmelser. Cypern, Grækenland, Luxembourg, Rumænien, Slovenien, Spanien, Tyskland og Ungarn har ikke anmeldt nogen gennemførelsesforanstaltninger (status pr. 17.10.2019).

66 Slovenien har givet meddelelse om delvis gennemførelse. Spanien har ikke givet meddelelse om gennemførelse. Selv om Tyskland har givet meddelelse om fuldstændig gennemførelse, anser Kommissionen ikke denne gennemførelse for at være fuldstændig (status pr. 17.10.2019).

67 Belgien, Bulgarien, Cypern, Danmark, Det Forenede Kongerige, Estland, Finland, Frankrig, Irland, Italien, Letland, Litauen, Nederlandene, Polen, Rumænien, Slovakiet, Sverige, Tjekkiet, Tyskland, Ungarn og Østrig (status pr. 17.10.2019).

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

69 Bulgarien, Italien, Portugal og Slovenien.

2. Beredskab og beskyttelse

Et vigtigt aspekt af arbejdet med at sikre en effektiv og ægte sikkerhedsunion er opbygning af modstandsdygtighed over for sikkerhedstrusler. Kommissionen hjælper medlemsstaterne og deres lokale myndigheder med at forbedre beskyttelsen af offentlige steder ved at gennemføre handlingsplanen fra oktober 2017 og partnerskabet for sikkerhed i det offentlige rum fra januar 2019 som led i EU's dagsorden for byerne. Dette omfatter de byer, som henvendt sig til Kommissionen og anmodet om støtte til at håndtere de udfordringer, de stod over for med hensyn til at beskytte det offentlige rum.

Udveksling af bedste praksis mellem lokale myndigheder og private aktører har afgørende betydning for øget sikkerhed i det offentlige rum. Dette tema var i centrum for den **europæiske sikkerhedsuge**, som blev afholdt den 14.-18. oktober 2019 af det EU-finansierede projekt "Protect Allied Cities against Terrorism in Securing Urban Areas" (PACTESUR) i den franske by Nice. Begivenheden samlede 500 deltagere fra byer i hele Europa, nationale myndigheder og forskningsinstitutioner og understregede vigtigheden af et tæt samarbejde mellem alle berørte parter, både offentlige og private, og de nye teknologiers betydning for en bedre beskyttelse af byerne. Beskyttelsen af det offentlige rum stod også på dagsordenen for den **europæiske uge for regioner og byer**, som blev afholdt i Bruxelles den 7.-10. oktober 2019, med en workshop om partnerskabet for sikkerhed i det offentlige rum som led i EU's dagsorden for byerne. Ugen havde fokus på de lokale myndigheders rolle inden for det sikkerhedspolitiske område, de store sikkerhedsmæssige udfordringer, som man i EU-lovgivningen og –finansieringen står over for med hensyn til det offentlige byrum, samt vigtige temaer som innovation ved hjælp af intelligente løsninger og teknologier, herunder begrebet indbygget sikkerhed, forebyggelse og social inklusion. Kommissionen er også med til at fremme bymæssig innovation på disse områder gennem sin seneste indkaldelse af projektforslag under initiativet for nyskabende foranstaltninger i byerne, hvoraf resultatet blev offentliggjort i august 2019. Blandt de udvalgte projekter vil tre byer (Piræus i Grækenland, Tammerfors i Finland og Torino i Italien) afprøve nye løsninger vedrørende sikkerhedsspørgsmål i byområder[70].

Med henblik på at forbedre **beskyttelsen af religiøse samlingssteder** og udforske behovet hos de forskellige religiøse grupper arrangerede Kommissionen et møde den 7. oktober 2019 med repræsentanter for de jødiske, muslimske, kristne og buddhistiske samfund. Som led i gennemførelsen af EU-handlingsplanen til støtte for beskyttelsen af offentlige steder fra 2017 viste mødet, at sikkerhedsbevidstheden og -beredskabet i de forskellige religiøse samfund varierer betydeligt, hvilket understreger, hvor vigtigt det er at fortsætte udvekslingen af god praksis. Mødet gjorde det også klart, at det er muligt at indføre grundlæggende sikkerhedsforanstaltninger og en øget sikkerhedsbevidsthed uden at gøre de religiøse samlingssteder mindre åbne eller mindre tilgængelige. Kommissionen vil indsamle eksempler på god praksis samt oplysningsmateriale på sin elektroniske ekspertplatform og forelægge det indsamlede materiale for medlemsstaternes sikkerhedsmyndigheder i det offentlig-private forum for beskyttelse af offentlige steder.

Et område, der kræver yderligere opmærksomhed, er den voksende trussel, som **droner** udgør for sikkerheden i kritisk infrastruktur og i det offentlige rum. Som et supplement til den seneste EU-lovgivning[71] om sikre droneoperationer inden for bemandet luftfart og uden at undergrave mulighederne for gavnlig brug af droner støtter Kommissionen medlemsstaterne i at spore tendenser inden for ondsindet brug af droner ved at finansiere relevant forskning og gøre det lettere at afprøve modforanstaltninger. Det er af afgørende betydning at udveksle erfaringer og bedste praksis, som det fremgår af den internationale konference på højt niveau om at imødegå risiciene forbundet med ubemandede luftfartøjssystemer, som blev afholdt i Bruxelles den 17. oktober 2019. Begivenheden,

[70] Initiativet for nyskabende foranstaltninger i byerne er delvis finansieret af Den Europæiske Fond for Regionaludvikling. Læs mere på: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

[71] Kommissionens gennemførelsesforordning (EU) 2019/947 af 24. maj 2019 om regler og procedurer for operation af ubemandede luftfartøjer

som var arrangeret af Kommissionen, samlede 250 deltagere fra medlemsstaterne, internationale organisationer, tredjelande, erhvervslivet, den akademiske verden og civilsamfundet til en drøftelse af de sikkerhedsmæssige udfordringer, som droner udgør, og mulige løsninger på problemet. Mødet viste, at der er behov for regelmæssige risikovurderinger vedrørende droner og for et tæt samarbejde mellem luftfartsmyndighederne og de retshåndhævende myndigheder om at videreudvikle EU-lovgivningen om sikre droneoperationer. Der er også behov for yderligere afprøvning af modforanstaltninger mod droner gennem en koordineret europæisk tilgang. Derudover var man enige om vigtigheden af, at myndighederne og erhvervslivet arbejder tæt sammen om at udvikle droner, der er sikre, operationelt pålidelige og vanskelige at misbruge til ondsindede formål.

3. Den eksterne dimension

Eftersom de fleste af de sikkerhedsrisici, som Unionen står over for, er globale trusler, som rækker ud over EU's grænser, spiller samarbejdet med partnerlande, organisationer og relevante interessenter en afgørende rolle for indførelsen af en effektiv og ægte sikkerhedsunion.

Dette samarbejde bygger i høj grad på udvekslingen af oplysninger. Sideløbende med denne rapport har Kommissionen vedtaget en henstilling til Rådet om bemyndigelse til at indlede forhandlinger om en **aftale mellem EU og New Zealand om udveksling af personoplysninger for at bekæmpe grov kriminalitet og terrorisme**. Udvekslingen skal ske mellem Europol og de newzealandske kompetente myndigheder. En sådan aftale vil yderligere styrke Europols kapacitet til at samarbejde med New Zealand for at forebygge og bekæmpe kriminelle handlinger, der falder inden for rammerne af Europols målsætninger. Selv om samarbejdsordningen mellem Europol og det newzealandske politi fra april 2019 udstikker en ramme for et struktureret strategisk samarbejde, indeholder den ikke et retsgrundlag for udveksling af personoplysninger. Det er afgørende for et effektivt operationelt politisamarbejde, at udvekslingen af personoplysninger sker under fuld overholdelse af EU-retten og de grundlæggende rettigheder. Kommissionen har tidligere på grundlag af terrortruslen, migrationsrelaterede udfordringer og Europols operationelle behov identificeret otte prioriterede lande, som der bør indledes forhandlinger med i regionen Mellemøsten/Nordafrika[72]. Under hensyntagen til de operationelle behov hos de retshåndhævende myndigheder i hele EU og de potentielle fordele ved et tættere samarbejde på dette område, som også fremgik af opfølgningen på angrebet i Christchurch i marts 2019, finder Kommissionen det nødvendigt at tilføje New Zealand som et prioriteret land at indlede forhandlinger med på kort sigt.

Et andet vigtigt element i Unionens sikkerhedssamarbejde med tredjelandspartnere er overførslen af **passagerlisteoplysninger**. Den 27. september 2019 vedtog Kommissionen en henstilling til Rådet om bemyndigelse til at indlede forhandlinger om en aftale mellem **EU og Japan** om overførsel af passagerlisteoplysninger for at forhindre og bekæmpe terrorisme og grov kriminalitet af grænseoverskridende karakter under fuld overholdelse af databeskyttelsesreglerne og de grundlæggende rettigheder[73]. Rådets arbejdsgrupper er nu ved at undersøge henstillingen, og Kommissionen opfordrer Rådet til hurtigt at vedtage mandatet til at føre forhandlinger med Japan. Der vil være en konkret sikkerhedsmæssig fordel ved at få aftalen på plads inden De Olympiske Lege i 2020.

På verdensplan bakker Kommissionen op om det arbejde, som **Organisationen for International Civil Luftfart** gør for at indføre en standard for behandlingen af passagerlisteoplysninger. Hermed imødekommer Kommissionen FN's Sikkerhedsråds resolution 2396, der opfordrer alle FN's medlemsstater til at opbygge kapaciteten til at indsamle, behandle og analysere

[72] Jf. den ellevte statusrapport om indførelsen af en effektiv og ægte sikkerhedsunion (COM(2017) 608 final af 18.10.2017). De prioriterede lande er Algeriet, Egypten, Israel, Jordan, Libanon, Marokko, Tunesien og Tyrkiet.

[73] COM(2019) 420 final af 27.9.2019.

passagerlisteoplysninger. Den 13. september 2019 fremlagde Kommissionen et forslag[74] til Rådets afgørelse om den holdning, der skal indtages på EU's vegne i Rådet for Organisationen for International Civil Luftfart for så vidt angår standarder og anbefalinger vedrørende passagerlisteoplysninger. Rådets arbejdsgrupper er nu ved at undersøge forslaget, og Kommissionen opfordrer til hurtig vedtagelse af Rådets afgørelse. Unionens og medlemsstaternes holdning er også blevet fastlagt i et orienterende dokument om "standarder og principper for indsamling, anvendelse, behandling og beskyttelse af passagerlisteoplysninger", der blev fremlagt på det 40. møde i forsamlingen i Organisationen for International Civil Luftfart.

Når det gælder arbejdet med at indgå en ny passagerlisteaftale med **Canada** bestræber Kommissionen sig på hurtigt at kunne indgå en sådan aftale. I mellemtiden er der denne sommer blevet iværksat en fælles gennemgang og fælles evaluering af passagerlisteaftalen med **Australien** og en fælles evaluering af passagerlisteaftalen med **USA** med indledende besøg i Canberra og Washington i hhv. august og september 2019. Kommissionen informerede på et lukket møde den 14. oktober 2019 Europa-Parlamentets Udvalg om Borgernes Rettigheder og Retlige og Indre Anliggender om status for arbejdet med passagerlisteaftalerne med Japan, Australien og Canada.

Det går også fremad med sikkerhedssamarbejdet med partnerlandene på **Vestbalkan** med gennemførelsen af den fælles handlingsplan om terrorbekæmpelse for Vestbalkan fra oktober 2018. Den 9. oktober underskrev Kommissionen to ikkebindende bilaterale antiterrorordninger med Albanien og Republikken Nordmakedonien[75]. Ordningerne fastsætter individuelt tilrettelagte prioriterede foranstaltninger, som skal træffes af myndighederne i de respektive lande. Foranstaltningerne omfatter den fælles handlingsplans fem mål[76] og indikerer, hvilken støtte Kommissionen har til hensigt at yde. Det forventes, at der i de kommende uger vil blive underskrevet lignende ordninger med de øvrige partnerlande på Vestbalkan. Derudover underskrev Kommissionen den 7. oktober 2019 en aftale med Montenegro om samarbejde om grænseforvaltning mellem Montenegro og Det Europæiske Agentur for Grænse- og Kystbevogtning (Frontex). Aftalen gør agenturet i stand til at bistå Montenegro med grænseforvaltningen i et forsøg på at bekæmpe irregulær migration og grænseoverskridende kriminalitet og dermed øge sikkerheden ved EU's ydre grænser.

For at styrke samarbejdet med partnerlandene om bekæmpelsen af fælles sikkerhedstrusler opfordrer Kommissionen Rådet til:

- at vedtage bemyndigelsen til at indlede forhandlinger om en aftale mellem EU og **New Zealand** om udveksling af personoplysninger for at bekæmpe grov kriminalitet og terrorisme
- at vedtage bemyndigelsen til at indlede forhandlinger om en aftale mellem EU og **Japan** om overførsel af passagerlisteoplysninger
- at vedtage forslaget til **Rådets afgørelse om den holdning, der skal indtages på EU's vegne i Rådet for Organisationen for International Civil Luftfart** for så vidt angår standarder og anbefalinger vedrørende passagerlisteoplysninger.

VI. KONKLUSION

Denne rapport beskriver den lange række foranstaltninger, som EU har truffet for at imødegå fælles trusler i Europa og styrke vores fælles sikkerhed. Drevet af en fælles forståelse for, at de sikkerhedsmæssige udfordringer, vi står over for i dag, håndteres bedst ved at arbejde sammen indbyrdes og med tredjelande, er de fremskridt, vi har gjort med at indføre en effektiv og ægte

[74] COM(2019) 416 final af 13.9.2019.

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en.

[76] Den fælles handlingsplan omfatter foranstaltninger vedrørende følgende fem mål: en robust ramme for terrorbekæmpelse, effektiv forebyggelse og bekæmpelse af voldelig ekstremisme, effektiv informationsudveksling og effektivt operationelt samarbejde, opbygning af kapacitet til bekæmpelse af hvidvask af penge og finansiering af terrorisme samt bedre beskyttelse af borgere og infrastruktur.

sikkerhedsunion, resultatet af et tæt samarbejde mellem en lang række aktører baseret på tillid, ressourcedeling og fælles håndtering af trusler: Samarbejdet er sket på alle forvaltningsniveauer, fra byer og andre lokale aktører samt regioner og nationale myndigheder til Europa-Parlamentet og Rådet på EU-plan. Det er foregået med inddragelse af offentlige myndigheder, EU-agenturer, private aktører og civilsamfundet og ved hjælp af ekspertise, værktøjer og ressourcer på tværs af politikområder såsom transportpolitik, det digitale indre marked eller samhørighedspolitikken. På den måde er arbejdet i sikkerhedsunionen forankret i beskyttelsen af de grundlæggende rettigheder ved at værne om og fremme vores værdier.

Vi skal fortsætte indsatsen for at indføre en effektiv og ægte sikkerhedsunion. Det er nødvendigt at opnå hurtig enighed om vigtige verserende initiativer, herunder især: 1) lovgivningsforslaget om fjernelse af terrorrelateret onlineindhold, 2) lovgivningsforslaget om at forbedre de retshåndhævende myndigheders adgang til elektronisk bevismateriale, 3) lovgivningsforslaget om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningscenter for Cybersikkerhed og Netværket af Nationale Koordinationscentre samt 4) de endnu ikke færdigbehandlede lovgivningsforslag om stærkere og mere intelligente informationssystemer i forbindelse med sikkerhed og grænse- og migrationsforvaltning. For at opnå alle sikkerhedsmæssige fordele kræver det, at alle medlemsstater gennemfører EU-lovgivningen rettidigt og fuldstændigt, og at de vedtagne foranstaltninger og instrumenter omsættes i praksis. Det er navnlig vigtigt, at alle medlemsstater gennemfører den nyligt vedtagne lovgivning om interoperabilitet mellem EU's informationssystemer for sikkerhed og grænse- og migrationsforvaltning for at indfri det ambitiøse mål om at opnå fuld interoperabilitet senest i 2020. Endelig skal Europa fortsat være på vagt over for nye og skiftende trusler og fortsætte samarbejdet om at øge sikkerheden for alle borgere.