



Rådet for  
Den Europæiske Union

Bruxelles, den 18. oktober 2023  
(OR. en)

14394/23

COSI 181  
CRIMORG 139  
ENFOPOL 433  
CT 156  
COTER 186  
AVIATION 194  
JAI 1334

## FØLGESKRIVELSE

---

fra:	Martine DEPREZ, direktør, på vegne af generalsekretæren for Europa-Kommissionen
modtaget:	18. oktober 2023
til:	Thérèse BLANCHET, generalsekretær for Rådet for Den Europæiske Union

---

Komm. dok. nr.:	COM(2023) 659 final
Vedr.:	MEDDELELSE FRA KOMMISSIONEN TIL RÅDET OG EUROPA-PARLAMENTET om afværgelse af potentielle trusler fra droner

---

Hermed følger til delegationerne dokument COM(2023) 659 final.

Bilag: COM(2023) 659 final



EUROPA-  
KOMMISSIONEN

Bruxelles, den 18.10.2023  
COM(2023) 659 final

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

**om afværgelse af potentielle trusler fra droner**

## **I. INDLEDNING**

I denne meddelelse redegøres der for EU's politik til afværgelse af de potentielle trusler fra ikkesamarbejdende ubemandede luftfartøjssystemer, almindeligvis kendt som "droner". Det er en del af en bredere dronebekæmpelsespakke, der også omfatter to håndbøger, som giver praktisk vejledning om centrale tekniske aspekter af denne politik. Denne pakke blev bebudet som en flagskibsforanstaltning inden for rammerne af Kommissionens meddelelse "En dronestrategi 2.0 for et intelligent og bæredygtigt økosystem for ubemandede luftfartøjer i Europa"<sup>1</sup>. Denne meddelelse imødekommer behovet for at: i) tilvejebringe en omfattende og harmoniseret politisk ramme, ii) opbygge en fælles forståelse af de gældende procedurer for at imødegå den fortsatte udvikling af eventuelle trusler fra droner, iii) tage hensyn til den hurtige teknologiske udvikling.

### **A. Supplement til EU-rammen for droner**

Lovlig brug af droner er en vigtig del af vejen mod den dobbelte grønne og digitale omstilling som fastsat i EU's "dronestrategi 2.0". De spiller en vigtig rolle især inden for transport, forsvar, handel og tjenesteydelser. Antallet af droner, der anvendes i EU, forventes at stige betydeligt i de kommende år, og dronerne vil blive væsentligt forbedret med hensyn til hastighed, fleksibilitet, maksimal rækkevidde, nyttelastkapacitet, sensorernes præcision og anvendelse af kunstig intelligens. Denne udvikling vil føre til mere omfattende brug af droner til legitime og lovlige formål. For at dette potentiale kan realiseres, er det imidlertid nødvendigt at imødegå den potentielle trussel, som ikkesamarbejdende droner kan udgøre. En ikkesamarbejdende drone defineres ud fra arten af det manglende samarbejde, der kan være kriminelt, ulovligt (tilsigtede lovovertrædelser) eller amatøragtigt (uvidenhed, hensynsløshed).

Denne meddelelse omhandler trusler fra droner, der er udviklet til civil brug, og den har til formål at håndtere trusler fra disse droner i et civilt miljø. Selv om disse meddelelser ikke tager sigte på droner, der er udviklet til forsvarsformål, er der stadig flere indbyrdes forbindelser til forsvarsområdet. Disse forbindelser omfatter kriminelles eller terroristers potentielle brug af mindre droner, der er beregnet til forsvarsformål, samt synergier mellem teknologier til dronebekæmpelse. Droner, der er udviklet til forsvarsformål, kunne befinde sig i samme luftrum som civile droner, og i disse tilfælde skal de kunne identificeres af de kompetente myndigheder af hensyn til situationsbevidstheden.

Formålet med denne meddelelse er specifikt at *afværge* eventuelle trusler fra droner. Den har derfor ikke til formål at omfatte dronernes rolle på området indre sikkerhed i bredere forstand, nemlig deres anvendelse til retshåndhævelse, den offentlige sikkerhed eller sikring.

Medlemsstaternes myndigheder har det primære ansvar for at afværge truslerne fra ikkesamarbejdende droner. Medlemsstaterne drager dog også fordel af foranstaltninger på EU-niveau, der muliggør tættere samarbejde og koordinering med de forskellige midler og værktøjer, der anvendes til dette formål. Denne meddelelse fremmer derfor forskellige foranstaltninger vedrørende opbygning af fællesskaber og informationsudveksling. Den støtter også medlemsstaterne med vejledning, uddannelse, finansiering og operationelle procedurer.

Potentielt farlige hændelser med droner ses hyppigere i dag — både inden for og uden for EU's grænser. Det er derfor vigtigt, at de retshåndhævende myndigheder og andre offentlige myndigheder i EU og

---

<sup>1</sup> En dronestrategi 2.0 for et intelligent og bæredygtigt økosystem for ubemandede luftfartøjer i Europa (COM(2022) 652 final af 29. november 2022).

operatører af kritisk infrastruktur letter udbredelsen af fysiske eller digitale droneløsninger. Udformning af en dronebekæmpelsespolitik i EU vil bidrage til at styrke procedurerne for afprøvning af, hvor effektive de tilgængelige nye løsninger er, og til at lette den målrettede anvendelse af forskning og innovation på dette område. Ved at udforme denne dronebekæmpelsespolitik bidrager Kommissionen til at styrke EU-markedet for dronebekæmpelsesløsninger. Dette vil bane vejen for øget strategisk autonomi og teknologisk suverænitæt for EU, herunder inden for kritiske teknologier. Det vil fremme den europæiske kapacitet til at udvikle banebrydende løsninger på forsvars-, rumfarts- og civilsikkerhedsområdet og mindske afhængigheden af ikkeeuropæiske leverandører. Dette vil bygge på resultaterne af vurderingen af kritisk teknologisk afhængighed<sup>2</sup> og tilvejebringe yderligere data og analyser. Derudover vil det: i) danne grundlag for Kommissionens forståelse af brugen af kritiske teknologier og afhængigheden af ikkeeuropæiske leverandører og ii) give et solidt overblik over graden af afhængighed.

Med henblik på at afværge trusler fra ikke-samarbejdende droner ud fra en offentlig myndigheds perspektiv er det desuden vigtigt at: i) have indført klare og harmoniserede rammer og procedurer, ii) give de ansvarlige offentlige og private interessenter klare beføjelser til at gribe ind over for ikke-samarbejdende droner og iii) lette samarbejdet mellem interessenter, der ikke altid er vant til at samarbejde (retshåndhævende myndigheder, civile luftfartsmyndigheder, operatører, producenter, mobilnetoperatører). Med denne meddelelse fremlægges foranstaltninger til at: i) opbygge en fælles forståelse af gældende procedurer i forbindelse med imødegåelse af trusler fra droner, og ii) kortlægge eventuelle behov med hensyn til harmonisering af lovgivningsmæssige foranstaltninger

## **B. Imødegåelse af den aktuelle — og hurtigt voksende — trussel**

I både EU's strategi for sikkerhedsunionen<sup>3</sup> og dagsordenen for terrorbekæmpelse<sup>4</sup> understreges det, at truslen fra ikke-samarbejdende droner giver anledning til alvorlige problemer i Europa, som der skal tages hånd om.

De hastige fremskridt inden for droner udgør en stigende sikkerhedsrisiko. I de seneste år er der blevet afdækket planer om at forsøge at gøre brug af droner til terrorangreb<sup>5</sup>. Der har også været observationer af mistænkelige droner omkring kritisk infrastruktur såsom energianlæg, lufthavne og havne, hvilket tyder på potentielt misbrug af droner til fjendtlig indsamling af oplysninger. Droner anvendes af kriminelle, der er involveret i smugling på tværs af grænserne eller til at lette andre ulovlige aktiviteter, herunder narkotikahandel. Droner kan desuden være en kilde til cyberrisici, f.eks. hvis de anvendes til digital rekognoscering. Trusler fra droner er ikke blot et teknisk problem. I dag er det muligt at opdage og identificere de fleste droner, der er konstrueret til civile formål, men det er stadig meget vanskeligt at interagere med eller neutralisere dem (dvs. at overtage styringen med dem, få dem til at lande sikkert eller skyde dem ned), ofte på grund af manglende tilladelse hertil. Afværgelse af trusler fra droner bør derfor

---

<sup>2</sup> Der blev gennemført et Kommissionsinternt nærstudie af autonome systemer i 2022.

<sup>3</sup> Strategien for EU's sikkerhedsunion (COM(2020) 605 af 24. juli 2020).

<sup>4</sup> En EU-dagsorden for terrorbekæmpelse: foregribe, forebygge, beskytte, reagere (COM(2020) 795 final af 9. december 2020).

<sup>5</sup> Af eksempler kan nævnes: i) planen for en inspireret jihadist, der af en spansk domstol i oktober 2022 blev dømt for at have planlagt at angribe et stadion under en større fodboldkamp ved hjælp af en drone fyldt med sprængstoffer og ii) en belgisk statsborger, der er dømt for forsøg på et bombeangreb mod et fængsel ved hjælp af droner.

tages i betragtning ved fremtidige risikovurderinger ifølge direktivet om kritiske enheders modstandsdygtighed<sup>6</sup>.

Trusselsbilledet bliver endnu tydeligere, når man ser på hændelser i lande tæt på EU og i andre dele af verden. Droner viste sig at være en omkostningseffektiv og effektiv platform med dobbelt anvendelse, der har øget forsvarsinnovationen i den russiske krig mod Ukraine. Brugen af droner konstrueret til civile formål til ødelæggende angreb selv i forbindelse med andre væbnede konflikter (f.eks. i Yemen eller Syrien) er et fænomen, som sandsynligvis vil have konsekvenser for EU's indre sikkerhed. Terrorgruppers fremgangsmåde og deres øgede færdigheder inden for brug af standarddroner gør dem i stand til at nå vores grænser og udgør en trussel. Det samme gælder brugen af droner til målrettede attentater<sup>7</sup>.

Dronebekæmpelsesløsninger er imidlertid ikke kun nødvendige mod målrettede ondsindede formål. De er også nødvendige for at forebygge handlinger som følge af forsømmelighed eller uagtsom adfærd. De fleste brugere af droner i EU (navnlig autoriserede professionelle droneoperatører eller organiserede piloter, der udøver fritidsflyvning) overholder eksisterende regler, bestemmelser og tekniske forskrifter. Ikke desto mindre er uvidende, hensynsløse og kriminelle brugere af droner skyld i mange farlige hændelser med droner i hele EU. Store offentlige arrangementer er særligt sårbare over for sådanne forstyrrelser, og det samme gælder visse kritiske sektorer som lufttransport. Desuden kan ulovlig anvendelse af droner også påvirke den personlige sikkerhed og retten til privatlivets fred for den enkelte borger, navnlig når droner anvendes i beboelsesområder.

### **C. At holde trit med den teknologiske udvikling**

Beskyttelse af vores samfund mod ondsindede og ikkesamarbejdende droner kræver adgang til prisoverkommelige og pålidelige modforanstaltninger, der muliggør fleksible løsninger. Løsningerne vedrører normalt de tre aspekter, der handler om at opdage, opspore og identificere, mens de offentlige myndigheder også er interesserede i yderligere to aspekter: neutralisering og kriminalteknik.

På både forsvars- og civilsikkerhedsområdet er innovative dronebekæmpelsesløsninger allerede ved at blive udviklet og afprøvet. Deres adgang til markedet og udbredelse hos slutbrugere kan lettes ved hjælp af en overordnet EU-ramme for dronebekæmpelse, hvilket fremmes i denne meddelelse. Det er imidlertid ikke muligt at anvende en standardiseret universalløsning på gennemførelsen af dronebekæmpelsesforanstaltninger på grund af de mange forskellige mulige operationelle scenarier og områder.

Dronebekæmpelsesforanstaltninger skal derfor tilpasses forskellige behov og operationelle områder. Set fra myndigheder med ansvar for den indre sikkerheds synsvinkel kan der være situationer, hvor fuldstændig fysisk ødelæggelse af en drone er den foretrukne og eneste mulighed, f.eks. for at forhindre et umiddelbart forestående angreb mod mennesker eller infrastruktur. I andre tilfælde, såsom kriminel brug eller fjendtlig indsamling af oplysninger, er der stor interesse i at sikre kontrol over dronen for at få den til at lande, samtidig med at den forbliver så intakt som muligt, for at muliggøre en optimal kriminalteknisk efterforskning. Dette omfatter behovet for avancerede cyberløsninger til at tage kontrol over dronens operativsystem.

En af de teknologiske tendenser, der bør overvåges og anvendes aktivt, er udviklingen af sensorer til mere nøjagtig detektering af droner. Den eksisterende sensor kapacitet kan udvikles yderligere, ikke blot for at

---

<sup>6</sup> Direktiv (EU) 2022/2557 af 14. december 2022 om kritiske enheders modstandsdygtighed (EUT 2022 L 333, s. 164).

<sup>7</sup> Eksempler herpå er et mislykket attentatforsøg mod Venezuelas præsident og mexicanske narkokartellers brug af droner mod repræsentanter fra andre kriminelle organisationer.

opdage en drone, men også for at vurdere den trussel, den udgør, ved hjælp af analyse af flyvemønstre samt sporing af nyttelast og udstyr. Sensorer og detekteringsystemer skal være i stand til at håndtere dronernes skiftende former og kapacitet (hastighed, fleksibilitet, anvendelse til afledningsformål osv.). Kapaciteten hos offentlige myndigheder og private operatører af kritisk infrastruktur til at analysere data fra disse sensorer vil blive stadig vigtigere. Kunstig intelligens vil også spille en rolle, f.eks. til automatisk at generere advarsler, beregne risici, anslå ruter eller forudsige landingssteder. Nye tendenser på dronemarkedet skal derfor løbende overvåges og indarbejdes i dronebekæmpelsesløsningerne. Overvågningen af denne teknologiske udvikling bør gøre det muligt for myndighederne i EU at identificere investeringsprioriteter og støtte den udvikling, der er bedst egnet til at opfylde de operationelle behov, som medlemsstaternes retshåndhavende myndigheder og private operatører har givet udtryk for.

Med hensyn til interaktion og neutralisering er der behov for yderligere afprøvning af teknologier, der er bedst egnede i de forskellige miljøer og scenarier. På forsvarsområdet er der fundet løsninger til fysisk at ødelægge eller helt at opfange en drone, mens den befinder sig i luften, og dermed mindske genereringen af affald, der kan føre til personskader eller beskadigelse af genstande. Dette omfatter "dirigeret energi" i form af høj-energilasersystemer samt anvendelse af HF-systemer med høj effekt og netopfangelsessystemer samt digitale værktøjer til at opnå kontrol over ikkesamarbejdende droner.

For så vidt angår retshåndhævelse og efterforskning vil det være særlig nyttigt at kunne neutralisere en trussel fra en drone ved at tage kontrol over dens kontrolsystem og få den til at lande sikkert, hvilket vil give myndigheder og efterforskere den bedst mulige adgang til potentielt fysisk og digitalt bevismateriale. Der bør derfor være en bred vifte af forskellige løsninger, som er godkendt til forskellige formål, og som kan bruges til området indre sikkerhed. Det er derfor nødvendigt at fremme et reelt markeds- og innovationsmiljø for dronebekæmpelsesløsninger, der opfylder behovene på civilsikkerhedsområdet. Ellers vil udviklingen inden for dronebekæmpelsesløsninger efter al sandsynlighed ikke kunne holde trit med det stigende antal droner og deres kapacitet. Det er også vigtigt at strukturere og segmentere dette marked for at hjælpe de relevante myndigheder med at finde frem til de løsninger, der bedst opfylder deres behov.

Desuden er det vigtigt at overvåge de såkaldte dronebekæmpelsessystemer, der anvendes af kriminelle. Systemer til dronebekæmpelse består af anordninger, der enten transporteres af dronen eller styres fra jorden, og som er konstrueret på en sådan måde, at de kan skabe hindringer for specifikke dronebekæmpelsesforanstaltninger.

Endelig udvikles der også mange dronebekæmpelsessystemer til forsvarsformål. Selv om kravene er forskellige, har disse systemer ofte en række karakteristika og teknologier til fælles med systemer til civile formål, hvilket gør tæt samarbejde til en nødvendighed på forsvarsområdet.

Denne vedvarende teknologiske udvikling kræver også en konsekvent og løbende ajourført lovramme for anvendelsen af dronebekæmpelsessystemer.

## **II. UDFORMNING AF EN DRONEBEKÆMPELSESPOLITIK FOR EU**

Kommissionen har siden 2016 arbejdet sammen med medlemsstaterne og andre interessenter om eventuelle trusler fra droner, da EU's første workshop om dronebekæmpelse fandt sted. Siden da er der blevet iværksat en lang række initiativer til at lette opbygningen af fællesskaber, informationsudveksling, udvikling af bedste praksis og målrettet finansiering af projekter. Som følge af drøftelser med eksperter fra medlemsstaterne vil Kommissionen fortsat støtte disse igangværende initiativer og samtidig videreudvikle og integrere nye arbejdsområder med henblik på at udarbejde en fuldt udbygget dronebekæmpelsespolitik i EU. Dette arbejde vil bestå i de følgende seks vigtigste aktiviteter:



## A. Opbygning af fællesskaber og informationsdeling

En lang række forskellige netværk og aktører arbejder nu på EU-plan med dronebekæmpelsesløsninger. Der er derfor behov for at effektivisere og styre deres fremtidige aktiviteter i politisk, teknisk og operationel henseende for at: i) opbygge velfungerende grupper af interessenter, ii) sikre en effektiv udveksling af oplysninger og bedste praksis, iii) undgå dobbeltarbejde.

Kommissionen vil fremme eksisterende initiativer på teknisk plan og samtidig nedsætte en **ekspertgruppe under Kommissionen om dronebekæmpelse**, der skal yde rådgivning på politisk plan. Denne ekspertgruppe kan komme med strategisk input til forskellige politikker på EU-plan af relevans for dronebekæmpelsesaktiviteter, f.eks. inden for indre sikkerhed, grænseforvaltning eller kritisk infrastrukturens modstandsdygtighed. I den forbindelse vil ekspertgruppen skulle samarbejde med andre ekspertgrupper og, hvor det er relevant, med relevante arbejdsgrupper i Rådet.

Der afholdes regelmæssigt workshopper og ekspertmøder om dronebekæmpelsesløsninger og -politikker. Disse samler politiske beslutningstagere, tekniske eksperter og forskere fra Kommissionen, medlemsstaterne, andre EU-institutioner, EU-agenturer, EU-finansierede projekter, internationale organisationer og partnerlande. Disse aktiviteter har ført til løbende inddragelse af alle interessenter, hvilket har gjort deres operationelle og praktiske samarbejde markant lettere. I den forbindelse har Kommissionen oprettet det såkaldte "**Counter-UAS Information Hub**"<sup>8</sup>, som i øjeblikket har mere end 300 medlemmer. Denne onlineplatform opdateres regelmæssigt og rummer forskellige informationskilder såsom resultater fra relevante EU-finansierede projekter, præsentationer, rapporter og et halvårligt nyhedsbrev.

En anden vigtig del af opbygningen af fællesskaber og informationsdeling, navnlig med henblik på de retshåndhævende myndigheders operationelle behov, finder sted som en del af de EU-finansierede **europæiske retshåndhævelsesnetværk**. F.eks. har følgende netværk alle påbegyndt deres egne aktiviteter til afværgelse af trusler fra droner: Det Europæiske Netværk af Teknologiske Tjenester inden for Retshåndhævelse (ENLETS), EU-netværket for politi og grænsevagter i lufthavne (AIRPOL), EU-netværket for særlige indsatsenheder (ATLAS), EU's højrisikosikkerhedsnetværk. Den nyligt oprettede retshåndhævelsesnetværksgruppe, som er et initiativ fra GD HOME, der har til formål at fremme samarbejdet mellem politinetværk, og som finansieres af Kommissionen<sup>9</sup>, skal strømline de igangværende arbejdsområder på dronebekæmpelsesområdet i en særlig underarbejdsgruppe.

**Det Europæiske Unions Luftfartssikkerhedsagentur (EASA)** har udarbejdet ikkebindende retningslinjer, der hjælper myndigheder og lufthavne med at forberede sig på, reagere på og komme på fode

<sup>8</sup> Anvendelse af EU's CIRCABC-plattform, der støttes af Europa-Kommissionens [ISA<sup>2</sup>-programme](#), som fremmer interoperabilitetsløsninger for europæiske offentlige myndigheder.

<sup>9</sup> Formandskabet for den (uformelle) retshåndhævelsesnetværksgruppe (LENWG) varetages af Kommissionen, og den mødtes for første gang den 20. marts 2023 for at skabe et bedre samarbejde mellem de netværk, der finansieres af GD HOME. Efter en evalueringperiode på 12 måneder kan LENWG omdannes til en egentlig ekspertgruppe under Kommissionen.

igen efter dronehændelser<sup>10</sup>. For at fremme velinformede støtteaktiviteter og politikudformning på EU-plan er det vigtigt at have pålidelige og detaljerede udvekslinger af oplysninger om hændelser, der involverer droner i EU, ud over de udvekslinger, der allerede finder sted inden for specifikke kritiske områder såsom lufthavne. Samtidig med at efterforskningernes fortrolighed respekteres, er der et betydeligt potentiale for at forbedre udvekslingen af oplysninger om: i) de metoder, der anvendes af operatører af ikkesamarbejdende droner, ii) specifikke trusselsmønstre, iii) identificerede potentielle risici. For at lette og harmonisere udvekslingen af sådanne oplysninger om hændelser har Kommissionen udleveret en skabelon til rapportering af dronehændelser til medlemsstaterne. For yderligere at øge kvaliteten og hyppigheden af informationsdelingen vil Kommissionen undersøge muligheden for at oprette en **digital platform, der indeholder oplysninger om dronehændelser**, til brug for relevante offentlige myndigheder. Den kunne bruges til korrekt at identificere og sammenholde større sikkerhedshændelser, der involverer droner i EU. Dette kan også omfatte cyberområdet, da droner ikke kun anvendes til visuel rekognoscering, men også til digital rekognoscering. Denne platform vil være i overensstemmelse med de eksisterende rapporteringsforpligtelser i henhold til forordning (EU) nr. 376/2014<sup>11</sup> og vil ikke overlape den indsats, der allerede gøres.

Kommissionen vil også afholde regelmæssige klassificerede møder for at fremme udvekslingen af indhøstede erfaringer fra hændelser i et passende format.

#### **Vigtige foranstaltninger for opbygning af fællesskaber og informationsdeling**

- **Kommissionen vil nedsætte en ekspertgruppe bestående af eksperter fra medlemsstaterne og andre interessenter om dronebekæmpelsesaktiviteter.**
- **Kommissionen vil undersøge muligheden for at udvikle en digital platform, der indeholder oplysninger om dronehændelser.**
- **Kommissionen vil afholde regelmæssige møder for at lette udvekslingen af klassificerede informationer mellem medlemsstaterne om større sikkerhedshændelser, der involverer brug af droner.**

## **B. Afprøvning af dronebekæmpelsessystemer: identificering og afprøvning af løsninger**

Medlemsstaterne og de lokale myndigheder kan vælge fra en bred vifte af kommercielle cyber- og ikkecyberdronebekæmpelsesløsninger, som findes på markedet. Det kan være vanskeligt at træffe dette valg, navnlig for lokale enheder, der ikke har tilstrækkelig teknisk kapacitet. Kommissionen vil hjælpe medlemsstaternes myndigheder med at træffe det rette valg i forhold til deres operationelle behov ved at yde rådgivning og vejledning via den særlige ekspertgruppe om dronebekæmpelse og arbejdet i Kommissionens Fælles Forskningscenter (JRC).

Aktiviteter på EU-plan til afprøvning af dronebekæmpelsessystemer blev iværksat i 2019. De har til formål at udvikle en fælles metode til evaluering af systemer, der kan anvendes af retshåndhævende og andre offentlige myndigheder til at opdage, opspore og identificere potentielt ondsindede droner. En central søjle i disse aktiviteter er "Courageous"<sup>12</sup>-projektet (2021-2024), som finansieres af EU's Fond for Intern

---

<sup>10</sup> Den Europæiske Unions Luftfartssikkerhedsagentur (EASA) offentliggjorde i marts 2021 et sæt retningslinjer for håndtering af dronehændelser i lufthavne: [Drone Incident Management at Aerodromes](#).

<sup>11</sup> Europa-Parlamentets og Rådets forordning (EU) nr. 376/2014 af 3. april 2014 om indberetning og analyse af samt opfølgning på begivenheder inden for civil luftfart, ændring af forordning (EU).

<sup>12</sup> <https://courageous-isf.eu/>.

Sikkerhed — Politi (ISF-politi). Courageous ledes af det kongelige militærakademi i Belgien og har fået til opgave at: i) fastlægge relevante standardscenarier for afprøvning af dronebekæmpelsessystemer, ii) udvikle funktions- og præstationskrav, iii) udvikle en afprøvningsmetode. I forbindelse med projektet afprøves desuden sensorer og integrerede systemers ydeevne. Resultaterne af projektet deles løbende med medlemsstaterne samt udvalgte partnerlande og internationale organisationer. Når projektet er afsluttet, vil Kommissionen og konsortiet bag Courageous forelægge medlemsstaterne muligheder for at sikre projektets bæredygtighed og anbefale en **metode til afprøvning af dronebekæmpelsesfaciliteter** i medlemsstaterne.

Den teknologiske udvikling af relevans for dronebekæmpelsessystemer går meget stærkt. Aktiviteterne i forbindelse med afprøvning skal derfor suppleres med konstant overvågning af tendenser for at identificere både de mest lovende løsninger og eventuelle nye udfordringer, som udviklingen af dronebekæmpelsessystemer står over for. JRC har opbygget kapacitet til at foretage denne overvågning og identificere disse nye udfordringer. Dette er til gavn for medlemsstaterne og giver værdifuldt input til afprøvningsinitiativer på EU-plan. Oplysningerne vil blive delt via de relevante kanaler, navnlig ekspertgruppen.

Standardisering er et instrument til harmonisering af teknologiske løsninger. I forbindelse med Courageous-projektet blev der udarbejdet konkrete råd til præstandardisering, på grundlag af hvilke gennemførligheden af — og behovet for — iværksættelse af standardiseringsprocesser kan vurderes yderligere. På EU-plan er der gjort gode fremskridt med udviklingen af frivillige præstationskrav til detektionsudstyr uden for luftfart (f.eks. røntgenapparater og metaldetektorer<sup>13</sup>). Sammen med eksperter fra medlemsstaterne og industrien vil Kommissionen nu også udvikle **frivillige præstationskrav** til dronebekæmpelsessystemer, og hvor det er relevant, i overensstemmelse med bestemmelserne i forordningen om cybersikkerhed<sup>14</sup>. Etablering af en certificeringsproces for dronebekæmpelsessystemer bør fortsat være en midtvejsmålsætning. Hvor det er relevant, vil der også blive taget hensyn til hybride civile/forsvarsrelaterede standarder.

Standardisering og certificering af cybersikkerheden i dronebekæmpelsessystemer er et andet centralt element — navnlig hvis de kommer fra leverandører fra lande uden for EU. På nuværende tidspunkt er der fortsat usikkerhed om beskyttelsesgraden for data, som indsamles af visse detektionssystemer. Desuden er det vigtigt så vidt muligt at forebygge hacking og misbrug af dronebekæmpelsessystemer ved at sikre deres komponenters cyberrobusthed.

I september 2022 vedtog Kommissionen et forslag til en forordning om cyberrobusthed<sup>15</sup> med det formål at udarbejde generelle cybersikkerhedsregler for produkter med digitale komponenter — både hardware og software — med adgang til det indre marked. Den foreslåede nye forordning har til formål at indføre obligatoriske cybersikkerhedskrav for disse produkter. Disse krav vil omfatte cybersikkerhed som følge af standardindstillinger og indbygget sikkerhed samt krav for at imødegå sårbarheder. Som foreslået af Kommissionen vil dronesystemer, der ikke udelukkende er udviklet til nationale sikkerhedsformål eller militære formål, og som ikke allerede er certificeret i overensstemmelse med forordning (EU) 2018/1139, være omfattet af disse nye regler som produkter med digitale elementer med undtagelse af dem, der udelukkende er udviklet til nationale sikkerheds- eller forsvarsformål.

---

<sup>13</sup> Kommissionens henstilling om frivillige ydeevnekrav til røntgenudstyr, der anvendes i det offentlige rum (C(2022) 4179 final).

<sup>14</sup> Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed) og om cybersikkerhedscertificering af informations- og kommunikationsteknologi.

<sup>15</sup> Forslag til Europa-Parlamentets og Rådets forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020 (COM(2022) 454 final).

### Vigtige foranstaltninger for afprøvning af dronebekæmpelsessystemer

- **Kommissionen vil arbejde på at gennemføre en harmoniseret metode til afprøvning af dronebekæmpelsessystemer baseret på resultaterne af Courageous-projektet.**
- **JRC vil udarbejde en årlig rapport om den tekniske udvikling inden for dronebekæmpelsesteknologi.**
- **Kommissionen vil i samarbejde med relevante grupper af eksperter, som f.eks. Retshåndhævelsesnetværkene, ENLETS, HRNS og AIRPOL, udvikle et sæt frivillige præstationskrav til dronebekæmpelsessystemer.**

## C. Praktisk vejledning og operationel støtte

Tackling af trusler fra ikkesamarbejdende droner er allerede blevet udpeget som en prioritet i en række publikationer fra JRC, f.eks. i retningslinjer med fokus på beskyttelse af bygninger i omgivende områder<sup>16</sup> og i den særlige undersøgelse vedrørende dronetransporterede sprængstofladninger<sup>17</sup>. Desuden fremhæver den nylige publikation<sup>18</sup> om begrebet indbygget sikkerhed betydningen af at integrere forholdsmæssige, passende og multifunktionelle beskyttelsesforanstaltninger i en gennemtænkt tilgang helt fra de indledende planlægnings- og udformningsfaser af et projekt, herunder foranstaltninger til bekæmpelse af angreb ved hjælp af droner.

Den Europæiske Unions Luftfartssikkerhedsagenturs håndbog om håndtering af dronehændelser i og omkring lufthavne indeholder desuden vejledning i, hvordan der kan udvikles passende ordninger og procedurer, som understøtter et hurtigt, effektivt og forholdsmæssigt system til håndtering af hændelser i og omkring lufthavne. På den måde kan indstillinger af flytrafikken eller lukning af luftrum eller start- og landingsbaner undgås eller begrænses til et minimum, og lukning af lufthavne kan anvendes som en sidste udvej. I EASA's arbejde tages hensyn til Organisationen for International Civil Luftfarts retningslinjer for luftfartssikkerheden<sup>19</sup>.

JRC har udarbejdet to nye håndbøger:

- ***Protection against Unmanned Aircraft Systems: Handbook on UAS protection of Critical Infrastructure and Public Space — A five Phase approach for C-UAS stakeholders** (foreligger ikke på dansk).*
- ***Protection against Unmanned Aircraft Systems: Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites** (foreligger ikke på dansk).*

På **uddannelsesområdet** blev der i forbindelse med det EU-finansierede projekt DroneWISE<sup>20</sup> udarbejdet en pakke af dronebekæmpelsesstrategier for styring, kontrol og koordinering til førstehjælpsydere. I forbindelse med projektet blev der også udarbejdet ti undervisningsmoduler, en håndbog og en portal med

<sup>16</sup> Karlos, V. and Larcher, M., Guideline — Building Perimeter Protection, EUR 30346 EN, Den Europæiske Unions Publikationskontor, Luxembourg, 2020.

<sup>17</sup> Truslen fra ubemandede luftfartøjssystemer, der anvender sprængstoffer, blev undersøgt af JRC i: Larcher M, Karlos V, Valsamos G, Solomos G: Scenario study: drones carrying explosives, JRC107683, 2018.

<sup>18</sup> Europa-Kommissionen, Security by Design: Protection of public spaces from terrorist attacks, JRC131172, 2022.

<sup>19</sup> ICAO's luftfartssikkerhedshåndbog (DOC 8973-restricted) hjælper medlemsstaterne med at gennemføre bilag 17 til Chicagokonventionen ved at give vejledning i, hvordan dens standarder og anbefalede praksis (SARP) indeholdt i [luftfartssikkerhedshåndbogen](#) skal anvendes.

<sup>20</sup> <https://dronewise-project.eu/>.

onlinekurser. Disse undervisningsmoduler er blevet integreret i læreplanen for CEPOL, som er Den Europæiske Unions Agentur for Uddannelse inden for Retshåndhævelse. Et andet ISF-projekt, der var centreret om dronebekæmpelsesundervisning, var Skyfall-projektet. Der er behov for yderligere at udvide den tilgængelige undervisning til at omfatte private udbydere af sikkerhedskurser, navnlig dem, der er ansvarlige for beskyttelse af kritisk infrastruktur.

Kommissionens **program for rådgivere til EU's sikkerhedstjenester (EU PSA)**<sup>21</sup> indeholder et særligt afsnit om dronebekæmpelsesaktiviteter, som omfatter: i) en særlig sårbarhedsvurdering med hensyn til knudepunkter med høj risiko og infrastruktur, ii) praktisk vejledning i, hvordan man håndterer truslen fra droner, iii) praktiske råd om, hvordan man håndterer tilgængeliggørelse af dronedetektionsudstyr i forbindelse med højrisikohændelser. Kommissionen vil undersøge behovet for at oprette en EU-pulje af dronebekæmpelsesudstyr, som stilles til rådighed for medlemsstaterne til at støtte dem ved store arrangementer.

**Øvelser** såsom dem, der organiseres med retshåndhævelsesnetværket på EU-plan, bidrager til det operationelle beredskab på forskellige områder af den indre sikkerhed. Hvor det er relevant vil Kommissionen arbejde med de relevante netværk om at inkludere dronebekæmpende elementer i fremtidige øvelser. Dette vil bidrage til yderligere at øge viden og udveksling af bedste praksis ved hjælp af forskellige løsninger. Ét krav til en effektiv reaktion på trusler fra droner er, at der skal kunne finde pålidelig, sikker kommunikation sted mellem forskellige myndigheder. Afværgelse af trusler fra droner vil derfor være en del af den fremtidige planlægning af øvelser, der skal gennemføres som led i det EU-finansierede BroadEU.Net Preparation-projekt, som tester grundlaget for EU's fremtidige kritiske kommunikationssystem<sup>22</sup>. Desuden kan der gennemføres fælles øvelser, herunder med deltagelse af eksperter i cybersikkerhed og dronesikkerhed, i håndtering af cyberrisici i forbindelse med brug af droner, samt digitale løsninger til neutralisering af droner.

#### **Vigtige foranstaltninger for praktisk vejledning og operationel støtte**

- **JRC vil offentliggøre to håndbøger som en del af dronebekæmpelsespakken.**
- **Kommissionen vil i samarbejde med relevante agenturer støtte udvidelsen af den eksisterende dronebekæmpelsesundervisning til den private sikkerhedssektor.**
- **Kommissionen vil integrere dronebekæmpelseskomponenterne i planlægningen af øvelser i samarbejde med retshåndhævelsesnetværk.**

## **D. Forskning og innovation**

EU fortsætter med at finansiere sit sikkerheds-/forskningsprogram som en del af **Horisont Europa (2021-2027)**<sup>23</sup>. Dette sikkerheds-/forskningsprogram tegner sig for ca. 50 % af den samlede offentlige finansiering, der investeres i EU og dets medlemsstater på sikkerhedsområdet. Som strategisk bidragsyder til EU's forskellige sikkerhedspolitiske prioriteter er denne sikkerhedsforskning også allerede begyndt at se

<sup>21</sup>[https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa\\_en](https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en).

<sup>22</sup> EU's kritiske kommunikationssystem vil tilvejebringe en sikker bredbåndsbaseret infrastruktur for at sikre grænseoverskridende interoperabilitet mellem de kommunikationssystemer, der anvendes af retshåndhævende myndigheder og indsatspersonel i Schengenområdet.

<sup>23</sup> Tidligere, indtil slutningen af 2020, blev sikkerhedsforskning og innovation finansieret under Horisont 2020 og det 7. rammeprogram.

på truslerne fra droner. Vigtige eksempler omfatter ALADDIN, som fastlægger løsninger til detektion og neutralisering af droner i områder med adgangsbegrænsning<sup>24</sup>, eller 7SHIELD, som har undersøgt udviklingen af dronebekæmpelsesløsninger til jordsegmenter i kritisk ruminfrastruktur. ALFA-projektet var også vellykket med hensyn til at udvikle et system til detektion og opsporing af droner, der anvendes til smugling<sup>25</sup>. Disse forsknings- og innovationsinitiativer kan videreføres under Horisont Europa, valideres eller suppleres med foranstaltninger, der gennemføres inden for ISF-politi.

I fremtiden vil Kommissionen lette den mere systematiske udveksling af relevante projekter med relevante interessenter, herunder via det europæiske forsknings- og innovationsfællesskab for sikkerhed<sup>26</sup>. Dette vil yderligere styrke den specifikke dataudveksling. Det vil også gøre det muligt at indsamle brugerkrav mere effektivt og formidle disse krav til industrien med henblik på at styre innovation. Desuden vil systematisk udveksling af projekter bidrage til at muliggøre en struktureret dialog med medlemsstaterne og interessenter med henblik på at identificere lovende teknologier, værktøjer og løsninger, som en gruppe af medlemsstaternes myndigheder kan anvende. I den forbindelse vil Kommissionen sammen med medlemsstaterne<sup>27</sup> vurdere muligheden for at: i) skabe et uafhængigt forskningsemne om dronebekæmpelsesløsninger i Horisont Europas fremtidige arbejdsprogrammer, ii) støtte specifikke innovative systemer gennem prækommercielle indkøb<sup>28</sup>. Dette er i fuld overensstemmelse med den kapacitetsbaserede tilgang, der er beskrevet i arbejdsdokumentet fra Kommissionens tjenestegrene "Enhancing security through research and innovation"<sup>29</sup>.

Det er afgørende at styrke synergierne i forbindelse med dronebekæmpelsesløsninger mellem Europas civilsikkerheds-, forsvars- og rumindustri. Formålet med dette bør være at fremme synergier inden for drone- og dronebekæmpesesteknologier mellem de tre sektorer<sup>30</sup>. I praksis betyder en styrkelse af disse synergier, at forsvarsprojekter kan drage fordel af innovativ udvikling på det civile område, mens civil luftfart kan drage fordel af udviklingen på forsvarsområdet.

**Den Europæiske Forsvarsfond** og de foregående programmer tilskynder til og støtter samarbejdsbaseret, grænseoverskridende forskning og udvikling på forsvarsområdet. Som supplement til og styrkelse af medlemsstaternes indsats fremmer Den Europæiske Forsvarsfond samarbejdet mellem virksomheder og forskere af enhver størrelse og fra alle medlemsstater i EU. Programmerne forud for Den Europæiske Forsvarsfond har allerede finansieret dronebekæmpelsesprojekter som led i forskning og udvikling i forsvar.

---

<sup>24</sup> <https://cordis.europa.eu/project/id/740859>.

<sup>25</sup> Alfa er også grundlaget for ISF-projektet Courageous og dets aktiviteter i forbindelse med afprøvning.

<sup>26</sup> Det europæiske forsknings- og innovationsfællesskab for sikkerhed (CERIS) samler interessenter inden for sikkerhedsforskning, lige fra politiske beslutningstagere, slutbrugere, den akademiske verden og industrien til civil sikkerhed: [https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security\\_en](https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en).

<sup>27</sup> I programsammensætningen "Civilsikkerhed for samfundet" under Horisont Europa.

<sup>28</sup> Prækommercielle indkøb er en tilgang til offentlige indkøb af forsknings- og udviklingstjenester, som blev skitseret i meddelelsen om prækommercielle indkøb (C(2007) 799 final) af 14.12.2007). Det er et vigtigt redskab til at stimulere innovationen, da det sætter den offentlige sektor i stand til at styre udviklingen af nye løsninger i retning af dens behov.

<sup>29</sup> Arbejdsdokument fra Kommissionens tjenestegrene "Enhancing security through research and innovation" (SWD(2021) 422 final af 15.12.2021).

<sup>30</sup> (SWD(2022) 362 af 10.11.2022). Som beskrevet i statusrapporten om gennemførelsen af handlingsplanen om synergier mellem civilsikkerheds-, forsvars- og rumindustrien under foranstaltning 9.

Den Europæiske Forsvarsfonds arbejdsprogram for 2023 indbefatter en udviklingsforanstaltning til dronebekæmpelse<sup>31</sup> med et vejledende budget på 43 mio. EUR. Foranstaltningen har til formål at udvikle hardware- eller softwaremoduler til en omfattende mobil løsning til bekæmpelse af en lang række droner, herunder sværme.

Det vigtigste forventede resultat af Den Europæiske Forsvarsfonds støtte til dronebekæmpelsesområdet i 2021-2027 er en udviklet prototype til en dronebekæmpelsesløsning, der kan føre til eventuelle fremtidige fælles indkøb på EU-plan. Teknologiske udfordringer inden for dronebekæmpelsessystemer imødegås gennem EU-ordningen for forsvarsinnovation. EU-ordningen for forsvarsinnovation omfatter desuden et indsatsområde for væksthuse med dobbelt anvendelse for at fremme et bedre samarbejde mellem det civile område og forsvarsområdet og anspore til teknologisk modning og tilpasning.

En anden bærende søjle for innovation — og specifikt for anvendt forskning i, hvordan trusler fra droner kan imødegås — er JRC's arbejde. Som led i JRC's projekt Drone C-UAS vil JRC se på aktive og passive teknologier som modforanstaltninger, og hvordan disse teknologier kan anvendes til at garantere sikkerheden i det offentlige rum og kritisk infrastruktur.

I den forbindelse, og som et første skridt, vil JRC oprette et **levende laboratorium** til at undersøge dronebekæmpessteknologier, og hvordan disse teknologier kan anvendes i den virkelige verden. Laboratoriets opsætning vil omfatte planlægning, forberedelse og gennemførelse af en løsning. Det vil også omfatte detektion, opsporing, identifikation, neutralisering og integration af interessenter og processer. Anvendelsesområdet for gennemførelsen af det levende laboratorium vil omfatte integration med bemandede og ubemandede trafikstyringssystemer, navnlig U-space<sup>32</sup>. Det levende laboratorium vil også undersøge, hvordan maskinlæring og kunstig intelligens kan integreres med henblik på at forbedre de overordnede præstationer ved en dronebekæmpelsesløsning.

På mellemlang sigt vil JRC's levende laboratorium blive udviklet til et **ekspertisecenter for dronebekæmpelse**.

**Prioriterede foranstaltninger med henblik på at få mest muligt ud af forskning og innovation**

- **Kommissionen og medlemsstaterne vil træffe afgørelse om fremtidige behov for nye dronebekæmpelsesløsninger, der skal imødegås af relevante europæiske forsknings- og innovationsprogrammer, navnlig Horisont Europa.**
- **Kommissionen og medlemsstaterne vil opstille en liste over lovende dronebekæmpelsesløsninger og vurdere gennemførligheden af prækommercielle indkøb af nogle af disse løsninger.**
- **Kommissionen vil identificere idéer, teknologier og løsninger, der skal integreres i udviklingen af forsvarskapacitet, og vil støtte projekter, der har til formål at udbrede disse idéer, teknologier og løsninger til civile sektorer.**
- **JRC vil oprette et ekspertisecenter for dronebekæmpelse som en videreudvikling af det levende laboratorium.**

<sup>31</sup> C(2023) 2296 Kommissionens gennemførelsesafgørelse af 29.3.2023 om finansiering af Den Europæiske Forsvarsfond, oprettet ved Europa-Parlamentets og Rådets forordning (EU) 2021/697 og om vedtagelse af arbejdsprogrammet 2023 — Del II.

<sup>32</sup> Kommissionens gennemførelsesforordning (EU) 2021/664 om et regelsæt for U-space. Termen "U-space" anvendes til at beskrive ubemandede trafikstyringssystemer for at sikre sikker interaktion med andre enheder, der anvender det samme rum i byområder og andre steder.

## E. Finansiering af støtte

Kommissionen vil fortsat yde finansiel støtte til relevante dronebekæmpelsesaktiviteter, primært gennem ISF, men også inden for rammerne af instrumentet for finansiel støtte til grænseforvaltning og visumpolitik (IGFV) og Horisont Europa-programmet (til forsknings- og innovationsrelaterede foranstaltninger).

ISF's tematiske facilitet vil støtte: i) de europæiske retshåndhævelsesnetværk, ii) JRC's arbejde i forbindelse hermed, iii) den nye ekspertgruppe for dronebekæmpelse og iv) oprettelsen af en platform til udveksling af oplysninger. Kommissionen finansierer allerede projekter med henblik på at afprøve og godkende systemer til detektion og lokalisering af droner, der ulovligt krydser EU's ydre grænser. Disse projekter er baseret på resultater fra tidligere EU-finansierede forskningsprojekter<sup>33</sup>.

Under ISF's tematiske facilitet vil Kommissionen i første halvdel af 2024 iværksætte en **indkaldelse af forslag**, der specifikt har til formål at støtte tilgængeliggørelse af dronebekæmpelsesløsninger med potentiel høj udnyttelse.

Medlemsstaterne opfordres til at gennemføre denne meddelelse og udnytte resultaterne af EU-finansieret forskning i dronebekæmpelsesløsninger gennem deres ISF-programmer.

### **Vigtige foranstaltninger for finansiering af støtte**

- **Kommissionen vil iværksætte en indkaldelse af forslag vedrørende dronebekæmpelsesløsninger under ISF's arbejdsprogrammer under den tematiske facilitet for 2026-2027.**
- **Medlemsstaterne opfordres til at gøre fuld brug af deres ISF-programmer for 2021-2027 med henblik på at identificere og indføre effektive dronebekæmpelsesløsninger.**

## F. Undersøgelse af lovgivningsmæssige foranstaltninger

Selv om der findes EU-lovgivning, som regulerer lovlig brug af droner, er der i øjeblikket ingen specifikke regler til dronebekæmpelse, der fastsætter en fælles harmoniseret ramme for medlemsstaternes myndigheder, operatører og producenter. Selv om Den Europæiske Unions Luftfartssikkerhedsagenturs ikke-bindende retningslinjer vedrørende håndtering af dronehændelser i lufthavne (som tidligere nævnt i denne meddelelse) blev positivt modtaget af sektoren, gør deres rådgivende karakter og begrænsede anvendelsesområde dem utilstrækkelige til at afbøde truslen fra ikkesamarbejdende droner. Da behovet for

<sup>33</sup> Eksempler herpå er projekter, der finansieres under IGFV's specifikke foranstaltninger vedrørende: i) innovation inden for sø-/kyst- og/eller landgrænser og ii) Frontex. Nogle projekter, der finansieres under den specifikke foranstaltning vedrørende innovation inden for sø-/kyst- og/eller landgrænser, fokuserer på at afprøve innovative overvågningsteknologier. Der er også en specifik foranstaltning for indkøb og tilrådighedsstillelse af udstyr, som de europæiske grænsemyndigheder kan indsætte med henblik på detektion og lokalisering af droner, der krydser grænser i forbindelse med ulovlige eller kriminelle aktiviteter. Denne specifikke foranstaltning vil gøre det muligt for medlemsstaterne at indkøbe to dronebekæmpelsessystemer. Som en EU-merværdi skal det tekniske udstyr, der indkøbes i forbindelse med de specifikke foranstaltninger, som led i de årlige bilaterale forhandlinger efter anmodning fra Frontex stilles til rådighed for Frontex i en periode på op til fire måneder om året til brug for dets fælles operationer.

effektivt at forhindre uautoriseret brug af droner er stadig stigende, vil Kommissionen i tæt samarbejde med eksperter fra medlemsstaterne yderligere analysere behovet for fremtidige lovgivningsmæssige eller ikke-lovgivningsmæssige foranstaltninger. I den forbindelse vil Kommissionen iværksætte en særlig **kortlægningsundersøgelse** for at fastlægge de aktuelle lovgivningsmæssige rammer. Denne kortlægningsundersøgelse bør også tage hensyn til ICAO's rammer og udvikling samt tage hensyn til, at regler til afværgelse af eventuelle trusler fra droner ikke unødigt bør hindre lovlige aktiviteter, herunder blandt organiserede piloter, der udøver fritidsflyvning.

Lufthavne i EU nyder godt af detaljerede og omfattende sikkerhedsregler, der også dækker truslen fra droner. For at sikre, at luftfartsmyndighederne og lufthavnene er mere modstandsdygtige over for de risici, som droner giver anledning til, og i overensstemmelse med en evidensbaseret tilgang, vil Kommissionen i samarbejde med medlemsstaterne **identificere potentielle yderligere sårbarheder i forbindelse med beskyttelse mod ikkesamarbejdende droner i en sikkerhedsrisikovurdering, der kan kræve lovgivningsmæssige ændringer.**

Der er i den forbindelse behov for en struktureret dialog med industrien og droneproducenterne om foranstaltninger med hensyn til indbygget sikkerhed (f.eks. robuste systemer til beskyttelse mod spoofing, kapacitetsbegrænsninger, deling af kommunikationsprotokoller og opdateringer til dronebekæmpelsesdatabaser).

**Vigtige foranstaltninger med henblik på at undersøge lovgivningsmæssige foranstaltninger**

- **Kommissionen vil iværksætte en kortlægningsundersøgelse med henblik på fastlæggelse af behovet for lovgivningsmæssige rammer og potentialet for harmonisering af medlemsstaternes love og procedurer.**
- **I overensstemmelse med en evidensbaseret tilgang vil Kommissionen foretage en sikkerhedsrisikovurdering af droner inden for luftfarten med henblik på at identificere potentielle yderligere sårbarheder i lufthavne, som kan give anledning til lovgivningsmæssige ændringer.**
- **Kommissionen vil indgå i en struktureret dialog med industrien om behovet for — og arten af — potentielle yderligere specifikke foranstaltninger vedrørende sikkerheden ved droner.**

### **III. VEJEN FREM**

For at sikre, at hurtig teknologisk udvikling og det stigende antal droner ikke fører til en ukontrolleret stigning i antallet af trusler fra ikkesamarbejdende droner, er der behov for at øge samarbejdet på EU-plan på grundlag af den omfattende dronebekæmpelsespolitik for EU, som fremgår af denne meddelelse. I den forbindelse vil de nuværende aktiviteter på EU-plan blive videreført og suppleret med den række vigtige foranstaltninger, der er anført i denne meddelelse, og som vil blive gennemført i de kommende år.

De aktiviteter, der skitseres i denne meddelelse, dækker perioden frem til 2030. Senest i 2027 vil der blive foretaget en midtvejsevaluering af ekspertgruppen, mens der er planlagt en fuldstændig revision af EU's dronebekæmpelsesprogram senest i 2030.