Raad van de
Europese Unie

Brussel, 18 oktober 2023
(OR. en)

14394/23

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

BEGELEIDENDE NOTA

van:	de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur
ingekomen:	18 oktober 2023
aan:	mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie
nr. Comdoc.:	COM(2023) 659 final
Betreft:	MEDEDELING VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT over de bestrijding van mogelijke dreigingen van drones

Hierbij gaat voor de delegaties document COM(2023) 659 final.

Bijlage: COM(2023) 659 final

EUROPESE
COMMISSIE

Brussel, 18.10.2023
COM(2023) 659 final

MEDEDELING VAN DE COMMISSIE AAN DE RAAD EN HET EUROPEES PARLEMENT

over de bestrijding van mogelijke dreigingen van drones

I. INLEIDING

In deze mededeling wordt het beleid van de EU uiteengezet om mogelijke dreigingen van niet-coöperatieve onbemande luchtvaartuigsystemen (UAS), algemeen bekend als "drones", tegen te gaan. Het maakt deel uit van een breder "counter-dronepakket" dat ook twee handboeken omvat met praktische richtlijnen over belangrijke technische aspecten van dit beleid. Dit pakket werd aangekondigd als een kernactie in het kader van de mededeling van de Commissie "Een dronestrategie 2.0 voor een slim en duurzaam ecosysteem voor onbemande luchtvaartuigen in Europa"[1]. Deze mededeling komt tegemoet aan de behoefte om: i) een alomvattend en geharmoniseerd beleidskader te bieden; ii) een gemeenschappelijk inzicht te verkrijgen in de toepasselijke procedures om het hoofd te bieden aan de voortdurend evoluerende dreigingen van drones; en iii) rekening te houden met de snelle technologische ontwikkelingen.

A. Aanvulling op het EU-kader voor drones

Het legitieme gebruik van drones is een belangrijk onderdeel van de verwezenlijking van de dubbele groene en digitale transitie, zoals uiteengezet in de "Drone-strategie 2.0" van de EU. Zij spelen een belangrijke rol, met name op het gebied van vervoer, defensie, handel en diensten. Het aantal drones dat in de EU wordt gebruikt, zal de komende jaren naar verwachting aanzienlijk toenemen, met sterke verbeteringen wat betreft snelheid, wendbaarheid, maximale actieradius, laadvermogen, precisie van sensoren en gebruik van kunstmatige intelligentie. Deze ontwikkelingen zullen leiden tot een breder spectrum van legitieme en rechtmatige toepassingen van drones. Om dit potentieel te bereiken, is het echter noodzakelijk om de potentiële dreiging van niet-coöperatieve drones aan te pakken. Een niet-coöperatieve drone moet worden gedefinieerd op basis van de aard van de niet-coöperativiteit, waaronder crimineel of illegaal gebruik (een beoogde inbreuk op de regelgeving), dan wel amateurisme (onwetendheid, onvoorzichtigheid).

Deze mededeling behandelt dreigingen van drones voor civiel gebruik en is bedoeld om dreigingen van deze drones in een civiele omgeving aan te pakken. Hoewel drones die zijn ontworpen voor defensiedoeleinden niet centraal staan in deze mededeling, zijn er wel verschillende verbanden met het defensiedomein. Deze verbindingen omvatten het mogelijke gebruik van kleinere drones die door criminelen of terroristen voor defensiedoeleinden zijn ontworpen, evenals de synergieën tussen counter-dronetechnologieën. Drones die zijn ontworpen voor defensiedoeleinden, kunnen van hetzelfde luchtruim gebruikmaken als civiele drones, en in die gevallen moeten ze door de bevoegde autoriteiten kunnen worden geïdentificeerd met het oog op situationeel bewustzijn.

Het toepassingsgebied van deze mededeling betreft specifiek het *bestrijden* van de potentiële dreigingen van drones. In deze mededeling wordt dan ook niet de bredere dimensie van de rol van drones op het gebied van interne veiligheid behandeld, zoals de inzet ervan voor rechtshandhaving, openbare veiligheid of beveiliging.

De autoriteiten van de lidstaten zijn in de eerste plaats verantwoordelijk voor het tegengaan van de dreigingen van niet-coöperatieve drones. De lidstaten profiteren echter ook van maatregelen op EU-niveau, die nauwere samenwerking en coördinatie mogelijk maken voor de verschillende hiertoe te gebruiken middelen en instrumenten. Daarom worden in deze mededeling verschillende acties voor

[1] Een dronestrategie 2.0 voor een slim en duurzaam ecosysteem voor onbemande luchtvaartuigen in Europa (COM(2022) 652 final van 29 november 2022).

gemeenschapsopbouw en informatie-uitwisseling gestimuleerd. De lidstaten worden ook ondersteund met begeleiding, opleiding, financiering en operationele procedures.

Potentieel gevaarlijke incidenten met drones komen steeds vaker voor — zowel binnen de EU als daarbuiten. Het is daarom belangrijk om de toepassing van fysieke of digitale counter-drone-oplossingen voor rechtshandhavingsinstanties, andere overheidsinstanties in de EU en exploitanten van kritieke infrastructuur te vergemakkelijken. Het opstellen van een counter-dronebeleid van de EU helpt de procedures voor het testen van de efficiëntie van beschikbare nieuwe oplossingen te versterken en het doelgericht gebruik van onderzoek en innovatie op dat gebied te vergemakkelijken. Door dit counter-dronebeleid op te stellen, helpt de Commissie een EU-markt voor counter-drone-oplossingen te versterken. Dit beleid effent de weg voor meer strategische autonomie en technologische soevereiniteit voor de EU, ook op het gebied van kritieke technologieën. Het bevordert de Europese capaciteiten om geavanceerde oplossingen te ontwikkelen op het gebied van defensie, ruimtevaart en civiele veiligheid en vermindert de afhankelijkheid van niet-Europese leveranciers. Het bouwt voort op de resultaten van de evaluatie van afhankelijkheden van kritieke technologieën[2] en verschaft verdere gegevens en analyses. Dit beleid omvat ook: i) input om de Commissie inzicht te geven in het gebruik van kritieke technologieën en de afhankelijkheid van niet-Europese leveranciers; en ii) een gedegen overzicht van de mate van afhankelijkheid.

Bovendien is het voor overheidsinstanties bij het bestrijden van dreigingen van niet-coöperatieve drones ook belangrijk dat: i) zij beschikken over duidelijke en geharmoniseerde kaders en procedures; ii) de verantwoordelijke openbare en particuliere belanghebbenden duidelijke bevoegdheid krijgen om in te grijpen tegen niet-coöperatieve drones; en iii) samenwerking wordt bevorderd tussen belanghebbenden die niet altijd gewend zijn om samen te werken (rechtshandhavingsautoriteiten, burgerluchtvaartautoriteiten, exploitanten, fabrikanten, beheerders van mobiele netwerken). In deze mededeling worden maatregelen voorgesteld om: i) een gemeenschappelijk begrip op te bouwen van toepasselijke procedures bij dreigingen van drones; en ii) mogelijke behoeften op het gebied van harmonisatie van regelgevingsmaatregelen in kaart brengen.

B. Het aanpakken van een bestaande en snel evoluerende dreiging

Zowel in de strategie voor de veiligheidsunie[3] als in de terrorismebestrijdingsagenda[4] wordt benadrukt dat de dreiging van niet-coöperatieve drones in Europa een ernstig probleem vormt en moet worden aangepakt.

De snel voortschrijdende capaciteiten van drones vormen een groeiend veiligheidsrisico. De afgelopen jaren zijn er plannen ontdekt om te trachten drones in te zetten voor terroristische aanslagen[5]. Er zijn ook verdachte drones waargenomen in de buurt van kritieke infrastructuur, zoals energievoorzieningen, luchthavens en havens, wat wijst op mogelijk misbruik van drones voor het verzamelen van vijandige informatie. Drones worden gebruikt door criminelen bij smokkel over landsgrenzen of andere illegale activiteiten, waaronder drugshandel. Drones kunnen bovendien een bron van cyberrisico's zijn,

[2] Een in 2022 door de Commissie uitgevoerde interne diepgaande beoordeling van autonome systemen.

[3] Mededeling betreffende de EU-strategie voor de veiligheidsunie (COM(2020) 605 final van 24 juli 2020).

[4] Een terrorismebestrijdingsagenda voor de EU: anticiperen, voorkomen, beschermen en reageren (COM(2020) 795 final van 9 december 2020).

[5] Enkele voorbeelden zijn: i) het plan van een geïnspireerde jihadist die in oktober 2022 door een Spaanse rechtbank werd veroordeeld omdat hij van plan was tijdens een grote voetbalwedstrijd een stadion aan te vallen met een drone vol explosieven; en ii) een Belgisch staatsburger die werd veroordeeld voor een poging tot een bomaanslag met behulp van drones tegen een gevangenis.

bijvoorbeeld als ze worden gebruikt voor digitale verkenning. Bedreigingen van drones zijn niet alleen een technisch probleem. Tegenwoordig kunnen de meeste drones die voor civiele doeleinden zijn ontworpen, worden gedetecteerd en geïdentificeerd, maar het is nog steeds een hele uitdaging om ze aan te pakken of te neutraliseren (om ze onder controle te krijgen, ze veilig te laten landen of neer te schieten), vaak vanwege het ontbreken van wettelijke toestemming om dit te doen. Dit geldt met name voor particuliere exploitanten van kritieke infrastructuur. Het tegengaan van de dreigingen van drones moet daarom in aanmerking worden genomen bij toekomstige risicobeoordelingen in het kader van de richtlijn betreffende de weerbaarheid van kritieke entiteiten[6].

Het dreigingsbeeld wordt nog duidelijker als we kijken naar incidenten in landen in de buurt van de EU en in andere delen van de wereld. Drones blijken een kostenefficiënt en doelmatig platform te zijn voor tweeërlei gebruik, dat de defensie-innovatie in de Russische oorlog tegen Oekraïne heeft gestimuleerd. Het gebruik van voor civiele doeleinden bedoelde drones voor destructieve aanvallen, zelfs in andere gewapende conflicten (zoals in Jemen of Syrië), is een verschijnsel met waarschijnlijke gevolgen voor de interne veiligheid van de EU. De werkwijze van terroristische groeperingen en de verbeterde vaardigheden bij het gebruik van "off-the-shelf drones" kunnen onze grenzen bereiken en een bedreiging vormen. Hetzelfde geldt voor het gebruik van drones voor doelgerichte moordpogingen[7].

Counter-drone-oplossingen zijn echter niet alleen nodig tegen gericht kwaadwillig gebruik. Ze zijn ook nodig om incidenten veroorzaakt door nalatigheid of roekeloosheid te voorkomen. De meeste dronegebruikers in de EU (met name bevoegde professionele piloten op afstand of georganiseerde vrijetijdspiloten) voldoen aan de bestaande regels, voorschriften en technische beperkingen. Toch zijn onwetende, onvoorzichtige en criminele dronegebruikers verantwoordelijk voor veel gevaarlijke incidenten met drones in de gehele EU. Grootschalige openbare evenementen zijn bijzonder kwetsbaar voor dergelijke verstoringen, evenals bepaalde kritieke sectoren zoals het luchtvervoer. Bovendien kan het onrechtmatige gebruik van drones ook gevolgen hebben voor de persoonlijke veiligheid en het recht op privacy van individuele leden van het publiek, met name wanneer drones in woonwijken worden gebruikt.

C. Scherpere aandacht voor technologische ontwikkelingen

Het beschermen van de maatschappij tegen kwaadwillige en niet-coöperatieve drones vereist ook toegang tot betaalbare en betrouwbare tegenmaatregelen waarmee flexibele oplossingen mogelijk zijn. De oplossingen hebben doorgaans betrekking op de drie aspecten van opsporing, tracering en identificatie, terwijl overheidsinstanties ook belang hebben bij twee aanvullende aspecten: neutralisatie en forensisch onderzoek.

Zowel op het gebied van defensie als op het gebied van civiele veiligheid worden al counter-drone-oplossingen ontwikkeld en getest. Hun toegang tot de markt en de acceptatie ervan door eindgebruikers kunnen worden vergemakkelijkt door een overkoepelend EU-kader voor de bestrijding van drones, zoals dat in deze mededeling wordt bevorderd. Vanwege de grote verscheidenheid aan mogelijke operationele scenario's en omgevingen is het echter niet mogelijk om een enkele, gestandaardiseerde aanpak te hanteren voor het uitvoeren van maatregelen tegen drones.

---

[6] Richtlijn (EU) 2022/2557 van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten (PB 2022 L 333, blz. 164).

[7] Voorbeelden hiervan zijn een mislukte poging om de president van Venezuela te vermoorden en Mexicaanse drugskartels die drones inzetten tegen leden van andere criminele organisaties.

Maatregelen tegen drones moeten daarom worden aangepast aan verschillende behoeften en verschillende operationele omstandigheden. Vanuit het perspectief van de autoriteiten die verantwoordelijk zijn voor de binnenlandse veiligheid, kunnen er situaties zijn waarin de volledige fysieke vernietiging van een drone de voorkeur heeft en de enige optie is, bijvoorbeeld om een dreigende aanval op personen of infrastructuur te voorkomen. In andere gevallen, zoals bij crimineel gebruik of het op vijandige wijze verzamelen van informatie, is het van groot belang dat controle over de drone wordt verkregen om deze zo intact mogelijk te laten landen, zodat een optimaal forensisch onderzoek mogelijk is. Dit omvat de behoefte aan geavanceerde cyberoplossingen om de controle van het besturingssysteem van een drone over te nemen.

Een van de technologische trends die moet worden gemonitord en actief moet worden gebruikt, is de ontwikkeling van sensoren voor een nauwkeurigere opsporing van drones. Bestaande sensorcapaciteiten kunnen verder worden ontwikkeld, niet alleen om een drone op te sporen, maar ook om de dreiging die deze vormt, te beoordelen door middel van vluchtpatroonanalyse, detectie van payload en van apparatuur. Sensoren en detectiesystemen moeten kunnen omgaan met de veranderende vormen en capaciteiten van drones (snelheid, wendbaarheid, mogelijkheid om lokmiddelen in te zetten enz.). De capaciteit van overheidsinstanties en particuliere exploitanten van kritieke infrastructuur om gegevens van deze sensoren te analyseren, wordt steeds belangrijker. Kunstmatige intelligentie speelt ook een rol, bijvoorbeeld door automatisch waarschuwingen te genereren, risico's te berekenen of routes of landingsplaatsen te voorspellen. Nieuwe trends in dronemarkten moeten dus continu worden gemonitord en geïntegreerd in counter-drone-oplossingen. De monitoring van deze technologische ontwikkelingen moet de autoriteiten in de EU in staat stellen prioriteiten voor investeringen vast te stellen en de meest geschikte ontwikkelingen te ondersteunen om tegemoet te komen aan de operationele behoeften die de rechtshandhavingsautoriteiten van de lidstaten en particuliere exploitanten naar voren brengen.

Wat aanpak en neutralisatie betreft, zijn verdere tests nodig met betrekking tot technologieën die geschikt zijn voor verschillende omgevingen en scenario's. Op het gebied van defensie zijn oplossingen gevonden om drones fysiek te vernietigen of al in de lucht volledig over te nemen, waardoor er minder brokstukken ontstaan die mensen kunnen verwonden of schade aan voorwerpen kunnen aanbrengen. Dit omvat gerichte energie in de vorm van hoogenergetische lasers, evenals het gebruik van krachtige radiofrequentie- en netopnamesystemen en digitale hulpmiddelen om controle te krijgen over niet-coöperatieve drones.

Voor rechtshandhaving en onderzoek zou het bijzonder nuttig zijn om een dronebedreiging te kunnen neutraliseren door de controle over het besturingssysteem over te nemen en de drone veilig te laten landen, zodat autoriteiten en onderzoekers de best mogelijke toegang hebben tot potentieel fysiek en digitaal bewijsmateriaal. Daarom moet een breed spectrum van verschillende oplossingen beschikbaar en gevalideerd zijn voor verschillende doeleinden op het gebied van interne beveiliging. Het is daarom noodzakelijk om een echt innovatieve marktomgeving te creëren voor counter-drone-oplossingen die voldoen aan de behoeften van de civiele veiligheid. Anders is het onwaarschijnlijk dat de ontwikkelingen op het gebied van counter-drone-oplossingen gelijke tred zullen houden met de toenemende aantallen en capaciteiten van de drones zelf. Het is ook van essentieel belang om deze markt te structureren en te segmenteren om de relevante autoriteiten te helpen de oplossingen te vinden die het best aan hun behoeften voldoen.

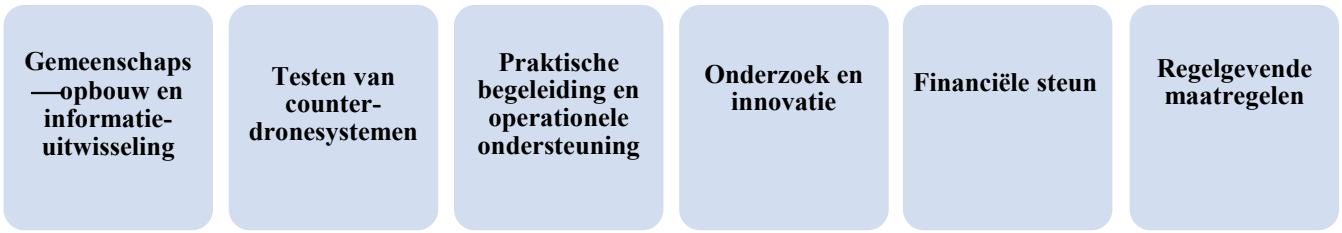
Daarnaast is het belangrijk om zogenaamde counter-counter-dronesystemen die door criminelen worden gebruikt, te blijven monitoren. Counter-counter-dronesystemen zijn apparaten die ofwel op de drone zijn gemonteerd ofwel vanaf de grond worden ingezet en zijn ontworpen om specifieke maatregelen tegen drones te belemmeren.

Ten slotte zijn er ook veel counter-dronesystemen ontwikkeld voor defensiedoeleinden. Hoewel de vereisten verschillend zijn, hebben zij vaak gemeenschappelijke kenmerken en technologieën met systemen voor civiele doeleinden, waardoor nauwe samenwerking met defensie nodig is.

Dit evoluerende technologische landschap vereist ook een consistent en voortdurend bijgewerkt regelgevingskader voor het gebruik van counter-dronesystemen.

II. HET FORMULEREN VAN EEN COUNTER-DRONEBELEID VAN DE EU

De Commissie werkt sinds 2016, toen de eerste EU-workshop voor de bestrijding van drones plaatsvond, samen met de lidstaten en andere belanghebbenden aan de potentiële dreiging van drones. Sindsdien is een breed spectrum van initiatieven opgezet om gemeenschapsopbouw, informatie-uitwisseling, de ontwikkeling van beste praktijken en de specifieke financiering van projecten te vergemakkelijken. Als resultaat van gesprekken met deskundigen uit de lidstaten blijft de Commissie deze lopende initiatieven ondersteunen en tegelijkertijd nieuwe werkterreinen verder ontwikkelen en integreren om een volwaardig EU-beleid voor de bestrijding van drones op te stellen. Deze werkzaamheden zullen bestaan uit de volgende zes kernactiviteiten:



A. Gemeenschapsopbouw en informatie-uitwisseling

Inmiddels werken een groot aantal verschillende netwerken en actoren op EU-niveau aan counter-drone-oplossingen. Daarom bestaat de behoefte hun toekomstige activiteiten in beleids-, technisch en operationeel opzicht te stroomlijnen en te sturen met het oog op: i) het opbouwen van functionerende gemeenschappen van belanghebbenden; ii) het zorgen voor een doeltreffende uitwisseling van informatie en beste praktijken; en iii) het vermijden van dubbel werk.

De Commissie zal bestaande initiatieven op technisch niveau stimuleren en daarbij een **deskundigengroep voor de bestrijding van drones** van de Commissie oprichten om op beleidsniveau advies te verstrekken. Deze deskundigengroep levert strategische input voor verschillende beleidsmaatregelen op EU-niveau die relevant zijn voor de bestrijding van drones, zoals op het gebied van interne veiligheid, grensbeheer of de weerbaarheid van kritieke infrastructuur. Daartoe werkt de deskundigengroep samen met andere deskundigengroepen en, in voorkomend geval, met relevante werkgroepen van de Raad.

Regelmatig vinden workshops en bijeenkomsten van deskundigen over oplossingen en beleid tegen drones plaats. Deze brengen beleidsmakers, technische deskundigen en onderzoekers van de Commissie, lidstaten, andere EU-instellingen, EU-agentschappen, door de EU gefinancierde projecten, internationale organisaties en partnerlanden samen. Deze activiteiten hebben geleid tot de voortdurende betrokkenheid van alle belanghebbenden, waardoor hun operationele en praktische samenwerking aanzienlijk is vergemakkelijkt. Daartoe heeft de Commissie de **Counter-UAS-informatiehub**[8] opgericht, die momenteel meer dan 300 leden telt. Dit online platform wordt regelmatig bijgewerkt en bevat verschillende informatiebronnen, zoals resultaten van relevante door de EU gefinancierde projecten, presentaties, rapporten en een halfjaarlijkse nieuwsbrief.

Een ander belangrijk onderdeel van gemeenschapsopbouw en informatie-uitwisseling, met name voor de operationele behoeften van de rechtshandhavingsinstanties, vindt plaats in het kader van de door de EU gefinancierde **Europese rechtshandhavingsnetwerken**. Onder meer de volgende netwerken zijn begonnen met hun eigen activiteiten om dreigingen van drones tegen te gaan: het Europees netwerk van technologische diensten voor wetshandhaving (Enlets); het EU-netwerk voor politie- en grenswachteenheden op luchthavens (Airpol); het EU-netwerk van speciale interventie-eenheden (Atlas); en het netwerk voor beveiliging tegen hoge risico's van de EU. De nieuw opgerichte werkgroep rechtshandhavingsnetwerken is een door de Commissie gefinancierd initiatief van DG HOME om de samenwerking tussen politienetwerken te bevorderen[9]. In een speciale subwerkgroep worden activiteiten op het gebied van de bestrijding van drones op elkaar afgestemd.

Het **Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA)** heeft niet-bindende richtsnoeren opgesteld die autoriteiten en luchthavens helpen bij de voorbereiding en reactie op drone-incidenten en bij het herstel van dergelijke incidenten[10]. Om geïnformeerde ondersteuningsactiviteiten en beleidsvorming op EU-niveau te bevorderen, is het essentieel dat er betrouwbare en gedetailleerde informatie wordt uitgewisseld over incidenten met drones in de EU, naast de uitwisselingen die al

[8] Met behulp van het CIRCABC-platform van de EU, dat wordt ondersteund door het ISA²-programma van de Europese Commissie, dat interoperabiliteitsoplossingen voor Europese overheidsdiensten bevordert.

[9] De (informele) werkgroep rechtshandhavingsnetwerken (Lenwg) wordt voorgezeten door de Commissie en is op 20 maart 2023 voor het eerst bijeengekomen om een betere samenwerking tussen de door DG HOME gefinancierde netwerken te bevorderen. Na een evaluatieperiode van twaalf maanden kan de Lenwg worden omgevormd tot een officiële deskundigengroep van de Commissie.

[10] Het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA) heeft in maart 2021 een reeks richtsnoeren gepubliceerd voor de beheersing van drone-incidenten op luchthavens: Drone Incident Management at Aerodromes.

plaatsvinden over specifieke kritieke gebieden zoals luchthavens. Met volledige inachtneming van de vertrouwelijkheid van onderzoeken kan de uitwisseling van informatie aanzienlijk worden verbeterd ten aanzien van: i) methoden die worden gebruikt door exploitanten van niet-coöperatieve drones; ii) specifieke dreigingspatronen; en iii) in kaart gebrachte potentiële risico's. De Commissie heeft de lidstaten een sjabloon verstrekt voor de rapportage van drone-incidenten om de uitwisseling van dergelijke informatie over incidenten te vergemakkelijken en te harmoniseren. Ook onderzoekt de Commissie de mogelijkheid om een **digitaal platform met informatie over drone-incidenten** op te zetten voor gebruik door relevante overheidsinstanties om de kwaliteit en frequentie van de informatie-uitwisseling verder te verhogen. Het platform kan worden ingezet om belangrijke veiligheidsincidenten met drones in de EU naar behoren te inventariseren en bij te houden. Dit kan ook de cyberdimensie omvatten, aangezien drones niet alleen worden gebruikt voor visuele verkenning, maar ook voor digitale verkenning. Dit platform is in overeenstemming met de bestaande rapportageverplichtingen op grond van Verordening (EU) nr. 376/2014[11] en geen duplicatie van bestaande inspanningen.

De Commissie organiseert ook regelmatig besloten bijeenkomsten om de uitwisseling van lessen uit incidenten in een passende vorm te bevorderen.

Kernacties voor gemeenschapsopbouw en informatie-uitwisseling

- **De Commissie richt een deskundigengroep op, bestaande uit deskundigen uit de lidstaten en andere belanghebbenden op het gebied van activiteiten voor de bestrijding van drones.**
- **De Commissie onderzoekt de mogelijkheid om een digitaal platform te ontwikkelen met informatie over drone-incidenten.**
- **De Commissie organiseert regelmatig bijeenkomsten om de uitwisseling van geclassificeerde informatie tussen de lidstaten over belangrijke veiligheidsincidenten waarbij drones worden gebruikt, te vergemakkelijken.**

B. Testen van counter-dronesystemen: oplossingen inventariseren en testen

De lidstaten en lokale autoriteiten kunnen kiezen uit een breed spectrum van commerciële cyber- en niet-cyberoplossingen tegen drones die op de markt verkrijgbaar zijn. Het maken van deze keuze is een uitdaging, vooral voor lokale entiteiten die niet over voldoende technische capaciteiten beschikken. De Commissie helpt de autoriteiten van de lidstaten de juiste keuze te maken voor hun operationele behoeften door advies en begeleiding te verstrekken via de bijzondere deskundigengroep voor de bestrijding van drones en het werk van het Gemeenschappelijk Centrum voor onderzoek (JRC) van de Commissie.

In 2019 zijn activiteiten op EU-niveau gestart om systemen tegen drones te testen. Ze hebben tot doel een gemeenschappelijke methode te ontwikkelen voor het evalueren van systemen die door rechtshandhavingsinstanties en andere overheidsinstanties kunnen worden gebruikt om potentieel kwaadaardige drones op te sporen, te traceren en te identificeren. Een centrale pijler van deze activiteiten is het project "Courageous"[12] (2021-2024), dat wordt gefinancierd door het Fonds voor interne veiligheid – Politie (ISF Police) van de EU. Courageous wordt geleid door de Belgische Koninklijke Militaire School en de doelen van het project zijn: i) het identificeren van relevante standaardscenario's voor het testen van

[11] Verordening (EU) 376/2014 van het Europees Parlement en de Raad van 3 april 2014 inzake het melden, onderzoeken en opvolgen van voorvallen in de burgerluchtvaart (PB L 122 van 24.4.2014, blz. 18).

[12] https://courageous-isf.eu/

counter-dronesystemen; ii) het ontwikkelen van functionele en prestatie-eisen; en iii) het ontwikkelen van een testmethode. Het project test ook de prestaties van sensoren en geïntegreerde systemen. De resultaten van het project worden voortdurend gedeeld met de lidstaten, geselecteerde partnerlanden en internationale organisaties. Na de voltooiing van het project zullen de Commissie en het Courageous-consortium de lidstaten opties voorleggen om de duurzaamheid van het project te waarborgen en een aanbeveling doen voor een **methode voor testfaciliteiten tegen drones** in de lidstaten.

De technologische ontwikkelingen die relevant zijn voor counter-dronesystemen gaan snel. Daarom moeten testactiviteiten worden aangevuld met het voortdurend volgen van trends om zowel de meest veelbelovende oplossingen als mogelijke nieuwe uitdagingen voor de ontwikkeling van systemen tegen drones op te sporen. Het JRC heeft capaciteit opgebouwd om deze monitoring uit te voeren en deze nieuwe uitdagingen te onderkennen. Dit komt de lidstaten ten goede en levert waardevolle input voor testinitiatieven op EU-niveau. De informatie zal worden gedeeld via passende kanalen, met name de deskundigengroep.

Standaardisatie is een instrument om technologische oplossingen te harmoniseren. In het Courageous-project is specifiek advies opgesteld over pre-standaardisatie, op basis waarvan de haalbaarheid en de noodzaak van het invoeren van normalisatieprocessen verder kan worden beoordeeld. Op EU-niveau is er goede vooruitgang geboekt met de ontwikkeling van vrijwillige prestatie-eisen voor detectieapparatuur buiten de luchtvaart (bijvoorbeeld voor röntgenapparatuur en metaaldetectoren[13]). Samen met deskundigen uit de lidstaten en de industrie zal de Commissie nu ook **vrijwillige prestatie-eisen** ontwikkelen voor systemen tegen drones, in voorkomend geval in samenhang met de bepalingen van de cyberbeveiligingsverordening[14]. Het opzetten van een certificeringsproces voor counter-dronesystemen moet een doelstelling op middellange termijn blijven. In voorkomend geval zullen ook hybride normen voor civiele bescherming worden overwogen.

Een ander belangrijk element is het standaardiseren en certificeren van de cyberbeveiliging van counter-dronesystemen, vooral als deze worden geleverd door leveranciers uit niet-EU-landen. In dit stadium blijft er onzekerheid bestaan over hoe goed de gegevens die door bepaalde detectiesystemen worden verzameld, worden beschermd. Daarnaast is het belangrijk om het hacken en misbruiken van counter-dronesystemen zoveel mogelijk te voorkomen door de cyberweerbaarheid van hun onderdelen te waarborgen.

In september 2022 heeft de Commissie een voorstel voor een verordening betreffende cyberweerbaarheid[15] vastgesteld, met als doel algemene cyberbeveiligingsregels op te stellen voor producten met digitale elementen — zowel hardware als software — die op de eengemaakte markt worden gebracht. De voorgestelde nieuwe verordening heeft tot doel verplichte cyberbeveiligingsvereisten voor deze producten in te voeren. Deze vereisten omvatten cyberbeveiliging door ontwerp en door standaardinstellingen, evenals vereisten om kwetsbaarheden aan te pakken. In het voorstel van de Commissie zouden dronesystemen die niet uitsluitend voor doeleinden van nationale veiligheid of voor militaire doeleinden zijn ontwikkeld, en die nog niet zijn gecertificeerd overeenkomstig Verordening (EU) 2018/1139, onder deze nieuwe regels vallen als producten met digitale elementen, met uitzondering van systemen die uitsluitend zijn ontwikkeld voor doeleinden van nationale veiligheid of voor militaire doeleinden.

[13] Aanbeveling van de Commissie inzake vrijwillig in acht te nemen prestatie-eisen voor röntgenapparatuur voor gebruik in openbare ruimten (C(2022) 4179 final).

[14] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie.

[15] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020 (COM(2022) 454 final).

Kernacties voor het testen van counter-dronesystemen

- **De Commissie werkt aan de invoering van een geharmoniseerde testmethode voor counter-dronesystemen op basis van de resultaten van het Courageous-project.**
- **Het JRC stelt jaarlijks een verslag op over de technische ontwikkelingen op het gebied van technologie tegen drones.**
- **De Commissie zal, in samenwerking met relevante deskundigengroepen, zoals de wetshandhavingsnetwerken ENLETS, HRSN en Airpol, een reeks vrijwillige prestatie-eisen voor counter-dronesystemen ontwikkelen.**

C. Praktische begeleiding en operationele ondersteuning

In een aantal publicaties van het JRC is de aanpak van dreigingen van niet-coöperatieve drones al als een prioriteit aangemerkt, zoals in richtsnoeren die gericht zijn op de perimeterbeveiliging van gebouwen[16] en in het specifieke onderzoek naar door drones vervoerde explosieve ladingen[17]. Bovendien wordt in de recente publicatie[18] over het concept van beveiliging door ontwerp het belang benadrukt dat de integratie van proportionele, passende en multifunctionele beschermingsmaatregelen vanaf het begin van de plannings- en ontwerpfase van een project op doordachte manier moet plaatsvinden, waarbij maatregelen worden opgenomen om aanvallen met gebruik van drones tegen te gaan.

Verder biedt de handleiding van de EASA over de beheersing van drone-incidenten op luchthavens richtsnoeren voor de ontwikkeling van passende regelingen en procedures voor een incidentresponssysteem op luchthavens dat snel, effectief en proportioneel is. Op deze manier kunnen het stilleggen van het luchtverkeer of de sluiting van het luchtruim of de start- en landingsbanen worden vermeden of tot een minimum worden beperkt en blijft een sluiting van luchthavens een laatste redmiddel. Het werk van de EASA sluit aan bij de richtsnoeren van de Internationale Burgerluchtvaartorganisatie op het gebied van luchtvaartbeveiliging[19].

Het JRC heeft twee nieuwe handboeken ontwikkeld:

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS protection of Critical Infrastructure and Public Space - A five Phase approach for C-UAS stakeholders* **(**Handboek over bescherming van kritieke infrastructuur en openbare ruimten tegen UAS - Een vijffasenaanpak voor C-UAS-belanghebbenden)

- ***Protection against Unmanned Aircraft Systems:*** *Handbook on UAS Risk Assessment and Principles for Physical Hardening of Buildings and Sites* (Handboek over UAS-risicobeoordeling en beginselen voor de fysieke verharding van gebouwen en locaties)

[16] Karlos, V. en Larcher, M., Guideline - Building Perimeter Protection, EUR 30346 EN, *Bureau voor publicaties van de Europese Unie*, Luxemburg, 2020.

[17] De dreiging van UAS die met explosieven zijn geladen, is onderzocht door het JRC in: Larcher, M., Karlos, V., Valsamos, G., Solomos, G., "Scenario study: drones carrying explosives", JRC107683, 2018.

[18] Europese Commissie, "Security by Design: Protection of public spaces from terrorist attacks", JRC131172, 2022.

[19] De Aviation Security Manual (Doc 8973 – vertrouwelijk) van de ICAO ondersteunt de lidstaten bij de uitvoering van bijlage 17 bij het Verdrag van Chicago met richtsnoeren voor de toepassing van de normen en aanbevolen praktijken (SARP's) Aviation Security Manual.

Op het gebied van **opleiding** heeft het door de EU gefinancierde project DroneWise[20] een pakket van commando-, controle- en coördinatiestrategieën tegen drones ontwikkeld voor hulpdiensten. Het project heeft ook tien opleidingsmodules, een handboek en een online opleidingsportaal opgeleverd. Deze opleidingsmodules zijn geïntegreerd in het curriculum van Cepol, het Agentschap van de Europese Unie voor opleiding op het gebied van rechtshandhaving. Het Skyfall-project is ander ISF-project waarin counter-drone-opleidingen zijn ontwikkeld. Het is nodig om de beschikbare opleidingen verder uit te breiden naar particuliere beveiligingsbedrijven, met name ondernemingen die verantwoordelijk zijn voor de bescherming van kritieke infrastructuur.

Het **EU-programma voor veiligheidsadviseurs (EU PSA)**[21] heeft een afdeling over activiteiten tegen drones, met: i) een specifieke kwetsbaarheidsbeoordeling voor voorzieningen en infrastructuur met een hoog risico; ii) praktisch advies over hoe om te gaan met de dreiging van drones; en iii) praktisch advies over hoe om te gaan met de inzet van drone-opsporingsapparatuur tijdens evenementen met een hoog risico. De Commissie zal onderzoeken of het nodig is een EU-pool van apparatuur voor de bestrijding van drones op te zetten die de lidstaten bij grootschalige evenementen kunnen gebruiken.

Oefeningen zoals die welke in het kader van het netwerk voor rechtshandhaving op EU-niveau worden georganiseerd, dragen bij tot de operationele paraatheid op verschillende gebieden van de interne veiligheid. In voorkomend geval zal de Commissie met de relevante netwerken samenwerken om in toekomstige oefeningen counter-drone-elementen op te nemen. Dit zal helpen om de kennis en de uitwisseling van beste praktijken verder te vergroten, waarbij gebruik wordt gemaakt van verschillende oplossingen. Een vereiste voor een doeltreffende respons op dreigingen die uitgaan van drones, is dat er betrouwbare en veilige communicatie tussen de verschillende autoriteiten moet zijn. Daarom maakt de bestrijding van dreigingen van drones deel uit van de toekomstige planning van oefeningen als onderdeel van het door de EU gefinancierde voorbereidingsproject BroadEU.net, waarbij de basis van het toekomstige EU-systeem voor kritieke communicatie wordt getest[22]. Bovendien kunnen gezamenlijke oefeningen worden gehouden, waarbij deskundigen op het gebied van cyberbeveiliging en dronebeveiliging de cyberrisico's van drones toelichten, evenals digitale oplossingen om drones te neutraliseren.

Kernacties voor praktische begeleiding en operationele ondersteuning

- **Het JRC publiceert twee handboeken als onderdeel van het counter-dronepakket.**
- **De Commissie ondersteunt, in samenwerking met de relevante agentschappen, de uitbreiding van bestaande dronebestrijdingsopleidingen naar de particuliere beveiligingssector.**
- **De Commissie integreert, in samenwerking met de rechtshandhavingsnetwerken, onderdelen voor de bestrijding van drones in de planning van oefenoperaties.**

[20] https://dronewise-project.eu/

[21] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en

[22] Het EU-systeem voor kritieke communicatie zorgt voor een veilige breedbandinfrastructuur om de grensoverschrijdende interoperabiliteit van de communicatiesystemen die worden gebruikt door rechtshandhavers en hulpdiensten in het Schengengebied, te waarborgen.

D. Onderzoek en innovatie

De EU financiert haar programma voor veiligheidsonderzoek voort als onderdeel van **Horizon Europa (2021-2027)**[23]. Dit programma voor veiligheidsonderzoek vertegenwoordigt ongeveer 50 % van de totale overheidsfinanciering die in de EU en haar lidstaten wordt geïnvesteerd op het gebied van veiligheid. Als strategische bijdrage aan verschillende prioriteiten van het veiligheidsbeleid van de EU is in dit veiligheidsonderzoek ook al een begin gemaakt met het aanpakken van de dreigingen van drones. Bekende voorbeelden zijn onder meer Aladdin, met oplossingen voor het opsporen en neutraliseren van drones in beperkt toegankelijke gebieden[24], of 7SHIELD, waarin onderzoek is gedaan naar de ontwikkeling van counter-drone-oplossingen voor de grondsegmenten van kritieke infrastructuur in de ruimte. In het ALFA-project is een systeem ontwikkeld voor het opsporen en traceren van drones die voor smokkel worden gebruikt[25]. Deze onderzoeks- en innovatie-initiatieven kunnen in het kader van Horizon Europa worden voortgezet, gevalideerd of aangevuld met activiteiten die met steun van het ISF Police worden ondernomen.

In de toekomst zal de Commissie de meer systematische uitwisseling van relevante projectresultaten met relevante belanghebbenden vergemakkelijken, onder meer via de gemeenschap voor Europees onderzoek en innovatie op het gebied van veiligheid[26]. Dit zorgt voor een verdere versterking van de specifieke gegevensuitwisseling. Hiermee kunnen ook efficiënter de behoeften van gebruikers worden verzameld en aan de industrie worden doorgegeven om innovatie te stimuleren. Bovendien helpt de systematische uitwisseling van projectresultaten een gestructureerde dialoog met de lidstaten en belanghebbenden mogelijk te maken om veelbelovende technologieën, instrumenten en oplossingen in kaart te brengen die door een groep autoriteiten van de lidstaten kunnen worden gebruikt. In dat verband beoordeelt de Commissie samen met de lidstaten[27] de mogelijkheid om: i) counter-drone-oplossingen een specifiek onderzoeksonderwerp te maken in de toekomstige werkprogramma's van Horizon Europa; en ii) specifieke innovatieve systemen via precommerciële inkoop[28] te ondersteunen. Dit is volledig in lijn met de vermogensgerichte benadering die wordt beschreven in het Werkdocument van de diensten van de Commissie "Meer veiligheid dankzij onderzoek en innovatie"[29].

Het is van cruciaal belang de synergieën in counter-drone-oplossingen tussen de Europese civiele veiligheids-, defensie- en ruimtevaartindustrie te versterken. Het doel hiervan is het bevorderen van synergieën in drone- en counter-dronetechnologieën tussen de drie sectoren[30]. In de praktijk betekent het

---

[23] Voorheen, tot eind 2020, werden veiligheidsonderzoek en -innovatie gefinancierd in het kader van Horizon 2020 en het zevende kaderprogramma.

[24] https://cordis.europa.eu/project/id/740859

[25] ALFA is ook de basis voor het ISF-project Courageous en zijn testactiviteiten.

[26] De gemeenschap voor Europees onderzoek en innovatie op het gebied van veiligheid (CERIS) brengt belanghebbenden op het gebied van veiligheidsonderzoek samen, variërend van beleidsmakers en eindgebruikers, de academische wereld en de industrie tot belanghebbenden in de civiele veiligheid: https://home-affairs.ec.europa.eu/networks/ceris-community-european-research-and-innovation-security_en

[27] In de samenstelling van het programmacomité van Horizon Europa "Civiele veiligheid voor de samenleving".

[28] Precommerciële inkoop (PCP) is een aanpak van overheidsopdrachten voor onderzoeks- en ontwikkelingsdiensten (O&O) die wordt beschreven in de PCP-mededeling (COM(2007) 799 final van 14.12.2007). Het is een belangrijk instrument om innovatie te stimuleren, omdat het de overheidssector in staat stelt de ontwikkeling van nieuwe oplossingen op zijn behoeften af te stemmen.

[29] Werkdocument van de diensten van de Commissie "Meer veiligheid dankzij onderzoek en innovatie" (SWD(2021) 422 final van 15.12.2021).

[30] SWD(2022) 362 van 10.11.2022. Zoals beschreven in het voortgangsverslag over de uitvoering van het actieplan inzake synergieën tussen de civiele bescherming en de ruimtevaartindustrie in het kader van actiepunt 9.

versterken van deze synergieën dat defensieprojecten kunnen profiteren van innovatieve ontwikkelingen in het civiele domein, terwijl civiele luchtvaart kan profiteren van ontwikkelingen op defensiegebied.

Het **Europees Defensiefonds (EDF)** en de daaraan voorafgaande programma's stimuleren en ondersteunen gezamenlijk, grensoverschrijdend onderzoek en ontwikkeling op defensiegebied. Het EDF vult de inspanningen van de lidstaten aan en versterkt de samenwerking tussen bedrijven en onderzoeksorganisaties, ongeacht hun omvang, van alle lidstaten in de EU. De voorafgaande programma's van het EDF hebben al projecten ter bestrijding van drones gefinancierd als onderdeel van defensieonderzoek en -ontwikkeling.

Het EDF-werkprogramma voor 2023 bevat een ontwikkelingsactie voor de bestrijding van drones[31], met een indicatief budget van 43 miljoen EUR. De actie is gericht op de ontwikkeling van hardware- of softwaremodules voor een uitgebreide mobiele oplossing ter bestrijding van een breed spectrum van drones, waaronder zwermen.

Het belangrijkste verwachte resultaat van de steun van het EDF op het gebied van de bestrijding van drones in de periode 2021-2027 is een ontwikkeld prototype van een counter-drone-oplossing in de aanloop naar mogelijke toekomstige gezamenlijke aanbestedingen op EU-niveau. Technologische uitdagingen op het gebied van counter-dronesystemen worden aangepakt via de EU-regeling voor defensie-innovatie (Eudis). Bovendien omvat de Eudis een onderdeel voor incubatoren voor tweeërlei gebruik om een betere samenwerking tussen de civiele en defensiedomeinen te bevorderen en om technologische doorontwikkeling en aanpassing te stimuleren.

Een andere belangrijke pijler voor innovatie, en specifiek voor toegepast onderzoek naar de manier waarop dreigingen van drones kunnen worden tegengegaan, is het werk van het JRC. Als onderdeel van het Drone C-UAS-project van het JRC beoordeelt het JRC actieve en passieve technologieën voor tegenmaatregelen, en hoe deze technologieën kunnen worden gebruikt om de veiligheid van openbare ruimten en kritieke infrastructuur te waarborgen.

Het JRC zet daarvoor als eerste stap een **levend lab** op om technologieën tegen drones te onderzoeken en hoe deze technologieën in de praktijk kunnen worden toegepast. De lab-opstelling omvat de planning, voorbereiding en uitvoering van een oplossing. Ook de opsporing, tracering, identificatie en neutralisatie van drones komen aan bod, naast de integratie van belanghebbenden en processen. De uitvoering van het levend lab omvat integratie met beheersystemen voor bemande en onbemande luchtvaart, met name U-space[32]. In het levend lab wordt ook onderzocht hoe machinelearning en kunstmatige intelligentie kunnen worden geïntegreerd om de algehele prestaties van oplossingen voor de bestrijding van drones te verbeteren.

Op middellange termijn wordt dit levend lab van het JRC ontwikkeld tot een **kenniscentrum voor de bestrijding van drones**.

[31] C(2023) 2296 Commission Implementing Decision of 29.3.2023 on the financing of the European Defence Fund established by Regulation (EU) 2021/697 of the European Parliament and the Council and the adoption of the work programme for 2023 - Part II (Uitvoeringsbesluit C(2023) 2296 van de Commissie van 29.3.2023 betreffende de financiering van het bij Verordening (EU) 2021/697 van het Europees Parlement en de Raad opgerichte Europees Defensiefonds en de vaststelling van het werkprogramma voor 2023 - deel II).

[32] Uitvoeringsverordening (EU) 2021/664 van de Commissie inzake een regelgevingskader voor U-space. De term "U-space" is vastgesteld om het beheer van onbemand luchtvaartuigverkeer te beschrijven om te zorgen voor veilige interactie met andere entiteiten die dezelfde ruimte gebruiken in stedelijke gebieden en op andere locaties.

Kernacties om onderzoek en innovatie optimaal in te zetten

- **De Commissie en de lidstaten beslissen over de toekomstige behoeften aan nieuwe counter-drone-oplossingen, die door relevante Europese onderzoeks- en innovatieprogramma's onderzocht kunnen worden, met name Horizon Europa.**
- **De Commissie en de lidstaten stellen een lijst van veelbelovende counter-drone-oplossingen op en beoordelen de haalbaarheid van precommerciële inkoop van een aantal van deze oplossingen.**
- **De Commissie brengt ideeën, technologieën en oplossingen in kaart om deze te integreren in de ontwikkeling van defensiecapaciteiten, en ondersteunt projecten om deze ideeën, technologieën en oplossingen in de civiele sectoren te verspreiden.**
- **Het JRC richt een kenniscentrum ter bestrijding van drones op als verdere ontwikkeling van een levend lab.**

E. Financiële steun

De Commissie blijft financiële steun verlenen aan relevante activiteiten tegen drones, voornamelijk via het ISF, maar ook in het kader van het instrument voor financiële steun voor grensbeheer en visumbeleid (BMVI) en het Horizon Europa-programma (voor activiteiten op het gebied van onderzoek en innovatie).

De thematische faciliteit van het ISF ondersteunt: i) de Europese rechtshandhavingsnetwerken; ii) de gerelateerde werkzaamheden van het JRC; iii) de nieuwe counter-dronedeskundigengroep; en iv) het opzetten van een platform voor informatie-uitwisseling. De Commissie financiert nu al projecten voor het testen en valideren van systemen voor het opsporen en lokaliseren van drones die onrechtmatig de buitengrenzen van de EU overschrijden. Die projecten zijn gebaseerd op resultaten van eerdere door de EU gefinancierde onderzoeksprojecten[33].

In het kader van de thematische faciliteit van het ISF zal de Commissie in de eerste helft van 2024 een **oproep tot het indienen van voorstellen** doen die specifiek gericht is op de ondersteuning van de inzet van counter-drone-oplossingen met een hoog toepassingspotentieel.

De lidstaten worden aangemoedigd om deze mededeling uit te voeren en via hun ISF-programma's gebruik te maken van de resultaten van door de EU gefinancierd onderzoek naar counter-drone-oplossingen.

[33] Voorbeelden hiervan zijn projecten die zijn gefinancierd in het kader van de specifieke BMVI-acties op het gebied van: i) innovatie voor zee-/kust- en/of landsgrenzen; en ii) Frontex. Van de projecten die worden gefinancierd in het kader van de specifieke actie inzake innovatie voor zee-/kust- en/of landsgrenzen, zijn er enkele gericht op het testen van innovatieve surveillancetechnologieën. Er is ook een specifieke actie voor de aankoop en beschikbaarstelling van uitrusting voor inzet door Europese grensautoriteiten om drones op te sporen en te lokaliseren die grenzen overschrijden in verband met illegale of criminele activiteiten. Deze specifieke actie stelt de lidstaten in staat twee counter-dronesystemen aan te kopen. De technische uitrusting die in het kader van de specifieke acties is aangekocht moet als EU-meerwaarde, op verzoek van Frontex in het kader van de jaarlijkse bilaterale onderhandelingen, gedurende een periode van maximaal vier maanden per jaar ter beschikking worden gesteld van Frontex voor gebruik in de gezamenlijke operaties.

Kernacties voor financiële steun

- **De Commissie doet een oproep tot het indienen van voorstellen over counter-drone-oplossingen in het kader van de thematische werkprogramma's van het ISF voor de periode 2026-2027.**
- **De lidstaten zullen worden aangemoedigd ten volle gebruik te maken van hun ISF-programma's voor 2021-2027 om efficiënte oplossingen voor het tegengaan van drones vast te stellen en uit te voeren.**

F. Onderzoek naar regelgevende maatregelen

Hoewel de EU het legitieme gebruik van drones heeft gereguleerd, zijn er op EU-niveau momenteel geen specifieke voorschriften voor de bestrijding van drones die een gemeenschappelijk geharmoniseerd kader vormen voor autoriteiten van de lidstaten, exploitanten en fabrikanten. De niet-bindende EASA-richtsnoeren ter bestrijding van drone-incidenten op luchthavens (waarnaar eerder in deze mededeling is verwezen) zijn door de sector positief ontvangen, maar zij zijn door hun adviserende karakter en beperkte toepassingsgebied onvoldoende om de dreiging van niet-coöperatieve drones te beperken. Aangezien de noodzaak om ongeoorloofd gebruik van drones doeltreffend te voorkomen voortdurend toeneemt, zal de Commissie, in nauwe samenwerking met deskundigen uit de lidstaten, de noodzaak van wetgevende of niet-wetgevende maatregelen in de toekomst verder analyseren. Daartoe zal de Commissie een specifieke **inventarisatie** starten om het huidige regelgevingslandschap in kaart te brengen. In dit onderzoek moet ook rekening worden gehouden met het ICAO-kader en de ontwikkelingen hierin, en met het feit dat regels ter bestrijding van de potentiële dreigingen van drones rechtmatige activiteiten, waaronder de activiteiten van georganiseerde vrijetijdspiloten, niet onnodig mogen belemmeren.

Luchthavens in de EU beschikken over gedetailleerde en uitgebreide beveiligingsregels die ook de dreiging van drones betreffen. De Commissie zal in samenwerking met de lidstaten, volgens een empirisch onderbouwde aanpak, **mogelijke aanvullende kwetsbaarheden in de bescherming tegen niet-coöperatieve drones in kaart brengen middels een veiligheidsrisicobeoordeling die wijzigingen in de regelgeving kan vereisen** om ervoor te zorgen dat luchtvaartautoriteiten en luchthavens weerbaarder zijn voor de risico's van drones.

In dit verband is een gestructureerde dialoog met de sector en met dronefabrikanten nodig over maatregelen inzake beveiliging door ontwerp (bijvoorbeeld robuuste systemen tegen spoofing, capaciteitsbeperkingen, het delen van communicatieprotocollen en updates voor counter-dronedatabases).

Kernacties voor het onderzoeken van regelgevende maatregelen

- **De Commissie initieert een inventarisatie-onderzoek om de behoeften op het gebied van regelgeving en de mogelijkheden om de wetgeving en procedures in de lidstaten te harmoniseren, in kaart te brengen.**
- **De Commissie volgt een empirisch onderbouwde aanpak om een risicobeoordeling van de beveiliging van de luchtvaart ten aanzien van drones uit te voeren om mogelijke bijkomende kwetsbaarheden van luchthavens te identificeren, hetgeen wijzigingen in de regelgeving zou kunnen vereisen.**
- **De Commissie gaat een gestructureerde dialoog aan met de sector over de noodzaak en de aard van mogelijke aanvullende specifieke maatregelen met betrekking tot de beveiliging van drones.**

III. VOLGENDE STAPPEN

Om ervoor te zorgen dat snelle technologische ontwikkelingen en het toenemende aantal drones niet leiden tot een ongecontroleerde toename van dreigingen die uitgaan van niet-coöperatieve drones, moet de samenwerking op EU-niveau worden geïntensiveerd, op basis van het alomvattende EU-beleid tegen drones dat in deze mededeling wordt uiteengezet. Daartoe worden de huidige activiteiten op EU-niveau voortgezet en aangevuld met de reeks kernacties die in deze mededeling zijn opgesomd en die in de komende jaren zullen worden uitgevoerd.

De activiteiten die in deze mededeling worden beschreven, betreffen de periode tot 2030. In 2027 zal via de deskundigengroep een tussentijdse inventarisatie plaatsvinden, en een volledige evaluatie van het counter-droneprogramma van de EU wordt uiterlijk tegen 2030 gepland.