EUROPESE
COMMISSIE

Straatsburg, 1.4.2025
COM(2025) 148 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE RAAD, HET EUROPEES ECONOMISCH EN SOCIAAL COMITÉ EN HET COMITÉ VAN DE REGIO'S

ProtectEU: een Europese strategie voor interne veiligheid

1. ProtectEU: een Europese strategie voor interne veiligheid

Veiligheid is het fundament waarop al onze vrijheden zijn gebaseerd. Democratie, de rechtsstaat, grondrechten, het welzijn van Europeanen, concurrentievermogen en welvaart zijn allemaal afhankelijk van ons vermogen om te voorzien in een fundamentele veiligheidsgarantie. In het nieuwe tijdperk van veiligheidsbedreigingen dat we nu doormaken, is het vermogen van de EU-lidstaten om de veiligheid van hun burgers te waarborgen meer dan ooit afhankelijk van een **eensgezinde Europese aanpak voor de bescherming van onze interne veiligheid**. In een veranderend geopolitiek landschap moet Europa zijn blijvende belofte van vrede gestand doen.

De eerste stappen om een Europees veiligheidsapparaat op te bouwen, zijn al gezet. De afgelopen tien jaar hebben we de Unie uitgerust met verbeterde collectieve mechanismen om actie te ondernemen op het gebied van rechtshandhaving en justitiële samenwerking, grensbeveiliging, de bestrijding van zware en georganiseerde criminaliteit, de bestrijding van terrorisme en gewelddadig extremisme en de bescherming van de fysieke en digitale kritieke infrastructuur van de EU. De correcte uitvoering van eerder vastgestelde wetgeving en eerder ontwikkeld beleid blijft cruciaal.

Gelet op de aard van de huidige dreigingen en het intrinsieke verband tussen de interne en externe veiligheid van de EU moeten wij verdere maatregelen treffen.

Het dreigingsbeeld ziet er grimmig uit. De scheidslijnen tussen **hybride dreigingen** en openlijke oorlogsvoering zijn vervaagd. Rusland voert een hybride online- en offlinecampagne tegen de EU en haar partners om de maatschappelijke cohesie en democratische processen te verstoren en te ondermijnen, en om de solidariteit van de EU met Oekraïne te testen. Vijandige buitenlandse staten en door de staat gesteunde actoren proberen onze kritieke infrastructuur en toeleveringsketens te infiltreren en te ontwrichten, gevoelige gegevens te bemachtigen en zichzelf te positioneren met het oog op maximale ontwrichting in de toekomst. Zij gebruiken misdaad als dienst en criminelen als handlangers. Bovendien maakt onze afhankelijkheid van derde landen op het gebied van toeleveringsketens ons kwetsbaarder voor hybride campagnes van vijandige staten.

Machtige **georganiseerde criminele groeperingen** breiden zich uit in Europa, worden online gevoed, infiltreren in onze economie en hebben gevolgen voor onze samenleving, zoals wordt benadrukt in de dreigingsevaluatie van de Europese Unie voor zware en georganiseerde criminaliteit (EU-Socta), die onlangs door Europol is gepresenteerd[1]. Als de georganiseerde misdaad eenmaal voet aan de grond heeft in een gemeenschap of economische sector, wordt het uitbannen ervan een haast onmogelijk opgave: een derde van de meest bedreigende criminele groeperingen is al meer dan tien jaar actief. Cryptovaluta en parallelle financiële systemen helpen hen om hun opbrengsten van misdrijven wit te wassen en te verbergen.

In Europa is nog steeds sprake van terroristische dreiging. Regionale crises buiten de EU brengen een domino-effect teweeg, waardoor terroristische actoren over het hele ideologische spectrum opnieuw gemotiveerd worden om leden te werven, in te zetten of hun capaciteiten op te bouwen. Zij richten hun inspanningen op het gebied van radicalisering en rekrutering specifiek op de meest kwetsbare bevolkingsgroepen en met name bepaalde jongeren. Zij vormen een inspiratie voor aanvallen door eenlingen en voor een toename van tegen het systeem gericht extremisme, dat als doel heeft de democratische rechtsorde te ontwrichten.

De snelle **technologische vooruitgang** biedt essentiële instrumenten om ons veiligheidsapparaat te verbeteren. Cyberaanvallen en buitenlandse informatiemanipulatie komen echter steeds vaker voor, waarbij gebruik wordt gemaakt van nieuwe technologieën

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

zoals artificiële intelligentie. Kinderen, jongeren en ouderen lopen een groot risico online en de verspreiding van haatzaaiende uitlatingen online vormt een bedreiging voor de vrijheid van meningsuiting en de sociale cohesie.

Ons leven is minder veilig geworden, en dit wordt in toenemende mate gevoeld door Europeanen, wier **perceptie van veiligheid en beveiliging in de EU** zodanig is uitgehold dat, wanneer hen gevraagd wordt naar de toekomst, 64 % zich zorgen maakt over de veiligheid van de EU[2]. Ook het bedrijfsleven maakt zich steeds meer zorgen; misinformatie en desinformatie, criminaliteit en illegale activiteiten en cyberspionage staan allemaal in de top tien van grootste risico's die zijn vastgesteld in het Global Risks Report 2025 van het Wereld Economisch Forum[3].

Europeanen **moeten hun leven kunnen leiden zonder angst**, op straat, thuis, in het openbaar, in de metro en op het internet. De bescherming van mensen, met name degenen die het kwetsbaarst zijn voor aanvallen, staat centraal in de werkzaamheden van de EU op het gebied van veiligheid. Kinderen, vrouwen en minderheden, waaronder Joodse en moslimgemeenschappen, worden vaak onevenredig zwaar door die aanvallen getroffen. Dit is van essentieel belang om veerkrachtige en hechte samenlevingen op te bouwen.

De Commissie werkt momenteel aan een **Europese strategie voor interne veiligheid** om dreigingen de komende jaren beter het hoofd te bieden. Met aangescherpte juridische instrumenten, nauwere samenwerking en meer informatie-uitwisseling zullen wij onze veerkracht vergroten, alsook het collectieve vermogen om te anticiperen op veiligheidsdreigingen, deze te voorkomen, op te sporen en er doeltreffend op te reageren. Een eensgezinde aanpak van interne veiligheid kan de lidstaten helpen om de kracht van technologie te benutten om de veiligheid te versterken en niet te verzwakken, en tegelijkertijd een veilige digitale ruimte voor iedereen te bevorderen. Daarnaast ondersteunt een dergelijke aanpak een gemeenschappelijke reactie van de lidstaten op mondiale politieke en economische verschuivingen die van invloed zijn op de interne veiligheid van de Unie.

Deze strategie is gebaseerd op **drie beginselen** en stelt de eerbiediging van de rechtsstaat en de grondrechten centraal.

Ten eerste wordt de ambitie van een cultuuromslag op het gebied van veiligheid vastgesteld. Wij hebben een **maatschappijbrede benadering** nodig waarbij alle burgers en belanghebbenden worden betrokken, met inbegrip van het maatschappelijk middenveld, onderzoeksinstellingen, de academische wereld en particuliere entiteiten. Voor de acties in het kader van de strategie wordt daarom waar mogelijk een geïntegreerde, multistakeholderbenadering gevolgd.

Ten tweede **moeten veiligheidsoverwegingen in alle wetgeving, beleid en programma's van de EU worden geïntegreerd en gemainstreamd**, met inbegrip van het externe optreden van de EU. Wetgeving, beleid en programma's moeten worden voorbereid, herzien en uitgevoerd vanuit het oogpunt van veiligheid, waarbij ervoor moet worden gezorgd dat de nodige veiligheidsoverwegingen worden aangepakt om een coherente en alomvattende aanpak van de veiligheid te bevorderen.

Tot slot zijn voor een veilig, beveiligd en veerkrachtig Europa **wezenlijke investeringen nodig van de EU, haar lidstaten en de particuliere sector**. De in deze strategie vastgestelde prioriteiten en acties vereisen voldoende personele en financiële middelen om de uitvoering ervan te waarborgen. Zoals uiteengezet in de mededeling over de weg naar het volgende

[2] Flash Eurobarometer FL550: EU Challenges and Priorities.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, blz. 17.

meerjarig financieel kader[4], zal Europa de overheidsuitgaven voor veiligheid moeten verhogen en onderzoek en investeringen op het gebied van veiligheid moeten bevorderen en zo zijn strategische autonomie moeten vergroten.

Deze strategie vormt een aanvulling op de **strategie voor een paraatheidsunie**[5], waarin een geïntegreerde aanpak van alle risico's met betrekking tot de paraatheid voor conflicten, door de mens veroorzaakte rampen en natuurrampen, en crises wordt uiteengezet, en op het **witboek over de gereedheid van de Europese defensie 2030**[6], waarmee de ontwikkeling en verwerving van defensiecapaciteiten in de hele EU worden ondersteund om buitenlandse tegenstanders af te schrikken. De Commissie zal ook een **schild voor de Europese democratie** voorstellen om de democratische veerkracht in de EU te versterken. Samen schetsen deze initiatieven een visie voor een veilige, beveiligde en veerkrachtige EU.

Nieuw Europees bestuur op het gebied van interne veiligheid

De Commissie zal nauw samenwerken met de lidstaten en de EU-agentschappen om de EU-aanpak van interne veiligheid zowel op strategisch als op operationeel niveau te verbeteren.

Dit zal wordt bereikt door:

- **het consequent in kaart brengen van mogelijke gevolgen voor de veiligheid en paraatheid van nieuwe en herziene initiatieven van de Commissie vanaf het begin van en gedurende het gehele onderhandelingsproces;**
- **regelmatige vergaderingen van de projectgroep Europese interne veiligheid van de Commissie, ondersteund door strategische sectoroverschrijdende samenwerking binnen de Commissie;**
- **presentaties van de dreigingsanalyses in verband met de interne veiligheid ter ondersteuning van de werkzaamheden van de Europese Veiligheids- en defensieacademie;**
- **besprekingen met de lidstaten in de Raad over de veranderende uitdagingen op het gebied van interne veiligheid op basis van de dreigingsanalyse en uitwisseling over de belangrijkste beleidsprioriteiten;**
- **regelmatige rapportage aan het Europees Parlement en de Raad om de systematische uitvoering van belangrijke veiligheidsinitiatieven te volgen en te ondersteunen.**

2. Geïntegreerd situationeel bewustzijn en dreigingsanalyse

Wij zullen de EU voorzien van nieuwe manieren om informatie te delen en te combineren en een regelmatige dreigingsanalyse voor de interne veiligheid van de EU verstrekken, om daarmee bij te dragen tot een alomvattende risico- en dreigingsevaluatie.

Veiligheid begint met **doeltreffend anticiperen**. Het situationeel bewustzijn en de dreigingsanalyse waarop de EU vertrouwt, moeten alomvattend, voldoende autonoom en actueel zijn. De lidstaten worden aangemoedigd om bruikbare inlichtingen verder uit te breiden via de gezamenlijke capaciteit op het gebied van inlichtingenanalyse (SIAC), als centraal contactpunt voor de inlichtingen van de lidstaten. Die inlichtingen zijn van essentieel belang voor het beoordelen en bestrijden van dreigingen en uiteindelijk als basis voor beleids- en

[4] COM (2025) 46 final.
[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.

wetgevingsmaatregelen[7]. Wij moeten **op inlichtingen gebaseerde analyses** en **dreigingsevaluaties** op EU-niveau doeltreffender benutten en daarbij meer samenwerken.

Voortbouwend op de verschillende risico- en dreigingsevaluaties die op EU-niveau en voor specifieke sectoren zijn opgesteld[8], zal de Commissie **regelmatig dreigingsanalyses voor de interne veiligheid van de EU** opstellen om de belangrijkste veiligheidsuitdagingen in kaart te brengen, teneinde de beleidsprioriteiten te onderbouwen. Deze analyses zullen bijdragen tot de ontwikkeling van een flexibel en responsief intern veiligheidsbeleid waarmee de veranderende dreigingen doeltreffend worden aangepakt, mensen en bedrijven beter worden beschermd tegen aanvallen en gerichte beleidsinterventies tijdig mogelijk worden gemaakt. Deze dreigingsanalyses voor de interne veiligheid van de EU zullen ook bijdragen tot de door de Commissie en de hoge vertegenwoordiger ontwikkelde **alomvattende (sectoroverschrijdende en alle gevaren bestrijkende) risico- en dreigingsevaluatie**, zoals uiteengezet in de strategie voor een paraatheidsunie.

Vertrouwen en veilige verwerking zijn van essentieel belang voor het delen van informatie, en daarvoor is een betrouwbare en veilige infrastructuur nodig. De instellingen, organen en instanties van de Unie moeten ervoor zorgen dat zij **beveiligde communicatiekanalen** kunnen gebruiken voor de uitwisseling van gevoelige en gerubriceerde informatie tussen henzelf en met de lidstaten. Investeringen in **interoperabele veilige systemen** en betrouwbare technologie zullen de autonomie van de EU versterken en de EU beter in staat stellen crises te beheersen en operationele veerkracht te waarborgen. In dit verband dringt de Commissie er bij de medewetgevers op aan de onderhandelingen over de voorgestelde **verordening betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie** af te ronden, met name om te zorgen voor een gemeenschappelijk kader voor de behandeling van gevoelige niet-gerubriceerde en gerubriceerde informatie[9].

Om haar eigen operationele veiligheid en situationeel bewustzijn te waarborgen, zal de Commissie haar governancekader voor interne beveiliging herzien en een **centrum voor geïntegreerde beveiligingsoperaties (Integrated Security Operations Centre — ISOC)** oprichten om mensen, materiële activa en operaties op alle locaties van de Commissie te beschermen. De Commissie zal ook haar operationele en analytische capaciteit versterken om hybride dreigingen in kaart te brengen en te beperken.

In overeenstemming met de strategie voor een paraatheidsunie zullen overwegingen inzake paraatheid en veiligheid in de wetgeving, het beleid en de programma's van de EU worden geïntegreerd en gemainstreamd. Bij de voorbereiding of herziening van wetgeving, beleid of programma's zal de Commissie systematisch nagaan welke gevolgen de voorkeursoptie zou kunnen hebben uit het oogpunt van paraatheid en veiligheid. Deze benadering zal worden geschraagd door regelmatige opleidingen te organiseren voor beleidsmakers in de Commissie.

Ter ondersteuning van de lidstaten zal de Commissie de veranderende uitdagingen op het gebied van interne veiligheid en de belangrijkste beleidsprioriteiten met de Raad bespreken en deze regelmatig op de hoogte houden van de uitvoering van de strategie. Daarnaast zal de

[7] *Safer Together — Strengthening Europe's Civilian and Military Preparedness and Readiness*, blz. 23.

[8] Sectorale dreigingsevaluaties die als basis voor deze dreigingsanalyse zullen dienen, zijn onder meer de dreigingsevaluatie van de Europese Unie voor zware en georganiseerde criminaliteit (EU-Socta), het verslag over de stand van zaken en de tendensen in verband met het terrorisme in de Europese Unie (TE-SAT-verslag), het gezamenlijk cyberevaluatieverslag (JCAR) en toekomstige beoordelingen van dreigingen, risico's en methoden op het gebied van witwassen en terrorismefinanciering die door de Commissie en de Autoriteit voor de bestrijding van witwassen en terrorismefinanciering moeten worden uitgevoerd.

[9] COM (2022) 119 final.

Commissie het Europees Parlement en de relevante belanghebbenden op de hoogte houden en blijven betrekken bij alle relevante acties.

Kernacties

De Commissie zal:

- **regelmatige dreigingsanalyses voor de uitdagingen op het gebied van de interne veiligheid van de EU ontwikkelen en presenteren.**

De lidstaten worden aangespoord om:

- **de uitwisseling van inlichtingen met de SIAC te verbeteren en te zorgen voor betere informatie-uitwisseling met EU-agentschappen en -organen.**

Het Europees Parlement en de Raad worden aangemoedigd:

- **de onderhandelingen over de voorgestelde verordening betreffende informatiebeveiliging in de instellingen, organen en instanties van de Unie af te ronden.**

3. Versterkte veiligheidscapaciteiten van de EU

Wij zullen nieuwe instrumenten voor rechtshandhaving ontwikkelen, zoals een vernieuwd Europol, en betere middelen om de veilige uitwisseling van gegevens en de rechtmatige toegang tot gegevens te coördineren en te waarborgen.

Om veranderende dreigingen doeltreffend tegen te gaan, moet de EU haar veiligheidscapaciteiten versterken en innovatie bevorderen. Als de belangrijkste actoren die bedreigingen voor de interne veiligheid tegengaan, hebben rechtshandhavingsautoriteiten en justitiële autoriteiten de juiste operationele instrumenten en capaciteiten nodig om snel en doeltreffend op te treden. Het is belangrijk dat deze autoriteiten over de grenzen heen en tussen diensten kunnen communiceren en coördineren om dreigingen op doeltreffende wijze te voorkomen, op te sporen, te onderzoeken en te vervolgen.

EU-agentschappen en -organen voor interne veiligheid

De EU-agentschappen en -organen op het gebied van justitie, binnenlandse zaken en cyberbeveiliging spelen een sleutelrol in de veiligheidsarchitectuur van de EU — een rol die steeds groter wordt naarmate hun verantwoordelijkheden toenemen.

Vandaag, 25 jaar na de oprichting, staat **Europol** meer dan ooit centraal in het veiligheidskader van de EU. De dienst ondersteunt complexe grensoverschrijdende onderzoeken, vergemakkelijkt informatie-uitwisseling, ontwikkelt innovatieve politie-instrumenten en levert geavanceerde expertise voor rechtshandhaving. Verschillende factoren beletten Europol echter zijn operationele potentieel bij de ondersteuning van onderzoeks- en operationele activiteiten ter bestrijding van grensoverschrijdende criminaliteit optimaal te benutten: deze factoren variëren van onvoldoende middelen tot het feit dat zijn huidige mandaat geen betrekking heeft op nieuwe veiligheidsdreigingen, zoals sabotage, hybride dreigingen of informatiemanipulatie. Daarom zal de Commissie een **ambitieuze herziening van het mandaat van Europol** voorstellen om van Europol een echt operationele politiedienst te maken die de lidstaten beter ondersteunt. Het doel is de technologische expertise en capaciteit van Europol ter ondersteuning van nationale rechtshandhavingsinstanties te versterken, de coördinatie met andere instanties en organen en met de lidstaten te verbeteren, strategische partnerschappen met partnerlanden en de particuliere sector te versterken en te zorgen voor een versterkt toezicht op Europol.

Voorts zal de Commissie zich inzetten om **de doeltreffendheid en complementariteit van de EU-agentschappen en -organen voor interne veiligheid verder te verbeteren en een naadloze onderlinge samenwerking te bevorderen**.

Het mandaat van **Eurojust** zal worden beoordeeld en versterkt met het oog op een doeltreffendere justitiële samenwerking, waardoor de complementariteit en de samenwerking met Europol worden versterkt. Hieronder valt het vergroten van de doeltreffendheid van Eurojust en van zijn capaciteit om de justitiële autoriteiten van de lidstaten proactieve ondersteuning en analyse te bieden. Voorts zal de Commissie, gezien de unieke bevoegdheid van het **EOM** om strafbare feiten die de financiële belangen van de Unie schaden, te onderzoeken en te vervolgen, nagaan hoe de capaciteit van het EOM om middelen van de Unie te beschermen het best kan worden verbeterd. Dit houdt onder meer in dat de samenwerking tussen het EOM en Europol moet worden versterkt.

Doeltreffende en veilige informatie-uitwisseling tussen agentschappen is van cruciaal belang voor de samenwerking. Europol en Frontex moeten snel informatie uitwisselen, ook onder meer voor operationele doeleinden, in aansluiting op de gezamenlijke verklaring van januari 2024[10]. **eu-LISA** speelt een centrale rol bij het waarborgen van een veilige opslag en beschikbaarheid van gegevens met het oog op een betere coördinatie en efficiëntere informatie-uitwisseling tussen de agentschappen. Het **Bureau van de Europese Unie voor de grondrechten** levert expertise op het gebied van de bescherming van de grondrechten bij de ontwikkeling en uitvoering van veiligheidsbeleid.

De **EU-Autoriteit voor de bestrijding van witwassen en terrorismefinanciering (AMLA)** heeft de bevoegdheid gekregen om op een hit/no hit-basis informatie te vergelijken met informatie die door Europol, het EOM, Eurojust en het Europees Bureau voor fraudebestrijding beschikbaar is gesteld om gezamenlijke analyses van grensoverschrijdende zaken uit te voeren.

Het **Enisa** speelt een centrale rol bij de uitvoering van de Europese wetgeving inzake cyberbeveiliging. Bij de komende **herziening van de cyberbeveiligingsverordening** zal de Commissie zijn mandaat beoordelen en voorstellen het te moderniseren om de toegevoegde waarde ervan voor de EU te versterken.

De samenwerking tussen douane- en andere rechtshandhavingsinstanties zal worden versterkt met de voorgestelde oprichting van de **douaneautoriteit van de Europese Unie** en de **douanedatahub van de Europese Unie** in het kader van het EU-pakket douanehervorming. Informatie van de toekomstige hub en daarmee verband houdende gegevens van Europol, Eurojust, het EOM, OLAF, de AMLA en Frontex, in het kader van hun respectieve bevoegdheden, zullen de gezamenlijke analyse verbeteren en bijdragen tot samenhangender operationele activiteiten, met name aan de buitengrenzen. De Commissie moedigt de medewetgevers aan om de onderhandelingen over de EU-douanehervorming snel af te ronden en zal hen daartoe blijven bijstaan.

Bij de versterking van de complementariteit tussen het EOM, OLAF, Europol, Eurojust, de AMLA en de voorgestelde EU-douaneautoriteit zal ook worden voortgebouwd op de resultaten van de lopende evaluatie van de **fraudebestrijdingsarchitectuur van de EU**. De interne veiligheid kan baat hebben bij deze holistische benadering, die is gericht op een beter gebruik van zowel strafrechtelijke als administratieve middelen, interoperabiliteit van IT-systemen en betere samenwerking.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

Kritieke communicatie

Tegenwoordig worden **systemen voor kritieke communicatie**[11] in de meeste gevallen op geïsoleerde wijze op nationaal niveau gebruikt. Dit betekent dat eerstehulpverleners vaak niet met hun tegenhangers kunnen communiceren wanneer zij de grens met andere lidstaten overschrijden. In sommige lidstaten zijn er ook beperkingen op de communicatie tussen verschillende soorten eerstehulpverleners (bv. politie en ambulances). De normen van de meeste systemen voldoen niet aan de huidige eisen op het gebied van functionaliteit en veerkracht, waardoor het reactievermogen van eerstehulpverleners aanzienlijk wordt beperkt, met name over de grenzen heen.

Om de EU beter in staat te stellen op crises te reageren, zal de Commissie wetgeving voorstellen tot oprichting van een **Europees systeem voor kritieke communicatie (EUCCS)** om de systemen voor kritieke communicatie van de volgende generatie in de EU te verbinden. Het doel is om het EUCCS op drie strategische pijlers te baseren: operationele mobiliteit, sterke veerkracht en strategische autonomie. Met het EUCCS-initiatief zullen geharmoniseerde eisen worden vastgesteld en zal worden bijgedragen aan de modernisering van de systemen voor kritieke communicatie van de lidstaten, zodat zij naadloos kunnen functioneren. Ook zal het bereik van het systeem worden uitgebreid dankzij het toekomstige multiorbitale systeem IRIS^2 [12]. Met door de EU gefinancierde projecten zullen de technische capaciteiten van het EUCCS worden opgebouwd, waarbij voornamelijk gebruik wordt gemaakt van Europese technologieleveranciers, om de strategische autonomie van de EU in deze gevoelige sector te bevorderen.

Rechtmatige toegang tot gegevens

Rechtshandhavingsautoriteiten en justitiële autoriteiten moeten criminaliteit kunnen onderzoeken en op kunnen treden om criminaliteit te bestrijden. Momenteel hebben bijna alle vormen van zware en georganiseerde criminaliteit een digitale voetafdruk[13]. Ongeveer 85 % van de strafrechtelijke onderzoeken is nu afhankelijk van het vermogen van rechtshandhavingsinstanties om toegang te krijgen tot digitale informatie[14].

De **groep op hoog niveau inzake toegang tot gegevens voor een doeltreffende rechtshandhaving** heeft in zijn eindverslag[15] benadrukt dat rechtshandhavingsinstanties en de rechterlijke macht de afgelopen tien jaar terrein hebben verloren aan criminelen, aangezien criminelen gebruikmaken van instrumenten en producten uit andere rechtsgebieden, verstrekt door aanbieders die maatregelen hebben genomen die de rechtshandhavingsinstanties de middelen ontnemen om samen te werken bij rechtmatige verzoeken in individuele strafzaken. Systematische samenwerking tussen rechtshandhavingsinstanties en particuliere partijen, waaronder dienstverleners, is derhalve van essentieel belang bij toekomstige inspanningen om de meest bedreigende criminele netwerken en personen in de Unie en daarbuiten te ontwrichten.

Aangezien digitalisering alomtegenwoordig wordt en een steeds groeiende bron van nieuwe instrumenten voor criminelen wordt, is een kader voor toegang tot gegevens dat tegemoet komt aan de behoeften om onze wetgeving te handhaven en onze waarden te beschermen, van essentieel belang. Tegelijkertijd is het evenzeer cruciaal om ervoor te zorgen dat digitale

[11] Dat wil zeggen de netwerken die worden gebruikt door rechtshandhavingsinstanties, grenswachters, douaneautoriteiten, civiele bescherming, brandweerlieden, medische noodhulpverleners en andere belangrijke actoren voor de openbare veiligheid en beveiliging.

[12] EU-infrastructuur voor veerkracht, interconnectiviteit en beveiliging per satelliet.

[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[14] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52019PC0070.

[15] Eindverslag van de groep op hoog niveau inzake toegang tot gegevens voor een doeltreffende rechtshandhaving, 15 november 2024, 4802e306-c364-4154-835b-e986a9a49281_en.

systemen beveiligd blijven tegen ongeoorloofde toegang om de cyberbeveiliging te beschermen en bescherming te bieden tegen nieuwe veiligheidsdreigingen. Dergelijke toegangskaders moeten ook de grondrechten eerbiedigen en er onder meer voor zorgen dat privacy en persoonsgegevens naar behoren worden beschermd.

De afgelopen jaren heeft de EU maatregelen genomen om **internetcriminaliteit aan te pakken en de toegang tot digitaal bewijsmateriaal voor alle misdrijven te vergemakkelijken**, met de vaststelling van regels inzake elektronisch bewijsmateriaal die vanaf augustus 2026 volledig van toepassing zullen zijn[16]. Deze regels zullen worden aangevuld met internationale instrumenten voor de uitwisseling van informatie en bewijsmateriaal. De Commissie zal binnenkort voorstellen het nieuwe **VN-Verdrag tegen cybercriminaliteit** te ondertekenen en te sluiten.

Om gevolg te geven aan de aanbevelingen van de groep op hoog niveau[17] zal de Commissie in de eerste helft van 2025 een **routekaart presenteren met de juridische en praktische maatregelen die zij voorstelt te nemen om een rechtmatige en effectieve toegang tot gegevens te waarborgen**. In het kader van de follow-up van deze routekaart zal de Commissie prioriteit geven aan een beoordeling van het effect van de **regels inzake gegevensbewaring** op EU-niveau en aan de voorbereiding van een **technologieroutekaart inzake encryptie**, teneinde technologische oplossingen te vinden en te beoordelen die rechtshandhavingsinstanties in staat zouden stellen op rechtmatige wijze toegang te krijgen tot versleutelde gegevens, waarbij de cyberbeveiliging en de grondrechten worden gewaarborgd.

Operationele samenwerking

De Commissie zal samenwerken met de lidstaten, EU-agentschappen en -organen en partnerlanden om de operationele samenwerking te versterken, wat essentieel is voor een doeltreffendere aanpak om grensoverschrijdende georganiseerde misdaad en terrorisme te bestrijden.

Als belangrijkste EU-kader voor gezamenlijk optreden tegen zware en georganiseerde criminaliteit heeft het **Europees multidisciplinair platform tegen criminaliteitsdreiging (Empact)** aanzienlijke operationele resultaten opgeleverd. De volgende Empact-cyclus 2026-2029 biedt een kans om dit kader nog verder te versterken. Om de meest bedreigende criminele netwerken en personen te ontwrichten, moet de Unie haar inspanningen stroomlijnen en toespitsen op de meest dringende prioriteiten, door de toezeggingen van de lidstaten te versterken en ervoor te zorgen dat middelen op doeltreffende wijze worden gebruikt.

Daartoe zal de Commissie met de voorzitterschappen van de Raad en de lidstaten samenwerken om het **potentieel van Empact optimaal te benutten en de kernprioriteiten voor de volgende Empact-cyclus 2026-2029 aan te pakken**. Op deze prioritaire gebieden is er behoefte aan inlichtingen over de meest bedreigende criminele netwerken, gezamenlijke onderzoeken en operationele taskforces en een krachtige justitiële respons, met inbegrip van een “follow-the-money”-aanpak. Bovendien moet de Unie criminele rekrutering en infiltratie aanpakken en samenwerking en opleiding op het gebied van rechtshandhaving tussen verschillende agentschappen en op internationaal niveau versterken.

De Commissie zal ook andere vormen van **grensoverschrijdende operationele samenwerking op het gebied van rechtshandhaving tussen de lidstaten en de met de**

[16] Verordening (EU) 2023/1543 van het Europees Parlement en de Raad van 12 juli 2023 betreffende het Europees verstrekkingsbevel en het Europees bewaringsbevel voor elektronisch bewijsmateriaal in strafzaken en de tenuitvoerlegging van vrijheidsstraffen als gevolg van een strafprocedure (PB L 191 van 28.7.2023).

[17] Conclusies van de Raad over toegang tot gegevens voor doeltreffende rechtshandhaving (12 december 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/nl/pdf.

Schengenruimte geassocieerd landen ondersteunen. Het Schengengebied, zonder controles aan de binnengrenzen, vereist nauwe samenwerking en uitwisseling van informatie tussen de rechtshandhavingsinstanties in de lidstaten om een hoog niveau van interne veiligheid te waarborgen. Momenteel staan rechtshandhavingsfunctionarissen nog steeds voor uitdagingen bij het bewaken of uitvoeren van dringende interventies over de grenzen heen[18], en voor het bestrijden van hybride dreigingen is ook nauwere grensoverschrijdende samenwerking nodig. Er moet een **groep op hoog niveau voor de toekomst van de operationele samenwerking op het gebied van rechtshandhaving** worden opgericht om een gemeenschappelijke strategische visie te ontwikkelen.

Efficiënte uitwisseling van gegevens tussen rechtshandhavingsinstanties is ook van essentieel belang voor een doeltreffende grensoverschrijdende samenwerking. Zodra de **interoperabiliteitsarchitectuur** is opgezet, zal zij de rechtshandhavingsinstanties en Europol effectieve toegang bieden tot cruciale informatie. Tegelijkertijd moeten de EU en haar lidstaten prioriteit geven aan de bilaterale en multilaterale uitwisseling van informatie, door middel van de juridische en technische uitvoering van de **Prüm II-verordening**[19], in samenwerking met eu-LISA en Europol. Dit zal de veilige geautomatiseerde uitwisseling van vingerafdrukken, DNA-profielen, voertuigregistratiegegevens, gezichtsopnamen en politiegegevens via EU-routers mogelijk maken. Op nationaal niveau moeten de lidstaten de **richtlijn informatie-uitwisseling**[20] uitvoeren om de kanalen voor informatie-uitwisseling met het oog op een naadloze grensoverschrijdende informatiestroom te verbeteren en tegelijkertijd de integratie ervan te waarborgen met systemen op Unieniveau, zoals Siena[21].

Doeltreffende grensoverschrijdende samenwerking is ook afhankelijk van het bevorderen van een **gemeenschappelijke rechtshandhavingscultuur in de EU**. Gezamenlijke opleiding, kenniscentra en mobiliteitsprogramma's zijn van essentieel belang om dit doel te bereiken. De Commissie zal onderzoeken hoe de EU opleidingen voor de autoriteiten van de lidstaten het best kan ondersteunen, waarbij zij een beroep doet op **Cepol** als het EU-agentschap voor opleiding op het gebied van rechtshandhaving.

Versterken van de grensbeveiliging

Het versterken van de veerkracht en veiligheid van de buitengrenzen is van cruciaal belang om hybride dreigingen, zoals de inzet van migratie als wapen, te bestrijden, om te voorkomen dat actoren en goederen die een bedreiging vormen de EU binnenkomen, en om grensoverschrijdende criminaliteit en terrorisme doeltreffend te bestrijden. Het **Schengeninformatiesysteem (SIS) zal naar verwachting in 2026 worden verbeterd** om de lidstaten in staat te stellen signaleringen in te voeren van onderdanen van derde landen die betrokken zijn bij terrorisme, met inbegrip van buitenlandse terroristische strijders, en bij andere ernstige misdrijven, op basis van gegevens die derde landen met Europol delen.

[18] Zoals vermeld in de beoordeling door de Commissie van de uitvoering die door de lidstaten wordt gegeven aan Aanbeveling (EU) 2022/915 van de Raad van 9 juni 2022 inzake operationele samenwerking op het gebied van rechtshandhaving (5909/25).

[19] Verordening (EU) 2024/982 van het Europees Parlement en de Raad van 13 maart 2024 betreffende de geautomatiseerde gegevensbevraging en -uitwisseling ten behoeve van politiële samenwerking en tot wijziging van de Besluiten 2008/615/JBZ en 2008/616/JBZ van de Raad en de Verordeningen (EU) 2018/1726, (EU) 2019/817 en (EU) 2019/818 van het Europees Parlement en de Raad (de Prüm II-verordening) (PB L, 2024/982, 5.4.2024).

[20] Richtlijn (EU) 2023/977 van het Europees Parlement en de Raad van 10 mei 2023 betreffende de uitwisseling van informatie tussen de rechtshandhavingsinstanties van de lidstaten en tot intrekking van Kaderbesluit 2006/960/JBZ van de Raad, P L 134 van 22.5.2023, blz. 1.

[21] Applicatie voor veilige informatie-uitwisseling.

Een betere **interoperabiliteit** van de grootschalige EU-informatiesystemen zal de lidstaten essentiële informatie verschaffen over personen uit derde landen die de buitengrenzen overschrijden of voornemens zijn te overschrijden, en zal de autoriteiten helpen bij het beoordelen van de voorwaarden voor het toestaan van toegang tot het grondgebied van de lidstaten[22]. De Commissie zal nauw blijven samenwerken met de lidstaten en eu-LISA met het oog op de snelle invoering van deze systemen, met name het **inreis-uitreissysteem (EES), het Europees reisinformatie- en -autorisatiesysteem (Etias) en het herziene visuminformatiesysteem (VIS)**, om de vlotte werking en de veiligheidsvoordelen ervan te waarborgen.

Om de grensbeveiliging verder te verbeteren en de EU-samenwerking in het licht van veranderende dreigingen te versterken, **zal de Commissie voorstellen Frontex te versterken**. Het aantal Europese grens- en kustwachters moet in de loop der tijd verdrievoudigen tot 30 000. Het agentschap moet worden uitgerust met geavanceerde technologie voor bewaking en situationeel bewustzijn, met inbegrip van inlichtingen die relevant zijn voor het Europees geïntegreerd grensbeheer en toegang tot robuuste overheidsdiensten voor aardobservatie van de EU voor grenstoezicht, die uiterlijk in 2027 moeten worden uitgerold. Dit moet het vermogen om grensoverschrijdende criminaliteit aan de buitengrenzen op te sporen, te voorkomen en te bestrijden verder verbeteren en de lidstaten meer ondersteuning bieden bij de uitvoering van terugkeer, vooral met betrekking tot onderdanen van derde landen die een veiligheidsrisico vormen.

Document- en identiteitsfraude vergemakkelijkt migrantensmokkel, mensenhandel, clandestiene criminele bewegingen en handel in illegale goederen. De **detector van meerdere identiteiten (MID)**[23] zal, zodra deze operationeel is, de nationale autoriteiten beter in staat stellen personen te identificeren die meerdere identiteiten gebruiken, en identiteitsfraude tegen te gaan. De Commissie zal onderzoeken hoe de beveiliging van reis- en verblijfsdocumenten die aan EU-burgers en onderdanen van derde landen worden afgegeven, kan worden verbeterd. Daarnaast zal de Commissie beoordelen hoe EU-portemonnees voor digitale identiteit, die uiterlijk eind 2026 in het kader van het Europees kader voor digitale identiteit moeten zijn ingevoerd, kunnen bijdragen tot een betere beveiliging van reisdocumenten en een betere identiteitscontrole. Dit vormt een aanvulling op de voorstellen over digitale reiscredentials en de digitale reisapplicatie van de EU[24].

Reisinformatie is van cruciaal belang voor autoriteiten om bewegingen van criminelen, terroristen en anderen die een veiligheidsbedreiging vormen, te identificeren en te onderzoeken. Hoewel er een EU-kader voor informatie over de commerciële luchtvaart[25] bestaat, is de verwerking van gegevens van andere vervoerswijzen voor rechtshandhavingsdoeleinden versnipperd. Bijgevolg kunnen criminelen en terroristen ongemerkt verschillende vervoerswijzen gebruiken voor illegale activiteiten. De Commissie zal met de lidstaten en de

[22] Het inreis-uitreissysteem (EES) zal de lidstaten met name in staat stellen onderdanen van derde landen aan de buitengrenzen van het Schengengebied te identificeren en hun inreis en uitreis te registreren, zodat verblijfsduuroverschrijders systematisch kunnen worden geïdentificeerd. Voorafgaand aan de aankomst van een onderdaan van een derde land aan de buitengrenzen zal het Europees reisinformatie- en -autorisatiesysteem (Etias) en het visuminformatiesysteem (VIS) de lidstaten in staat stellen vooraf te beoordelen of de aanwezigheid van een onderdaan van een derde land op het grondgebied van de EU een veiligheidsrisico zou vormen.

[23] De MID is een van de interoperabiliteitscomponenten die zijn ingevoerd bij Verordening (EU) 2019/818 en Verordening 2019/817.

[24] https://ec.europa.eu/commission/presscorner/detail/nl/ip_24_5047.

[25] Kader voor persoonsgegevens van passagiers (PNR) en voorafgaand aan de aankomst van passagiers doorgegeven passagiersgegevens en vluchtinformatie ("advance passenger information" — API) vastgesteld bij Richtlijn (EU) 2016/681 ("PNR-richtlijn"), Verordening (EU) 2025/12 en Verordening (EU) 2025/13 ("API-verordeningen".

vervoerssector samenwerken om **het kader voor reisinformatie te versterken** door een Unieregeling te verkennen die exploitanten van particuliere vluchten verplicht passagiersgegevens te verzamelen en door te geven, de regels voor de verwerking van persoonsgegevens van passagiers te evalueren en na te gaan hoe de verwerking van informatie over reizen over zee kan worden gestroomlijnd. Voor het wegvervoer zal de Commissie een ruimer gebruik van systemen voor **automatische kentekenplaatherkenning (ANPR)** beoordelen en de mogelijkheden voor synergieën met het SIS vergroten.

Prognose-, innovatie- en capaciteitsgestuurde aanpak

De Commissie zal een **alomvattende prognosegestuurde aanpak van interne veiligheid op EU-niveau** ontwikkelen, op basis van beste praktijken die op nationaal niveau zijn vastgesteld. Met deze aanpak zal de beleidsvorming worden ondersteund en zullen investeringen in relevant door de EU gefinancierd veiligheidsonderzoek en -innovatie worden gestuurd.

Onderzoek en innovatie spelen een cruciale rol bij de interne veiligheid doordat oplossingen worden gevonden om opkomende dreigingen, waaronder misbruik van technologie, tegen te gaan[26]. De EU moet via door de EU gefinancierd veiligheidsonderzoek en -innovatie[27] blijven investeren in de ontwikkeling van innovatieve instrumenten en oplossingen om veiligheidsdreigingen aan te pakken, met inachtneming van de regels en de grondrechten van de EU. De Commissie moet de overgang van onderzoek naar uitrol ondersteunen om ervoor te zorgen dat die moderne capaciteiten daadwerkelijk worden benut, met prioriteit voor **moderne technologieën** zoals AI. Deze aanpak moet opleiding omvatten om het gebruik van AI-systemen en andere technische capaciteiten door rechtshandhavingsautoriteiten en justitiële autoriteiten te verbeteren. Bovendien moet, in voorkomend geval, het potentieel voor tweeërlei gebruik van technologieën in beide richtingen worden benut (van het civiele naar het defensiedomein en omgekeerd)[28].

De **EU-innovatiehub voor interne veiligheid**[29], een netwerk van innovatielabs met de meest recente innovatie-updates en doeltreffende oplossingen ter ondersteuning van de werkzaamheden van actoren op het gebied van interne veiligheid in de EU en de lidstaten, zal helpen onderzoek in de praktijk en in het beleid te integreren. Om de doeltreffendheid van Europol te vergroten, moet het Europol-instrumentenregister worden versterkt, zodat Europol geavanceerde technologieën kan identificeren, ontwikkelen, gezamenlijk aankopen en operationeel toepassen. Daarnaast zal de Commissie in haar Gemeenschappelijk Centrum voor onderzoek een **onderzoeks- en innovatiecampus op het gebied van veiligheid** oprichten, waar onderzoekers bijeen worden gebracht om de cyclus van onderzoeksresultaten tot innovatie, ontwikkeling en succesvolle uitvoering te verkorten en tegelijkertijd de kosten voor ontwikkeling, tests en validatie te verlagen.

Onze **Europese Onderzoeksruimte** is vanwege de aard ervan op samenwerking gebaseerd en daardoor toegankelijk voor buitenlandse inmenging en desinformatie. Na de goedkeuring van de aanbeveling van de Raad over onderzoeksveiligheid[30] nemen de Commissie en de lidstaten

[26] Zie het verslag van het Gemeenschappelijk Centrum voor onderzoek van de Commissie *Emerging risks and opportunities for EU internal security from new technologies*, https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] *Study on strengthening EU-funded security research and innovation — 20 years of EU-Funded Civil Security Research and Innovation* — 2025, https://data.europa.eu/doi/10.2837/0004501.
[28] Zoals uiteengezet in het rapport-Niinistö.
[29] Europese innovatiehub voor interne veiligheid | Europol.
[30] PB C/2024/3510van 30.5.2024.

maatregelen om de betrokken actoren meer zeggenschap te geven, onder meer door de oprichting van een expertisecentrum op het gebied van onderzoeksveiligheid.

Kernacties

De Commissie zal het volgende goedkeuren:

- **een wetgevingsvoorstel om Europol om te vormen tot een echt operationele rechtshandhavingsinstantie in 2026;**
- **een wetgevingsvoorstel ter versterking van Eurojust in 2026;**
- **een wetgevingsvoorstel ter versterking van de rol en taken van Frontex in 2026;**
- **een wetgevingsvoorstel tot oprichting van een Europees systeem voor kritieke communicatie in 2026.**

De Commissie zal:

- **in 2025 een routekaart presenteren waarin de te volgen koers voor rechtmatige en effectieve toegang tot gegevens voor rechtshandhaving wordt uiteengezet;**
- **in 2025 een effectbeoordeling voorbereiden met het oog op de actualisering van de regels inzake gegevensbewaring op EU-niveau, in voorkomend geval;**
- **in 2026 een technologieroutekaart voor encryptie presenteren om technologische oplossingen te vinden en te beoordelen om rechtmatige toegang tot gegevens door rechtshandhavingsinstanties mogelijk te maken;**
- **werken aan de oprichting van een groep op hoog niveau ter versterking van de operationele samenwerking op het gebied van rechtshandhaving;**
- **in 2026 in haar Gemeenschappelijk Centrum voor onderzoek een onderzoeks- en innovatiecampus op het gebied van veiligheid oprichten.**

De Commissie zal, in samenwerking met de lidstaten en de betrokken EU-agentschappen:

- **de Empact-architectuur versterken;**
- **werken aan de snelle uitrol van de interoperabiliteitsarchitectuur en de uitvoering van de Prüm II-verordening;**
- **het kader voor reisinformatie versterken.**

De lidstaten worden aangespoord om:

- **de richtlijn informatie-uitwisseling om te zetten en ten volle uit te voeren.**

4. Weerbaarheid tegen hybride dreigingen en andere vijandige activiteiten

Wij zullen weerbaarheid tegen hybride dreigingen opbouwen door kritieke infrastructuur beter te beschermen, de cyberbeveiliging te versterken, vervoersknooppunten en havens te beveiligen en onlinedreigingen te bestrijden.

Vijandige activiteiten die de veiligheid van de EU ondermijnen, komen steeds vaker voor en zijn steeds complexer geworden, waarbij kwaadwillige actoren hun arsenaal aanzienlijk hebben uitgebreid. Tegen de EU, haar lidstaten en partners gerichte hybride campagnes zijn geïntensiveerd, met onder meer sabotage van kritieke infrastructuur, brandstichting, cyberaanvallen, inmenging in verkiezingen, buitenlandse informatiemanipulatie en inmenging (FIMI), met inbegrip van desinformatie, en het inzetten van migratie als wapen. Vanwege hun politieke en operationele rol en de aard van de informatie die zij verwerken, worden de instellingen, organen en instanties van de Unie (“entiteiten van de Unie”) niet gespaard.

De EU moet **haar veerkracht vergroten**, de huidige instrumenten doeltreffend gebruiken en nieuwe manieren ontwikkelen om zowel nu als in de toekomst het hoofd te bieden aan deze veranderende dreigingen van overheids- en niet-overheidsactoren,

Kritieke infrastructuur

Bedreigingen voor **kritieke infrastructuur**, waaronder hybride dreigingen zoals sabotage en kwaadwillige cyberactiviteiten, vormen een groot probleem, met name voor de infrastructuur die de lidstaten verbindt — interconnectoren of grensoverschrijdende communicatiekabels — en vervoer. Sinds de Russische aanvalsoorlog tegen Oekraïne is de sabotage van kritieke infrastructuur toegenomen, met name in 2024, waardoor tal van lidstaten werden getroffen. Samenwerking tussen diensten op het gebied van rechtshandhaving, beveiliging en cyberbeveiliging, militaire en civiele bescherming, en particuliere actoren is van essentieel belang om op doeltreffende wijze op dergelijke handelingen te anticiperen, ze op te sporen, te voorkomen en erop te reageren.

Het verminderen van kwetsbaarheden en het versterken van de veerkracht van kritieke entiteiten is van essentieel belang om de ononderbroken verlening te waarborgen van essentiële diensten die van vitaal belang zijn voor de economie en de samenleving. De tijdige omzetting en de correcte uitvoering door alle lidstaten van de **richtlijn betreffende de weerbaarheid van kritieke entiteiten (CER-richtlijn)**[31] en de **richtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie (NIS 2-richtlijn)**[32] zijn daarom in dat verband van cruciaal belang.

Om snelle vooruitgang te waarborgen, zal de Commissie de lidstaten ondersteunen bij het identificeren van kritieke entiteiten[33] en het uitwisselen van goede praktijken inzake nationale strategieën en risicobeoordelingen met betrekking tot essentiële diensten, in samenwerking met de **Groep voor de weerbaarheid van kritieke entiteiten** en de **NIS-samenwerkingsgroep**. Indien zich verstoringen van kritieke infrastructuur voordoen met aanzienlijke grensoverschrijdende gevolgen, zal de **EU-blauwdruk voor kritieke infrastructuur** de respons op EU-niveau coördineren. De Commissie moedigt de Raad aan snel de **EU-cyberblauwdruk** goed te keuren, waarmee de coördinatie in de context van crisisbeheersing verder zal worden versterkt en nauwere samenwerking tussen autoriteiten op het gebied van fysieke en digitale veerkracht zal worden vergemakkelijkt. Na succesvolle stresstests in de energiesector in 2023 zal de Commissie **vrijwillige stresstests** in andere sleutelsectoren voor interne veiligheid bevorderen. Daarnaast zal de Commissie een **overzicht op Unieniveau van grensoverschrijdende en sectoroverschrijdende risico's** voor essentiële diensten verstrekken ter ondersteuning van de risicobeoordelingen van de lidstaten en als uitgangspunt voor een uitgebreide risicobeoordeling op EU-niveau. In overeenstemming met de strategie voor een paraatheidsunie zal de Commissie met de lidstaten samenwerken om na te gaan voor welke andere sectoren en diensten die niet onder de huidige wetgeving vallen, maatregelen moeten worden genomen.

De **EU-NAVO-taskforce voor de veerkracht van kritieke infrastructuur** heeft een uitstekende samenwerking bevorderd bij het delen van beste praktijken en het vergroten van de

[31] Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad.

[32] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

[33] De sectoren die onder de richtlijn vallen, zijn energie, vervoer, bankwezen, financiëlemarktinfrastructuur, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur, ruimtevaart, en voedselproductie, -verwerking en -distributie.

veerkracht in de sectoren energie, vervoer, digitale infrastructuur en ruimtevaart. Deze werkzaamheden zullen worden voortgezet in het kader van de **gestructureerde dialoog tussen de EU en de NAVO over veerkracht**. De **EU-toolbox tegen hybride dreigingen** biedt de lidstaten en partners krachtige ondersteuning bij de voorbereiding en bestrijding van hybride dreigingen. **Teams voor snelle reactie op hybride dreigingen**[34] bieden op verzoek kortlopende ondersteuning op maat aan lidstaten, verschillende EU-missies en -partners. Voorts zal de Commissie de EU-samenwerking op het gebied van de bestrijding van sabotage voortzetten door middel van activiteiten met deskundigen[35], waaronder een **specifiek gezamenlijk werkprogramma** voor de deskundigen om de informatie-uitwisseling te stroomlijnen en tegenmaatregelen uit te werken.

Incidenten met betrekking tot **onderzeese kabels** in Europa maken duidelijk dat er behoefte is aan krachtigere maatregelen en duidelijkere antwoorden. Zoals uiteengezet in het **EU-actieplan inzake kabelbeveiliging**[36] zal de Commissie samen met de hoge vertegenwoordiger samenwerken met de lidstaten, EU-agentschappen en partners zoals de NAVO, om bedreigingen voor onderzeese kabels te voorkomen, op te sporen, erop te reageren en tegen te gaan. Om een geïntegreerd situatiebeeld van dreigingen te ontwikkelen, zal de Commissie met de lidstaten samenwerken om op vrijwillige basis een geïntegreerd surveillancemechanisme voor onderzeese kabels per zeebekken te ontwikkelen en uit te rollen, te beginnen met een Noords-Baltische regionale hub.

Cyberbeveiliging

De hardnekkige aard van **kwaadwillige cyberactiviteiten**, die vaak deel uitmaken van een breder scala van multidimensionale en hybride dreigingen, vereist voortdurende aandacht en actie op Europees niveau. De afgelopen jaren heeft de Unie een reeks cyberbeveiligingswetten vastgesteld om de cyberweerbaarheid van NIS 2-entiteiten die actief zijn in kritieke sectoren van de EU en van entiteiten van de Unie te versterken[37], de beveiliging van digitale producten te verbeteren (verordening cyberweerbaarheid) en een kader inzake steun voor paraatheid en respons op incidenten vast te stellen (verordening cybersolidariteit). In januari 2025 heeft de Commissie het **Europees actieplan voor de cyberbeveiliging van ziekenhuizen en zorgaanbieders**[38] vastgesteld om de opsporing van dreigingen, de paraatheid en de crisisrespons te verbeteren. Het is van essentieel belang dat dit actieplan volledig wordt uitgevoerd. Om nieuwe dreigingen en ontwikkelingen aan te pakken, moeten wij tegelijkertijd onze acties opvoeren, met name op het gebied van informatie-uitwisseling, de beveiliging van de toeleveringsketen, gijzelsoftware en cyberaanvallen, alsook technologische soevereiniteit.

Bovendien vereist de uitvoering dat de huidige vaardighedenkloof op het gebied van cyberbeveiliging van 299 000 mensen wordt gedicht. De Commissie zal met de lidstaten samenwerken in het kader van de vaardigheidsunie[39] om het aantal werknemers op het gebied van cyberbeveiliging uit te breiden, met name door gebruik te maken van de nieuwe academie voor cyberbeveiligingsvaardigheden. Het strategisch plan voor STEM-onderwijs[40] draagt bij

[34] Strategisch kompas voor veiligheid en defensie van de EU 2022, blz. 22.
[35] De EU-veiligheidsadviseurs, het Europees netwerk voor explosievenopruiming, het Atlasnetwerk, het EU-netwerk voor beveiliging tegen hoge risico's, de EU-adviesgroep inzake CBRN-beveiliging, de Groep voor de weerbaarheid van kritieke entiteiten (CERG).
[36] JOIN (2025) 9 final.
[37] Verordening (EU, Euratom) 2023/2841 van het Europees Parlement en de Raad van 13 december 2023 tot vaststelling van maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie (PB L, 2023/2841, 18.12.2023).
[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM (2025) 90 final.
[40] COM (2025) 89 final.

tot de verbetering van de doorstroming van talent en de reactie van Europa op de behoeften van de arbeidsmarkt voor cyberbeveiliging.

Gelijktijdig met het vergroten van haar weerbaarheid zal de EU ten volle gebruik blijven maken van het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten (het **instrumentarium voor cyberdiplomatie**) om cyberdreigingen die afkomstig zijn van overheids- en niet-overheidsactoren te voorkomen, tegen te gaan en erop te reageren.

Beveiliging van ICT-toeleveringsketens

De **EU-toolbox inzake 5G-cyberbeveiliging** voorziet in het relevante kader om 5G-netwerken te beschermen, maar wordt momenteel onvoldoende uitgevoerd door de lidstaten. Er blijven onaanvaardbare veiligheidsrisico's bestaan, met name wat betreft de vervanging van aanbieders met een hoog risico. Met een geharmoniseerde aanpak van de beveiliging van de ICT-toeleveringsketen kan de huidige versnippering van de interne markt als gevolg van verschillende benaderingen op nationaal niveau worden aangepakt, kunnen kritieke afhankelijkheden worden voorkomen en kunnen de risico's in onze ICT-toeleveringsketens van leveranciers met een hoog risico worden afgebouwd, om zo onze kritieke infrastructuur te beveiligen.

In overeenstemming met deze aanpak zal de Commissie bij de komende **herziening van de cyberbeveiligingsverordening** de beveiliging en veerkracht van ICT-toeleveringsketens en -infrastructuur in een breder verband bezien. Daarnaast zal de Commissie voorstellen het **Europees kader voor cyberbeveiligingscertificering** te verbeteren om ervoor te zorgen dat toekomstige certificeringsregelingen tijdig kunnen worden vastgesteld en dat hiermee op de beleidsbehoeften kan worden ingespeeld.

Voortbouwend op bestaande of lopende sectorale beoordelingen[41] zal de Commissie samen met de lidstaten een **strategische planning ontwikkelen voor gecoördineerde risicobeoordelingen op het gebied van cyberbeveiliging**.

Cloud- en telecomdiensten zijn een belangrijke schakel geworden in de toeleveringsketens van kritieke infrastructuur, bedrijven en overheden. De Commissie zal maatregelen nemen om kritieke entiteiten aan te moedigen **cloud- en telecomdiensten** te kiezen **die een passend niveau van cyberbeveiliging bieden**, niet alleen rekening houdend met technische risico's, maar ook met strategische risico's en afhankelijkheden.

Gijzelsoftware en cyberaanvallen

Gijzelsoftware is een hardnekkige grote uitdaging in de EU en de rest van de wereld, waarover in één verslag de totale jaarlijkse kosten uiterlijk in 2031 op meer dan 250 miljard EUR worden geraamd[42]. Zowel de **NIS 2-richtlijn** als de **verordening cyberweerbaarheid** zullen de beveiligingsmaturiteit van entiteiten aanzienlijk verbeteren, waardoor het voor netwerken die gijzelsoftware gebruiken duurder wordt om hun aanvallen uit te voeren. Daarnaast zal de Commissie nauw samenwerken met de lidstaten om ervoor te zorgen dat meer gijzelsoftwareaanvallen, met name geavanceerde aanhoudende dreigingen, en betalingen van losgeld worden gemeld aan de rechtshandhavingsinstanties, waardoor onderzoeken worden vergemakkelijkt.

[41] Zoals op het gebied van 5G-netwerken, telecommunicatie, elektriciteit, hernieuwbare energie en verbonden voertuigen.

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

Om cyberaanvallen te voorkomen en een halt toe te roepen, moet de EU de informatie-uitwisseling tussen rechtshandhavingsinstanties, cyberbeveiligingsautoriteiten en -entiteiten, alsook particuliere partijen versterken, onder toezicht van Europol en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa).

Europol en Eurojust moeten blijven voortbouwen op de resultaten die zij hebben geboekt bij het beëindigen van activiteiten met gijzelsoftware, om de samenwerking op het gebied van rechtshandhaving te ondersteunen. Daartoe moet de rechtshandhaving optimaal gebruikmaken van samenwerkingsmechanismen, waaronder het **International Ransomware Response Model van Europol** en het **International Counter Ransomware Initiative (CRI)**[43], en moeten Enisa en Europol samenwerken om het register van decryptiehulpmiddelen voor gijzelsoftwarestammen[44] uit te breiden.

Technologische soevereiniteit

Cyberbeveiliging en technologische soevereiniteit zijn nauw met elkaar verbonden, en technologische afhankelijkheden moeten met voorrang worden aangepakt. De Unie moet **sturing geven aan de ontwikkeling en uitrol van nieuwe technologieën**, waarbij de Commissie werkt aan de **versterking van de capaciteiten op het gebied van strategische technologieën** zoals AI, kwantum, geavanceerde connectiviteit, cloud, edge en het internet der dingen[45], via toekomstige initiatieven zoals het Actieplan voor het AI-continent, de kwantumstrategie en andere initiatieven[46]. De Commissie zal steun blijven verlenen aan de tijdige uitrol van de meest recente internationaal overeengekomen **internetprotocollen** die van essentieel belang zijn voor het behoud van een schaalbaar en efficiënt internet met een hoger niveau van cyberbeveiliging. Er zijn ook verdere maatregelen nodig om **uitdagingen in verband met het radiospectrum** aan te pakken, zoals met betrekking tot GNSS-spoofing, verstoring, risico's en afhankelijkheden in de toeleveringsketen, zoals het gebruik van kwantumdetectietechnologieën en het verkennen van de ontwikkeling van capaciteit voor radiofrequentiemonitoring.

De uitrol van oplossingen inzake **post-kwantumcryptografie** (PQC) zal van cruciaal belang zijn om gevoelige communicatie en gegevens in rust te waarborgen en digitale identiteiten in het nieuwe kwantumtijdperk te beschermen. Op basis van de aanbeveling van 2024 over een routekaart voor een gecoördineerde uitvoering van de transitie naar post-kwantumcryptografie[47] werkt de Commissie samen met de lidstaten om die transitie te bevorderen. In dit verband moeten de lidstaten gevallen met een hoog risico in kritieke entiteiten identificeren en zo spoedig mogelijk en uiterlijk eind 2030 zorgen voor kwantumveilige encryptie voor deze gevallen met een hoog risico. De Commissie werkt ook samen met de lidstaten en het Europees Ruimteagentschap (ESA) aan de ontwikkeling en uitrol van de **Europese infrastructuur voor kwantumcommunicatie (EuroQCI)**[48], op basis van Quantum Key Distribution (QKD), in het kader van **IRIS²**, het programma van de Unie voor beveiligde connectiviteit. Beide initiatieven zullen entiteiten uiteindelijk in staat stellen gegevens veilig door te geven en informatie veilig op te slaan.

[43] https://counter-ransomware.org/.
[44] Beschikbaar via het project No More Ransom, https://www.nomoreransom.org/nl/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] bv. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, Quantum Flagship Homepage van Quantum Flagship | Quantum Flagship, de 3C-networken (COM(2024) 81 final) en het EU-actieplan inzake kabelbeveiliging (JOIN(2025) 9 final).
[47] Aanbeveling over een routekaart voor een gecoördineerde uitvoering van de transitie naar post-kwantumcryptografie | De digitale toekomst van Europa vormgeven.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

Kwantumtechnologieën zullen ook een belangrijke rol spelen in beveiligingstoepassingen: in het kader van de **kwantumstrategie** zal een **routekaart voor kwantumdetectie in beveiligingstoepassingen** worden ontwikkeld. In dezelfde geest werkt de Commissie aan het kwantumbestendig maken van haar voor de interne veiligheid kritieke systemen, waaronder haar gerubriceerde IT-systemen.

Een bedrijfsvriendelijk kader voor cyberbeveiliging

De komende herziening van de cyberbeveiligingsverordening biedt een kans om de **EU-wetgeving inzake cyberbeveiliging** te vereenvoudigen, in overeenstemming met het kompas voor concurrentievermogen. De Commissie zal nauw samenwerken met de lidstaten om te zorgen voor een snelle, coherente en bedrijfsvriendelijke uitvoering van het horizontale cyberbeveiligingskader dat is vastgesteld in de NIS 2-richtlijn, de verordening cyberweerbaarheid en de verordening cybersolidariteit, door eenvoud en samenhang te bevorderen en versnippering of overlapping van cyberbeveiligingsregels in Uniewetgeving en nationale wetgeving te voorkomen.

Om veilige toegang tot onlinediensten mogelijk te maken en de digitale veiligheid in de hele EU te versterken, zal het **Europees kader voor digitale identiteit** alle burgers en inwoners van de EU vóór eind 2026 betrouwbare portemonnees voor digitale identiteit bieden. De komende **Europese portemonnee voor ondernemingen** zal veilige grensoverschrijdende interacties tussen bedrijven en overheidsdiensten vergemakkelijken. Beide zijn essentiële voorwaarden voor de veilige en doeltreffender werking van de datagestuurde eengemaakte markt met instrumenten zoals één digitale toegangspoort, e-facturering, e-aanbesteding en het digitale productpaspoort.

Onlineveiligheid

Sommige van de ernstigste hybride dreigingen die de veiligheid en beveiliging van de mensen in Europa in gevaar brengen en gericht zijn op de democratische ruimte van de EU, vinden online plaats. Deze dreigingen omvatten illegale activiteiten en illegale online-inhoud, informatiemanipulatie met kunstmatige versterking, misleidende informatie en buitenlandse informatiemanipulatie en inmenging.

De strikte handhaving van de **digitaledienstenverordening** is van het grootste belang om te zorgen voor een veilige en toegankelijke onlineomgeving met verantwoordelijke actoren die ook bestand is tegen hybride dreigingen. De digitaledienstenverordening verplicht aanbieders van zeer grote onlineplatforms en van zeer grote onlinezoekmachines om risicobeoordelingen uit te voeren en risicobeperkende maatregelen te nemen voor systeemrisico's die voortvloeien uit het ontwerp, de werking of het gebruik van hun diensten. Dergelijke risico's kunnen negatieve gevolgen zijn voor het maatschappelijk debat en verkiezingsprocessen, alsook voor de openbare veiligheid, zoals verregaande inmenging door kwaadwillige buitenlandse overheidsactoren, bijvoorbeeld in verkiezingsprocessen. Opleiding van de bevoegde autoriteiten van de lidstaten over het gebruik van juridische instrumenten om illegale online-inhoud onmiddellijk te verwijderen, is belangrijk, vooral met betrekking tot gendergerelateerd cybergeweld. De digitaledienstenverordening voorziet in een crisisresponsmechanisme, dat kan worden geactiveerd wanneer buitengewone omstandigheden leiden tot een ernstige bedreiging van de openbare veiligheid of de volksgezondheid in de Unie of in aanzienlijke delen daarvan. In aanvulling op dit mechanisme hebben de Commissie en de nationale bevoegde autoriteiten die als digitaledienstencoördinatoren zijn aangewezen ook een vrijwillig **kader voor respons op incidenten in het kader van de digitaledienstenverordening** ontwikkeld. Digitaledienstencoördinatoren hebben ook maatregelen genomen om de integriteit van verkiezingen te helpen beschermen, bijvoorbeeld door het organiseren van

rondetafelgesprekken bij verkiezingen en stresstests[49]. Samen met de verordening betreffende politieke reclame[50] is de digitaledienstenverordening een van de onderdelen die verband houden met het waarborgen van de democratie en de integriteit van democratische processen, die kwetsbaar zijn en het doelwit kunnen worden van vijandige actoren, onder meer via digitale instrumenten en op sociale media.

De uitvoering van de **FIMI**-toolbox is een ander belangrijk onderdeel dat belangrijke ondersteuning op EU-niveau biedt. Het ondersteunen van de digitale geletterdheid en mediageletterdheid en kritisch denken is ook van cruciaal belang voor deze inspanningen[51].

Bestrijding van de inzet van migratie als wapen

Rusland heeft, met de hulp en doortastende steun van Belarus, migratie doelbewust als wapen ingezet en migratiestromen naar de buitengrenzen van de EU illegaal gefaciliteerd om onze samenlevingen te destabiliseren en de eenheid van de Europese Unie te ondermijnen. Dit brengt niet alleen de nationale veiligheid en soevereiniteit van de lidstaten in gevaar, maar ook de veiligheid en integriteit van het Schengengebied en de veiligheid van de Unie als geheel. In zijn conclusies van oktober 2024 heeft de Europese Raad benadrukt dat het niet mag worden toegestaan dat Rusland en Belarus, of enig ander land, onze waarden, waaronder het recht op asiel, misbruiken en onze democratie ondermijnen.

Zoals vermeld in de mededeling van de Commissie van 2024 over de inzet van migratie als wapen, heeft de Unie naast krachtige politieke steun financiële, operationele en diplomatieke maatregelen genomen, waaronder samenwerking met landen van herkomst en doorreis, om deze bedreigingen op doeltreffende wijze aan te pakken[52]. Deze reactie houdt in dat gebruik wordt gemaakt van het nieuwe door de Raad vastgestelde kader om sancties op te leggen aan personen en organisaties die zijn betrokken bij acties en beleidsmaatregelen zoals de inzet van migratie als wapen door Rusland, door de bevriezing van activa en reisverboden[53]. De EU zal dit kader waar nodig blijven gebruiken en de lidstaten blijven ondersteunen bij het bestrijden van deze dreiging.

Beveiliging van het vervoer

Zeehavens, luchthavens en landinfrastructuur zijn cruciale inreis- en uitreispunten. Zij spelen een cruciale rol in de economie en de samenleving van de EU en zijn van essentieel belang voor militaire mobiliteit. Deze vervoersknooppunten en -middelen zijn echter ook belangrijke doelwitten voor externe dreigingen en criminele activiteiten. Recente incidenten, waaronder inbreuken op de luchtvrachtbeveiliging en aanvallen op spoorweginfrastructuur, wijzen op de ernstige risico's. **Vervoersondernemers** kunnen zowel doelwitten als instrumenten zijn voor kwaadwillige actoren. De bestaande EU-rechtsinstrumenten hebben de beveiliging van de luchtvaart verbeterd[54], maar het hoge dreigingsniveau voor de burgerluchtvaart vereist een middel om incidenten te voorspellen en de betrokken lidstaten snel te raadplegen. De Commissie zal met de lidstaten samenwerken om de bestaande uitvoeringhandelingen op het gebied van luchtvaartbeveiliging te wijzigen om gerubriceerde informatie over **voorvallen in**

[49] Verkiezingentoolkit in het kader van de digitaledienstenverordening voor digitaledienstencoördinatoren 2025 , https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Verordening (EU) 2024/900 van het Europees Parlement en de Raad van 13 maart 2024 betreffende transparantie en gerichte politieke reclame (PB L, 2024/900, 20.3.2024).
[51] Actieplan voor digitaal onderwijs (2021-2027) — Europese onderwijsruimte.
[52] COM (2024) 570 final.
[53] Verordening (EU) 2024/2642 van de Raad van 8 oktober 2024 betreffende beperkende maatregelen naar aanleiding van de destabiliserende activiteiten van Rusland, ST/8744/2024/INIT (PB L, 2024/2642, 9.10.2024).
[54] Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart (PB L 97 van 9.4.2008, blz. 72).

verband met de beveiliging van de luchtvaart te delen. Daarnaast zal de Commissie **regelgevende maatregelen overwegen** om nieuwe dreigingen zoals **incidenten met luchtvracht** aan te pakken en de normen voor luchtvaartbeveiliging te versterken. Dit houdt ook in dat de **wetgeving inzake luchtvaartbeveiliging (AVSEC)** moet worden versterkt om maatregelen voor onmiddellijke respons mogelijk te maken en tegelijkertijd de "one stop security"-zone op luchthavens in de EU in stand te houden.

Bij de ontwikkeling van de komende **EU-havenstrategie** zal de Commissie, voortbouwend op de **Europese havenalliantie**, onderzoeken hoe de wetgeving inzake maritieme veiligheid verder kan worden versterkt om opkomende dreigingen doeltreffend aan te pakken, havens te beveiligen en de veiligheid van de toeleveringsketen in de EU te verbeteren. Daartoe zal de Commissie erop toezien dat deze wetgeving daadkrachtig wordt uitgevoerd en zal zij werken aan de harmonisatie van nationale praktijken en aan de versterking van achtergrondcontroles in havens. In aanvulling op de beveiligingsprotocollen voor luchtvracht zal de Commissie met de lidstaten en de particuliere sector samenwerken om deze protocollen uit te breiden om de zeevervoersketens te beveiligen.

De voorgestelde EU-douaneautoriteit zal risico's analyseren en beoordelen op basis van **douane-informatie** over goederen die de EU binnenkomen en verlaten en via de EU worden doorgevoerd, om de lidstaten te helpen voorkomen dat internationale toeleveringsketens door kwaadwillige actoren worden gebruikt. In overeenstemming met de strategie van de Europese Unie voor maritieme veiligheid[55] zal het komende **Europees oceaanpact** een sleutelrol spelen bij het vergroten van de maritieme veiligheid in de zeebekkens rond de EU en daarbuiten, onder meer door het opschalen van maritieme operaties met meerdere doelen en oefeningen aan te moedigen.

Weerbaarheid van toeleveringsketens

Europa moet minder gaan vertrouwen op technologieën uit derde landen, die kunnen leiden tot afhankelijkheid en veiligheidsrisico's. De Commissie streeft ernaar de afhankelijkheid van afzonderlijke buitenlandse leveranciers te verminderen, de risico's in onze toeleveringsketens van leveranciers met een hoog risico te verminderen en kritieke infrastructuur en industriële capaciteit op het grondgebied van de EU veilig te stellen, zoals gespecificeerd in het **kompas voor concurrentievermogen**[56] en de **Clean Industrial Deal**[57]. De Commissie zal een **industriebeleid voor interne veiligheid** bevorderen door samen te werken met bedrijfstakken van de EU in belangrijke sectoren (bv. vervoersknooppunten, kritieke infrastructuur) om beveiligingsoplossingen te ontwikkelen zoals detectieapparatuur, biometrische technologieën en drones, met ingebouwde functies voor beveiliging door ontwerp. Bij de **herziening van de EU-aanbestedingsregels** zal de Commissie beoordelen of de veiligheidsoverwegingen in de richtlijn betreffende overheidsopdrachten op defensie- en veiligheidsgebied van 2009[58] toereikend zijn om tegemoet te komen aan de behoeften op het gebied van rechtshandhaving en veerkracht van kritieke entiteiten.

De Commissie zal de lidstaten ondersteunen bij de **screening van buitenlandse directe investeringen (BDI's)** en de aanschaf van apparatuur voor logistieke hubs, om ervoor te zorgen dat kritieke infrastructuur en technologie veilig blijven.

[55] JOIN (2023) 8 final.
[56] COM (2025) 30 final.
[57] COM (2025) 85 final.
[58] Richtlijn 2009/81/EG betreffende de coördinatie van de procedures voor het plaatsen door aanbestedende diensten van bepaalde opdrachten voor werken, leveringen en diensten op defensie- en veiligheidsgebied (PB L 216, 20.8.2009).

Zodra de **verordening inzake noodsituaties en veerkracht voor de interne markt (Imera)** in werking is getreden, zal zij de EU helpen bij het beheersen van crises die kritieke toeleveringsketens en het vrije verkeer van goederen, diensten en personen verstoren. De verordening zal het mogelijk maken om crises snel te coördineren en crisisrelevante goederen en diensten in kaart te brengen, en voorzien in een toolbox om de beschikbaarheid ervan te waarborgen. Voorts zal de Commissie, in nauwe samenwerking met de lidstaten, voorstellen een **waarschuwingsmechanisme voor de beveiliging van het transport en de toeleveringsketen voor diverse instanties** op te zetten om een veilige en tijdige uitwisseling te waarborgen van relevante informatie die nodig is om op dreigingen te anticiperen en deze tegen te gaan.

Met de uitvoering van de verordening kritieke grondstoffen en de verordening voor een nettonulindustrie zal een toegenomen gebruik van duurzaamheid, veerkracht en Europese preferentiecriteria bij overheidsopdrachten van de EU bovendien de ontwikkeling van leidende markten bevorderen. Versterkte handelsbetrekkingen, bijvoorbeeld via partnerschappen voor grondstoffen en partnerschappen voor schone handel en investeringen, zullen de toeleveringsketens helpen diversifiëren.

Weerbaarheid tegen en paraatheid voor chemische, biologische, radiologische en nucleaire dreigingen

De Russische aanvalsoorlog tegen Oekraïne heeft het risico van **chemische, biologische, radiologische en nucleaire dreigingen (CBRN-dreigingen)** vergroot. Om de mogelijke verwerving en inzet van CBRN-materiaal als wapen aan te pakken, zal de Commissie de lidstaten en partnerlanden ondersteunen door middel van specifieke opleidingen en oefeningen. De Commissie zal ook de capaciteiten op het gebied van CBRN-paraatheid en -respons versterken, met prioritering van dreigingen, financiering van innovatie voor tegenmaatregelen, rescEU-capaciteit en de aanleg van voorraden medische tegenmaatregelen, onder de paraplu van een nieuw **actieplan voor CBRN-paraatheid en -respons**. Daarnaast zal de **EU-strategie voor medische tegenmaatregelen** de ontwikkeling van medische tegenmaatregelen ondersteunen, van onderzoek tot productie en distributie, om de EU te beschermen tegen pandemieën en CBRN-dreigingen.

Voortbouwend op de ervaring met de COVID-19-pandemie heeft de EU het kader voor gezondheidsbeveiliging versterkt[59]. De Commissie wijst EU-referentielaboratoria op het gebied van volksgezondheid aan om de capaciteiten voor bewaking en snelle opsporing op EU- en nationaal niveau te versterken. In 2025 zal een plan van de Unie inzake paraatheid, preventie en respons op het gebied van gezondheidsbeveiliging worden bekendgemaakt.

Kernacties

De Commissie zal:

- **in 2025 de cyberbeveiligingsverordening evalueren en herzien;**
- **maatregelen ontwikkelen om een cyberveilig gebruik van clouddiensten te waarborgen;**
- **in 2025 een EU-havenstrategie voorstellen;**
- **in 2026 de EU-aanbestedingsregels voor defensie en veiligheid herzien;**
- **in 2026 een nieuw actieplan voor CBRN-paraatheid en -respons presenteren.**

De Commissie zal, in samenwerking met de lidstaten:

[59] Met name via Verordening (EU) 2022/2371 inzake ernstige grensoverschrijdende gezondheidsbedreigingen.

- **de Europese infrastructuur voor kwantumcommunicatie (EuroQCI) ontwikkelen en uitrollen;**
- **zorgen voor een doeltreffende handhaving van de digitaledienstenverordening;**
- **werken aan de bestrijding van de inzet van migratie als wapen;**
- **een systeem voor voorvallen in verband met de beveiliging van de luchtvaart opzetten;**
- **werken aan een waarschuwingsmechanisme voor de beveiliging van het transport en de toeleveringsketen voor diverse instanties.**

De Raad wordt verzocht:

- **de aanbeveling van de Raad over de EU-cyberblauwdruk goed te keuren.**

De lidstaten worden aangespoord om:

- **de CER- en NIS 2-richtlijnen om te zetten en ten volle uit te voeren.**

5. De strijd tegen zware en georganiseerde criminaliteit opvoeren

Wij zullen de georganiseerde misdaad helpen bestrijden door strengere regels voor te stellen om georganiseerde criminele groeperingen aan te pakken, onder meer door onderzoek te doen, jongeren in de EU minder kwetsbaar te maken voor rekrutering voor criminaliteit, en meer maatregelen te nemen om de toegang tot criminele instrumenten en activa te blokkeren.

De georganiseerde misdaad profiteert van een veranderend landschap en groeit exponentieel. Zij haalt voordeel uit geavanceerde technologieën, is actief in meerdere rechtsgebieden en heeft sterke banden buiten de grenzen van de EU. Gezien deze complexe, transnationale dreigingen is coördinatie en ondersteuning op EU-niveau van vitaal belang.

Misdaadpreventie

De aanwerving van jongeren voor georganiseerde misdaad vormt in de EU een groeiend punt van zorg. Om de georganiseerde criminaliteit te bestrijden, moeten de **onderliggende oorzaken** ervan worden aangepakt door onderwijs en alternatieven voor een leven van misdaad aan te bieden door middel van een maatschappijbrede aanpak. De Commissie zal de integratie van veiligheidsoverwegingen in het onderwijs-, sociaal, werkgelegenheids- en regionaal beleid van de EU ondersteunen. De EU zal **op bewijzen gebaseerd beleid voor criminaliteitspreventie**[60] **bevorderen** dat is afgestemd op de lokale context.

Om ontvangers van onlinediensten, met name minderjarigen, te beschermen tegen onder meer personen die kinderen seksueel misbruiken, mensenhandelaars en onlinerekrutering voor criminaliteit of gewelddadig extremisme, verplichten de maatregelen in het kader van de **digitaledienstenverordening** aanbieders van onlineplatforms die toegankelijk zijn voor minderjarigen, om risico's te beheren en op te treden tegen illegale inhoud, waaronder haatzaaiende uitlatingen. De Commissie is voornemens **richtsnoeren voor de bescherming van minderjarigen** uit te vaardigen om aanbieders van onlineplatforms te helpen een hoog niveau van privacy, veiligheid en beveiliging van minderjarigen online te waarborgen. De richtsnoeren zullen een reeks aanbevelingen bevatten voor alle digitale diensten die in de Unie actief zijn, om de bescherming van minderjarigen online te verbeteren. In 2025 is de Commissie ook voornemens om een **EU-oplossing voor privacyveilige leeftijdsverificatie** te faciliteren, waarmee de kloof zal worden gedicht voordat de EUDI-portemonnee eind 2026 wordt aangeboden. De Commissie zal ook een actieplan tegen cyberpesten presenteren.

[60] https://www.eucpn.org/.

Voorts zal de Commissie de vrijwillige betrokkenheid van meerdere belanghebbenden bij onlineplatforms en andere relevante actoren blijven ondersteunen, onder meer via het EU-Internetforum en gerichte gedragscodes in het kader van de digitaledienstenverordening, zoals de gedragscode inzake illegale haatuitingen op internet van 2025. Het doel is het bewustzijn te vergroten, gezamenlijk te reageren op huidige en opkomende dreigingen, en goede praktijken voor risicobeperkende maatregelen op te stellen en uit te wisselen.

Op lokaal niveau blijkt uit de impact van de georganiseerde misdaad dat er regionale oplossingen nodig zijn om kwetsbaarheid en de aantrekkingskracht van illegale activiteiten te verminderen. Met de EU-agenda voor steden zullen de veiligheidsuitdagingen in steden worden aangepakt, waarbij wordt voortgebouwd op het initiatief EU-steden tegen radicalisering. De Commissie zal de lidstaten ondersteunen bij het verbeteren van de stedelijke en regionale veiligheid via het Europees Fonds voor regionale ontwikkeling.

Een sterkere onderwijsbasis en sterkere vaardigheden liggen ten grondslag aan veerkrachtige en hechte samenlevingen. Via de **vaardigheidsunie** en het **actieplan voor integratie en inclusie** zal de Unie mensen helpen weerbaarder te worden tegen mis- en desinformatie, radicalisering en rekrutering voor criminaliteit.

De bescherming van kinderen tegen alle vormen van geweld, waaronder criminaliteit, fysiek of geestelijk geweld, online en offline, is een kerndoelstelling van de EU. Om tegemoet te komen aan de specifieke behoeften van bijzonder kwetsbare groepen, zoals kinderen, die steeds vaker worden blootgesteld aan rekrutering en radicalisering, kinderlokking en seksueel misbruik van kinderen, cyberpesten, desinformatie en andere dreigingen, zal de EU een **actieplan voor de bescherming van kinderen tegen criminaliteit** ontwikkelen, dat de online- en offline-dimensies omvat. Zij zal een samenhangende en gecoördineerde aanpak vaststellen op basis van de beschikbare kaders en instrumenten, waaronder het toekomstige EU-centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen, en andere EU-organen en -agentschappen, en voorstellen doen voor verdere stappen waar lacunes blijven bestaan.

Ontmanteling van criminele netwerken en hun medeplichtigen

De strijd tegen criminele netwerken met een hoog risico, kopstukken en medeplichtigen moet worden opgevoerd. Hoewel onlangs opmerkelijke successen zijn geboekt[61], vormen verouderde regels en inconsistente definities van criminele netwerken een belemmering voor een doeltreffende strafrechtelijke respons en grensoverschrijdende samenwerking. De Commissie zal achterhaalde wetgeving op dit gebied evalueren en een nieuw **rechtskader inzake georganiseerde criminaliteit** voorstellen om de respons te versterken.

Administratieve handhaving kan de rechtshandhaving aanvullen met het oog op snellere resultaten — zoals is aangetoond door het EOM en het Europees Bureau voor fraudebestrijding (OLAF) bij de aanpak van **grensoverschrijdende fraude en misdrijven die de financiële belangen van de EU schaden**. Subsidiefraudeurs richten zich op sectoren als hernieuwbare energie, onderzoeksprogramma's en de landbouwsector[62]. De Commissie zal nagaan hoe het gebruik van strafrechtelijke en administratieve instrumenten kan worden gecoördineerd en de samenwerking met Europol, Eurojust en het EOM kan worden verbeterd. De Commissie zal ook steun blijven verlenen aan de bredere toepassing van de **administratieve aanpak** om lokale en andere administratieve autoriteiten in staat te stellen criminele infiltratie te ontwrichten[63].

[61] Met inbegrip van recente Empact-zaken.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

De EU werkt aan de versterking van haar rechtskader voor **corruptiebestrijding**[64]. Het Europees Parlement en de Raad moeten de onderhandelingen over het door de Commissie voorgestelde geactualiseerde kader voor corruptiebestrijding snel afronden. De Commissie zal een EU-strategie voor corruptiebestrijding presenteren om de integriteit te bevorderen en de coördinatie tussen alle relevante autoriteiten en belanghebbenden op dit gebied te versterken.

Vuurwapens spelen een belangrijke rol in het toenemende geweld door georganiseerde criminele groeperingen. De Commissie zal gemeenschappelijke strafrechtelijke normen inzake illegale vuurwapenhandel voorstellen. Een nieuw **EU-actieplan inzake illegale vuurwapenhandel** zal zijn gericht op het beschermen van de legale markt, het beperken van criminele activiteiten op basis van betere inlichtingen, en het versterken van de internationale samenwerking, met bijzondere aandacht voor Oekraïne en de Westelijke Balkan.

Voor illegaal verhandelde pyrotechnische artikelen die voor misdrijven worden gebruikt, zijn maatregelen nodig om de preventie en traceerbaarheid te verbeteren. De Commissie evalueert momenteel de richtlijn pyrotechnische artikelen en zal ook **strafrechtelijke sancties voor de handel in pyrotechnische artikelen** overwegen.

Volgen van geldstromen

Het **volgen van geldstromen** is van cruciaal belang voor de bestrijding van georganiseerde misdaad en terrorisme, maar blijft een grote uitdaging. Het verband tussen georganiseerde misdaad en geldstromen vereist intensieve en gecombineerde inspanningen om de toegang van criminele netwerken tot financieringsbronnen te verhinderen en mensen, bedrijven en overheidsbegrotingen beter te beschermen.

De EU heeft haar inspanningen opgevoerd met de nieuwe antiwitwasregels, waaronder de oprichting van de **EU-autoriteit voor de bestrijding van witwassen en terrorismefinanciering (AMLA)**[65]. Samenwerking tussen de AMLA, OLAF, het EOM, Eurojust en Europol is van essentieel belang voor de uitvoering van doeltreffende financiële onderzoeken. De Commissie zal het opzetten van **partnerschappen** ondersteunen, zowel die welke de samenwerking tussen instanties vergemakkelijken als partnerschappen waarbij de particuliere sector is betrokken.

Om de financiële motieven achter de georganiseerde misdaad weg te nemen, is het van essentieel belang dat activa worden ontnomen en criminele winsten in beslag worden genomen. De onlangs aangenomen strengere regels inzake **ontneming en confiscatie van vermogensbestanddelen**[66] moeten onverwijld door de lidstaten worden omgezet en ten volle worden toegepast. De bestrijding van parallelle financiële systemen die het antiwitwaskader van de EU omzeilen, met inbegrip van op cryptovaluta gebaseerde systemen, vereist ook innovatieve acties, uitwisseling van beste praktijken tussen de lidstaten en meer steun van Europol en Eurojust. De Commissie zal de haalbaarheid onderzoeken van een nieuw EU-breed systeem om winsten uit de georganiseerde misdaad en terrorismefinanciering te traceren, en zal ook tijdige en uitgebreide informatiestromen van **financiële-inlichtingeneenheden** naar rechtshandhavingsinstanties aanmoedigen. De Commissie zal nagaan hoe mazen in de wet kunnen worden gedicht en hoe de lidstaten kunnen worden ondersteund bij capaciteitsopbouw,

[64] Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de bestrijding van corruptie, ter vervanging van Kaderbesluit 2003/568/JBZ van de Raad en van de Overeenkomst ter bestrijding van corruptie waarbij ambtenaren van de Europese Gemeenschappen of van de lidstaten van de Europese Unie betrokken zijn en tot wijziging van Richtlijn (EU) 2017/1371 van het Europees Parlement en de Raad, COM(2023) 234 final, Brussel, 3.5.2023.

[65] https://www.amla.europa.eu/index_en.

[66] Richtlijn (EU) 2024/1260 van het Europees Parlement en de Raad van 24 april 2024 betreffende ontneming en confiscatie van vermogensbestanddelen (PB L, 2024/1260, 2.5.2024).

en zal verder werken aan het versterken van de samenwerking met derde landen die door criminelen worden misbruikt voor ondergronds bankieren.

Bestrijding van ernstige misdrijven

Naast het ontmantelen van criminele netwerken zijn ook gerichte inspanningen nodig om ernstige misdrijven aan te pakken. Om ons beter in staat te stellen **onlinefraude** — die zeer aanzienlijke financiële schade veroorzaakt[67] — te bestrijden, zal de Commissie preventieve maatregelen en doeltreffendere rechtshandhavingsmaatregelen ondersteunen en samenwerken met de lidstaten en belanghebbenden om slachtoffers te ondersteunen en te beschermen, onder meer door hen te helpen bij het terugvorderen van hun middelen. Deze inspanningen zullen worden geformaliseerd in een **actieplan betreffende onlinefraude**.

Voortbouwend op de EU-strategie voor een doeltreffendere bestrijding van seksueel misbruik van kinderen[68] voor de periode 2020-2025 zal de Commissie de medewetgevers ondersteunen bij het afronden van de twee wetgevingsvoorstellen[69] om online seksueel misbruik van kinderen te voorkomen en te bestrijden en de rechtshandhavingsmaatregelen tegen seksueel misbruik en seksuele uitbuiting van kinderen doeltreffender te maken. Met tijdelijke regels die tot april 2026 van kracht zijn, is het van essentieel belang een permanent rechtskader tot stand te brengen, en de Commissie moedigt de medewetgevers aan onderhandelingen aan te gaan over de ontwerpverordening tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen. De medewetgevers wordt ook verzocht vooruitgang te boeken bij de onderhandelingen over de richtlijn ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, waarin minimumvoorschriften zullen worden vastgesteld voor de definitie van strafbare feiten en sancties op het gebied van seksuele uitbuiting van kinderen.

De helft van de gevaarlijkste criminele netwerken van de EU is betrokken bij gewelddadige **drugshandel**. Hoewel de EU onlangs haar strijd tegen deze criminaliteit heeft opgevoerd[70], met name door het mandaat van het **EU-drugsagentschap** uit te breiden, zijn verdere maatregelen nodig. De Commissie zal nauw samenwerken met de lidstaten om een nieuwe **EU-drugsstrategie** voor te stellen. Zij zal ook het **rechtskader voor drugsprecursoren** herzien en een **EU-actieplan tegen drugshandel** voorstellen om routes en bedrijfsmodellen te verstoren. Het **publiek-private partnerschap van de Europese havenalliantie** voor versterkte bescherming van havens zal worden uitgebreid naar kleinere havens en binnenhavens en zal ervoor zorgen dat de regels inzake maritieme veiligheid worden gehandhaafd. Gezien de ernstige lokale gevolgen van drugshandel zal de Commissie steun blijven verlenen aan een evenwichtig, empirisch onderbouwd en multidisciplinair drugsbeleid, met paraatheid voor plotselinge drugsinstromen, met name synthetische opioïden.

Om uitbuiting van mensen tegen te gaan, heeft de EU nieuwe regels[71] vastgesteld en zal zij een **vernieuwde EU-strategie voor de bestrijding van mensenhandel** (2026-2030) invoeren, die betrekking heeft op alle fasen, van preventie tot vervolging, met bijzondere aandacht voor slachtofferhulp op zowel EU- als internationaal niveau.

In de strijd tegen **migrantensmokkel** zal de Commissie de inspanningen met belangrijke partners leiden via de nieuwe wereldwijde alliantie tegen migrantensmokkel, in samenwerking met Europol, Eurojust en Frontex, onder meer op het gebied van de onlinedimensie. De

[67] Global Anti-Scam Report 2024.
[68] COM (2020) 607 final
[69] COM (2022) 209 final en COM (2024) 60 final.
[70] COM (2023) 641 final.
[71] Richtlijn (EU) 2024/1712 van 13 juni 2024 tot wijziging van Richtlijn 2011/36/EU inzake de voorkoming en bestrijding van mensenhandel en de bescherming van slachtoffers daarvan (PB L, 2024/1712, 24.6.2024).

voorstellen van de Commissie inzake de bestrijding van mensensmokkel[72] moeten onverwijld worden aangenomen en uitgevoerd. Voorts heeft de Commissie, na de goedkeuring van de **toolbox voor vervoerders**[73], de contacten met buitenlandse autoriteiten en exploitanten aangehaald en zal zij blijven samenwerken met de luchtvaartsector en burgerluchtvaartorganisaties[74] om het bewustzijn over migrantensmokkel door de lucht te vergroten[75].

Milieucriminaliteit vormt een bedreiging voor het milieu, de volksgezondheid en de economie op lange termijn. De Commissie zal de lidstaten ondersteunen bij de uitvoering van de richtlijn milieucriminaliteit[76] en de operationele netwerken en acties op dit gebied[77] versterken. Een deugdelijke handhaving is van essentieel belang. Bovendien zal het onlangs aangenomen **Verdrag van de Raad van Europa inzake de bescherming van het milieu door middel van het strafrecht**[78] bijdragen tot krachtige en vergelijkbare inspanningen om milieucriminaliteit aan te pakken, zowel in Europa als daarbuiten.

Strafrechtelijke respons

Criminaliteit en terrorisme kunnen gevolgen hebben voor iedereen, waardoor het van essentieel belang is de rechten van **slachtoffers** te ondersteunen en te waarborgen om de schade te beperken en de algemene veiligheid en het vertrouwen in de autoriteiten te vergroten. Voortbouwend op de richtlijn slachtofferrechten zal de Commissie een nieuwe **EU-strategie voor de rechten van slachtoffers** invoeren.

De **strafrechtstelsels van de EU** hebben doeltreffende instrumenten nodig om opkomende dreigingen aan te pakken. Om dit te bereiken heeft de Commissie een **forum op hoog niveau over de toekomst van het strafrecht van de EU** opgezet. In dit forum worden de lidstaten, het Europees Parlement, EU-agentschappen en -organen en andere relevante belanghebbenden bijeengebracht. Dit forum heeft tot doel manieren te bespreken om ervoor te zorgen dat onze strafrechtstelsels doeltreffend, billijk en veerkrachtig blijven in het licht van veranderende uitdagingen, en tegelijkertijd de justitiële samenwerking te versterken en het wederzijds vertrouwen te vergroten, onder meer via digitalisering[79].

Kernacties

De Commissie zal:

- **in 2026 een wetgevingsvoorstel indienen voor gemoderniseerde regels inzake georganiseerde criminaliteit;**
- **in 2025 een wetgevingsvoorstel indienen om het rechtskader voor drugsprecursoren te herzien;**

[72] COM (2023) 755 final en COM (2023) 754 final.
[73] Toolbox voor het aanpakken van het gebruik van commerciële vervoermiddelen om irreguliere migratie naar de EU te vergemakkelijken.
[74] Met inbegrip van de International Burgerluchtvaartorganisatie. (ICAO).
[75] De Commissie zal ook de laatste hand leggen aan de verordening betreffende maatregelen tegen vervoerders die mensenhandel of migrantensmokkel faciliteren of zich daarmee inlaten, COM(2021) 753 final.
[76] Richtlijn (EU) 2024/1203 van het Europees Parlement en de Raad van 11 april 2024 inzake de bescherming van het milieu door middel van het strafrecht (PB L, 2024/1203, 30.4.2024).
[77] Het EU-netwerk voor de implementatie en handhaving van de milieuwetgeving (Impel), het Europees netwerk van openbaar aanklagers voor het milieu (ENPE), EnviCrimeNet en het EU-forum van milieurechters (EUFJE).
[78] Comité van deskundigen voor de bescherming van het milieu door middel van het strafrecht (PC-ENV) — Europees Comité voor strafrechtelijke vraagstukken.
[79] Met name door de oprichting van het systeem voor e-Justice Communication via Online Data Exchange (e-Codex) en het Europees Strafregisterinformatiesysteem — Onderdanen van derde landen (Ecris-TCN-systeem).

- **in 2025 een wetgevingsvoorstel indienen voor gemeenschappelijke strafrechtelijke normen inzake illegale vuurwapenhandel;**
- **nagaan of de richtlijnen inzake pyrotechnische artikelen en explosieven voor civiel gebruik moeten worden herzien;**
- **nagaan of het Europees onderzoeksbevel en het Europees aanhoudingsbevel verder moeten worden versterkt;**
- **in 2026 een nieuwe EU-strategie voor de bestrijding van mensenhandel presenteren;**
- **in 2026 een nieuwe EU-strategie voor de rechten van slachtoffers presenteren;**
- **uiterlijk in 2027 een EU-actieplan inzake de bescherming van kinderen tegen criminaliteit indienen;**
- **in 2025 een EU-actieplan tegen drugshandel presenteren;**
- **in 2026 een EU-actieplan tegen illegale vuurwapenhandel presenteren;**
- **de Europese havenalliantie vanaf 2025 stapsgewijs uitbreiden;**
- **in 2026 richtsnoeren in het kader van de digitaledienstenverordening over de bescherming van minderjarigen goedkeuren;**
- **in 2026 een EU-actieplan tegen cyberpesten presenteren.**

De lidstaten worden aangespoord om:

- **de nieuwe regels inzake ontneming en confiscatie van vermogensbestanddelen uiterlijk eind 2026 volledig om te zetten en ten volle te benutten;**
- **de administratieve aanpak te hanteren in de strijd tegen criminele infiltratie;**
- **publiek-private partnerschappen tegen witwassen op te zetten;**
- **de richtlijn ter voorkoming en bestrijding van geweld tegen vrouwen en huiselijk geweld om te zetten en ten volle uit te voeren.**

Het Europees Parlement en de Raad worden aangespoord om:

- **vooruitgang te boeken met de onderhandelingen over de verordening tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen en de richtlijn ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie;**
- **de onderhandelingen over de richtlijn inzake corruptiebestrijding af te ronden.**

6. Bestrijding van terrorisme en gewelddadig extremisme

Wij zullen een alomvattende terrorismebestrijdingsagenda invoeren om radicalisering te voorkomen, online- en openbare ruimten te beveiligen, financieringskanalen af te knijpen en te reageren op aanvallen wanneer deze zich voordoen.

Het dreigingsniveau van terrorisme in de EU is nog steeds hoog. Het houdt nauw verband met de overloopeffecten van geopolitieke gebeurtenissen, nieuwe technologieën en nieuwe vormen van terrorismefinanciering. Wij moeten ervoor zorgen dat de EU goed is toegerust om op dreigingen te anticiperen, radicalisering (zowel offline als online) te voorkomen, burgers en openbare ruimten te beschermen tegen aanvallen en doeltreffend te reageren op eventuele aanvallen. In 2025 zal een **nieuwe EU-agenda voor het voorkomen en bestrijden van terrorisme en gewelddadig extremisme** worden gepresenteerd, waarin toekomstige acties van de EU worden uiteengezet. In overeenstemming met de nieuwe agenda zullen de EU en de Westelijke Balkan in 2025 het nieuwe **gezamenlijke actieplan** ter voorkoming en bestrijding van terrorisme en gewelddadig extremisme ondertekenen.

Radicalisering voorkomen en mensen online beschermen

Net als bij de bestrijding van georganiseerde misdaad begint de bestrijding van terrorisme en gewelddadig extremisme met het **aanpakken van de onderliggende oorzaken** ervan. Het **EU-kenniscentrum voor de preventie van radicalisering** zal zijn steun aan beroepsbeoefenaren en beleidsmakers opvoeren met een nieuwe **alomvattende preventietoolbox** om vroegtijdige identificatie en interventies mogelijk te maken die zijn gericht op kwetsbare personen, met name minderjarigen. Radicalisering vindt vaak plaats in gevangenissen en om de lidstaten te ondersteunen bij het aanpakken van dit probleem, zal de Commissie nieuwe aanbevelingen doen.

Terroristische en gewelddadige extremisten gebruiken onlineplatforms om terroristische en schadelijke inhoud te verspreiden, geld aan te trekken en mensen te rekruteren. Kwetsbare gebruikers, met name minderjarigen, worden online in een alarmerend tempo geradicaliseerd. De **verordening inzake terroristische online-inhoud** heeft een belangrijke rol gespeeld bij het tegengaan van de verspreiding van terroristische online-inhoud, waardoor het meest gruwelijke en gevaarlijke materiaal snel kan worden verwijderd[80]. De Commissie evalueert momenteel de werking ervan en zal nagaan hoe dit kader het best kan worden versterkt.

Het **EU-crisisprotocol** voor een gezamenlijke en snelle respons van rechtshandhavingsinstanties en de technologiesector op een terroristische aanslag zal worden gewijzigd om te zorgen voor schaalbaarheid en flexibiliteit teneinde te reageren op de toenemende onlinedimensie van terroristische aanslagen. Het EU-Internetforum zal de belangrijkste weg blijven voor vrijwillige samenwerking met de technologiesector om terroristische en schadelijke online-inhoud aan te pakken. Voorts neemt de Commissie deel aan internationale initiatieven zoals de Christchurch Call Foundation en het wereldwijde internetforum ter bestrijding van terrorisme.

Tegengaan van terrorismefinanciering

Terroristen financieren hun activiteiten met crowdfundingcampagnes, cryptoactiva, neobanken of platforms voor onlinebetalingen. Rechtshandhavingsinstanties moeten deze geldstromen opsporen en onderzoeken. Hiervoor zijn middelen, instrumenten en deskundigheid nodig. Het **netwerk van financiële onderzoekers voor terrorismebestrijding** speelt een belangrijke rol. De Commissie zal de oprichting onderzoeken van een **nieuw EU-breed systeem voor het traceren van terrorismefinanciering**, waaronder intra-EU- en SEPA-transacties, overmakingen van cryptoactiva, online en elektronische betalingen, in aanvulling op de overeenkomst tussen de EU en de VS inzake het programma voor het traceren van terrorismefinanciering (TFTP).

De EU-begroting moet worden **beschermd tegen misbruik waarbij radicale/extremistische standpunten in de lidstaten worden bevorderd**. Het herziene **Financieel Reglement** bevat nu een bepaling dat een veroordeling voor “aanzetten tot discriminatie, haat of geweld” grond is voor uitsluiting van EU-financiering. De Commissie zal blijven zoeken naar de beste manier om de toolbox optimaal te benutten, ook bij de selectie van potentiële begunstigden. De bescherming van de EU-begroting is ook afhankelijk van nauwe samenwerking en informatie-uitwisseling met nationale autoriteiten, EU-agentschappen en -organen.

[80] Op 31 december 2024 waren er 1 426 bevelen tot verwijdering uitgevaardigd om terroristische inhoud te verwijderen of de toegang daartoe te blokkeren, waarvan de overgrote meerderheid gericht was tegen jihadistische terroristische inhoud, maar ook tegen rechtse terroristische inhoud.

Bescherming tegen aanvallen

Naast investeringen in het voorkomen van radicalisering is een belangrijk onderdeel van de bescherming van burgers het beperken van de middelen voor terroristen en criminelen om aanslagen te plegen. Er moeten maatregelen worden genomen met betrekking tot de instrumenten die terroristen gebruiken en om de doelwitten die het risico lopen te worden aangevallen, te beschermen.

Naast maatregelen op het gebied van vuurwapens zal de Commissie ook de **regels inzake precursoren voor explosieven herzien** om daarin chemische stoffen met een hoog risico op te nemen. **Openbare ruimten** blijven het vaakst het doelwit voor terroristische aanslagen, met name voor eenlingen. Om burgers tegen schade te beschermen, zal het **EU-programma voor veiligheidsadviseurs** worden versterkt om op verzoek van de lidstaten beoordelingen uit te voeren van de kwetsbaarheid van openbare ruimten, kritieke infrastructuur en evenementen met een hoog risico, en worden gefinancierd uit de EU-begroting in het kader van het Fonds voor interne veiligheid. De EU zal trachten de beschikbare financiering voor de bescherming van de openbare ruimte uit te breiden. De Commissie biedt de autoriteiten van de lidstaten en particuliere exploitanten ondersteuning door middel van specifieke richtsnoeren en instrumenten, zoals de **kennishub voor de bescherming van openbare ruimten**[81], en sinds 2020 miljoen is al 70 miljoen EUR beschikbaar gesteld om de bescherming van de openbare ruimte te ondersteunen.

De Commissie zal ook onderzoeken of er vereisten voor organisaties moeten worden ingevoerd om veiligheidsmaatregelen te overwegen of toe te passen op openbaar toegankelijke locaties, door samen te werken met lokale overheden en particuliere partners.

Gezien de duidelijke kwetsbaarheden zal de **EU-strategie voor de bestrijding van antisemitisme en de bevordering van het Joodse leven (2021-2030)** richting blijven geven aan de maatregelen van de Commissie ter bescherming van de Joodse gemeenschap. De Commissie zal er ook voor zorgen dat er passende instrumenten voorhanden zijn om de lidstaten te ondersteunen bij de bestrijding van **moslimhaat**.

Het gebruik van **drones** voor spionage en aanslagen vormt een steeds grotere uitdaging op het gebied van veiligheid. De Commissie zal een **geharmoniseerde testmethode voor droneafweersystemen** ontwikkelen, een **kenniscentrum voor de bestrijding van drones** opzetten en nagaan of de wetten en procedures van de lidstaten moeten worden geharmoniseerd[82].

Buitenlandse terroristische strijders

Om buitenlandse terroristische strijders te identificeren die terugkeren of binnenkomen aan de buitengrenzen van de EU, zijn gegevens nodig over personen die een terroristische dreiging vormen. Daartoe zal de Commissie samen met Europol haar **samenwerking met belangrijke derde landen versterken om biografische en biometrische gegevens te verkrijgen over personen die een terroristische dreiging kunnen vormen**, waaronder buitenlandse terroristische strijders, die vervolgens in het Schengeninformatiesysteem kunnen worden opgenomen met volledige inachtneming van de toepasselijke EU- en nationale rechtskaders. Het is daarom van cruciaal belang dat de lidstaten alle bestaande instrumenten gebruiken. Hieronder valt het invoeren van alle relevante informatie in het **SIS**, het verbeteren van biometrische controles en het uitvoeren van verplichte systematische controles van alle personen aan de buitengrenzen van de EU[83]. Bovendien zullen de door Frontex ontwikkelde

[81] Kennishub voor de bescherming van openbare ruimten.
[82] Naar aanleiding van de reeks kernacties in de counter-dronemededeling van 2023, COM(2023) 659 final.
[83] Met volledige inachtneming van de Schengengrenscode en de screeningverordening.

gemeenschappelijke risico-indicatoren de grensbewakingsautoriteiten van de lidstaten blijven ondersteunen bij het in kaart brengen en beoordelen van het risico op verdachte reizen door potentiële buitenlandse terroristische strijders.

Om ervoor te zorgen dat de lidstaten toegang blijven hebben tot de **slagveldinformatie** die is verzameld door het VN-onderzoeksteam dat zich ervoor inzet dat verantwoording wordt afgelegd voor door Da'esh/ISIS gepleegde oorlogsmisdaden (UNITAD) met het oog op de vervolging van buitenlandse terroristische strijders, zal de Commissie, samen met Eurojust, voorts nagaan of dit bewijsmateriaal kan worden opgeslagen in de gegevensbank voor bewijsmateriaal van internationale kernmisdrijven van Eurojust. Bovendien zal het nieuwe Europees **gerechtelijk register voor terrorismebestrijding** de rechterlijke instanties van de lidstaten blijven ondersteunen bij het snel vaststellen van grensoverschrijdende verbanden in terrorismezaken.

Kernacties

De Commissie zal:

- **in 2025 een nieuwe EU-agenda voor het voorkomen en bestrijden van terrorisme en gewelddadig extremisme goedkeuren;**
- **in 2025 een nieuw gezamenlijk actieplan voor de preventie en bestrijding van terrorisme en gewelddadig extremisme ondertekenen met de Westelijke Balkan;**
- **een nieuwe alomvattende preventietoolbox ontwikkelen met het EU-kenniscentrum;**
- **in 2026 de toepassing van de verordening inzake terroristische online-inhoud evalueren;**
- **in 2025 het EU-crisisprotocol wijzigen;**
- **in 2026 een wetgevingsvoorstel indienen tot herziening van de verordening over het op de markt brengen en het gebruik van precursoren voor explosieven;**
- **de haalbaarheid onderzoeken van een nieuw EU-breed systeem voor het traceren van terrorismefinanciering.**

De lidstaten worden aangespoord om:

- **biometrische controles te versterken en verplichte systematische controles aan de buitengrenzen van de EU uit te voeren;**
- **ten volle gebruik te maken van het Europees gerechtelijk register voor terrorismebestrijding.**

7. De EU als sterke mondiale speler op het gebied van veiligheid

Om de veiligheid van de EU te vergroten, zullen wij de operationele samenwerking stimuleren door middel van partnerschappen met belangrijke regio's zoals onze uitbreidings- en nabuurschapspartners, Latijns-Amerika en het Middellandse Zeegebied. Bij internationale samenwerking zal rekening worden gehouden met de veiligheidsbelangen van de EU, onder meer door gebruik te maken van EU-hulpmiddelen en -instrumenten.

De afgelopen jaren is duidelijk gebleken hoe intrinsiek de externe en interne veiligheid van de EU met elkaar zijn verbonden. De Russische aanvalsoorlog tegen Oekraïne, het conflict in Gaza, de situatie in Syrië en opkomende conflicten over de hele wereld hebben ernstige overloopeffecten gehad op de interne veiligheid van de EU. Om de gevolgen van mondiale instabiliteit voor haar interne veiligheid tegen te gaan, **moet de EU haar veiligheidsbelangen actief verdedigen** door externe dreigingen aan te pakken, smokkelroutes te verstoren en

corridors van strategisch belang, zoals handelsroutes, veilig te stellen. Tegelijkertijd zal de EU een sterke bondgenoot van partnerlanden blijven, en met hen samenwerken om de wereldwijde veiligheid te vergroten en gezamenlijke weerbaarheid tegen dreigingen op te bouwen.

De afgelopen jaren heeft de EU belangrijke stappen gezet om haar samenwerking op het gebied van veiligheid te versterken. Zij heeft operationele overeenkomsten inzake rechtshandhaving en justitiële samenwerking gesloten, alsook andere soorten regelingen met partnerlanden. Zij streeft actief aanvullende internationale overeenkomsten na, in overeenstemming met de onderhandelingsrichtsnoeren van de Raad, alsook initiatieven voor capaciteitsopbouw, die worden gefaciliteerd door EU-agentschappen en -organen. NDICI — Europa in de wereld is ook cruciaal voor het versterken van de veiligheid samen met partnerlanden.

De **op regels gebaseerde internationale orde** is een hoeksteen om de wereldwijde veiligheid te versterken. Veiligheidsdialogen, waaronder thematische dialogen, zijn van vitaal belang om deze inspanningen op te voeren. De uitvoering van het **strategisch kompas voor veiligheid en defensie**, samen met bilaterale en multilaterale samenwerkingskaders zoals stabilisatie- en associatieovereenkomsten en associatieovereenkomsten, en samenwerking met organisaties zoals de VN en de NAVO, zijn cruciaal om tot doeltreffende veiligheidsoplossingen te komen. De EU zal haar rol in multilaterale fora[84] blijven spelen en haar samenwerking versterken met relevante internationale en regionale organisaties en kaders, waaronder de NAVO, de Verenigde Naties, de Raad van Europa, Interpol, de G7, de OVSE en het maatschappelijk middenveld.

Regionale samenwerking

Als Het voortzetten van de onwrikbare steun van de EU aan **Oekraïne** en het versterken van de veiligheid en veerkracht van de **uitbreidingslanden van de EU** heeft hoge prioriteit en is een politieke en geostrategische noodzaak. Het ondersteunen van de veiligheid van de EU moet hand in hand gaan met de **versnelde integratie van de kandidaat-lidstaten in de veiligheidsarchitectuur van de EU**, tegelijkertijd met de consolidatie van hun regionale samenwerking. De Commissie zal het uitbreidingsbeleid van de EU gebruiken om de capaciteiten van kandidaat-lidstaten en potentiële kandidaat-lidstaten van de EU te ondersteunen. Zo kan worden gereageerd op dreigingen, kunnen de operationele samenwerking en informatie-uitwisseling worden verbeterd en kan de afstemming op de beginselen, wetgeving en instrumenten van de EU worden gewaarborgd. Het instrument voor pretoetredingssteun (IPA III) en de faciliteiten voor Oekraïne, Moldavië en de Westelijke Balkan zijn cruciaal voor het versterken van de veiligheid in zowel kandidaat-lidstaten als potentiële kandidaat-lidstaten.

De EU zal ook de **nabuurschapspartners** verder integreren in de veiligheidsarchitectuur van de EU. Via het **nieuwe pact voor het Middellandse Zeegebied** en de komende **strategische aanpak voor de Zwarte Zee** zal de Unie streven naar het opbouwen van regionale samenwerking en bilaterale strategische omvattende partnerschappen met een veiligheidsdimensie, in voorkomend geval, met regelmatige veiligheidsdialogen op hoog niveau. De operationele samenwerking met Noord-Afrika, het **Midden-Oosten en de Golfregio** zal worden versterkt, met name op het gebied van terrorismebestrijding, de bestrijding van witwassen, de illegale vuurwapenhandel en de productie van en handel in drugs, met name Captagon.

[84] Het Mondiaal Forum Terrorismebestrijding, de wereldwijde coalitie tegen Da'esh, het wereldwijd internetforum ter bestrijding van terrorisme, de Christchurch Call Foundation, de Global Coalition to Address Synthetic Drug Threats.

Om de toename van terroristische en criminele activiteiten en de mogelijke overloopeffecten daarvan in **Afrika bezuiden de Sahara, met name de Sahel, de Hoorn van Afrika en West-Afrika** aan te pakken, zal de EU de steun aan de Afrikaanse Unie, de regionale economische gemeenschappen en de landen in de regio opvoeren. In overeenstemming met de strategie van de Europese Unie voor maritieme veiligheid[85] zal de EU de samenwerking in de **Golf van Guinee, de Rode Zee en de Indische Oceaan** om mensenhandel en piraterij aan te pakken, versterken door steun te verlenen aan de samenwerking binnen Afrika en de regionale samenwerking, en met steun van de gecoördineerde maritieme aanwezigheid van de EU en het Maritiem Analyse- en Operatiecentrum op het gebied van verdovende middelen (MAOC-N).

De EU zal de operationele samenwerking met **Latijns-Amerika en het Caribisch gebied** versterken om criminele netwerken met een hoog risico te ontmantelen en te vervolgen en illegale activiteiten en smokkelroutes te ontwrichten, door samenwerkingskaders te versterken, zoals EU-CLASI (Latijns-Amerikaans Comité voor binnenlandse veiligheid) en het coördinatie- en samenwerkingsmechanisme inzake drugs. Tot de prioriteiten zullen de veerkracht en partnerschappen van logistieke hubs en de "follow-the-money"-benaderingen behoren. De EU zal de ontwikkeling van de Politiegemeenschap van Noord- en Zuid-Amerika (Ameripol) verder ondersteunen om het regionale equivalent van Europol te worden, en de justitiële samenwerking tussen de lidstaten en de regio versterken. De EU zal ook met **Zuid- en Centraal-Azië** samenwerken aan gemeenschappelijke veiligheidsuitdagingen in verband met terrorisme, handel in illegale goederen, waaronder drugs, mensenhandel en migrantensmokkel.

Daarnaast zal de EU regionale samenwerkingskaders in derde landen ondersteunen om hen verder te helpen illegale handel aan de bron een halt toe te roepen, in overeenstemming met het beginsel van gedeelde verantwoordelijkheid voor de gehele criminele toeleveringsketen. Bovendien zal de EU haar bijdrage leveren om de veiligheid van logistieke hubs in het buitenland te helpen versterken door **gezamenlijke inspecties in havens van derde landen** te coördineren.

Operationele samenwerking

Global Gateway zal duurzame en hoogwaardige infrastructuurprojecten in de digitale, klimaat- en energie-, vervoers-, gezondheids-, onderwijs- en onderzoekssectoren ondersteunen. De Commissie zal nu, waar relevant, veiligheidsoverwegingen opnemen in de toekomstige Global Gateway-investeringen. Hieronder vallen initiatieven die van cruciaal belang zijn voor de strategische autonomie van de EU en haar partnerlanden, zoals infrastructuurprojecten die veiligheidsbeoordelingen en risicobeperkende maatregelen omvatten.

De Commissie zal streven naar verdere **overeenkomsten tussen de EU en derde landen inzake samenwerking met Europol en Eurojust**, met name met Latijns-Amerikaanse landen.

Daarnaast is de proactieve deelname van niet-EU-landen aan **Empact** een van de meest doeltreffende middelen om de operationele samenwerking te versterken. De EU zal de betrokkenheid van derde landen, met name de Westelijke Balkan, het oostelijk nabuurschap, Afrika bezuiden de Sahara, Noord-Afrika, het Midden-Oosten, Latijns-Amerika en het Caribisch gebied, bij het kader verder aanmoedigen. Een ander instrument om de samenwerking met derde landen op het gebied van misdaadbestrijding te intensiveren, zijn de operationele taskforces tussen de lidstaten die door Europol worden gecoördineerd, waaraan derde landen kunnen deelnemen. De Commissie streeft er ook naar de onderhandelingen over de

[85] JOIN (2023) 8 final.

internationale overeenkomst tussen de **EU en Interpol**[86] af te ronden, om te zorgen voor een meer eensgezinde aanpak van mondiale veiligheidsdreigingen en grensoverschrijdende criminaliteit te bestrijden.

De **Unie moet ter plaatse aanwezig zijn in het kader van een Team Europa-aanpak**. Gespecialiseerd personeel van de Unie en de lidstaten speelt een cruciale rol om ervoor te zorgen dat het externe optreden van de Unie met kennis van zaken, gecoördineerd en responsief is. Om deze aanpak naar een hoger niveau te tillen, zal de Commissie, ondersteund door de hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid, de **verbindingsnetwerken** versterken en de inzet van regionale **verbindingsofficieren van Europol en Eurojust** vergemakkelijken, in overeenstemming met de operationele behoeften van de lidstaten.

De EU zal streven naar nauwere operationele samenwerking op het gebied van rechtshandhaving en justitiële samenwerking, en zal de uitwisseling van informatie in real time en gezamenlijke operaties via **gemeenschappelijke onderzoeksteams** in derde landen bevorderen, met de steun van Europol en Eurojust. De Commissie zal de lidstaten ook ondersteunen bij het opzetten van **gezamenlijke fusiecentra** waarin deskundigen en lokale rechtshandhavingsinstanties in strategische derde landen worden samengebracht.

Instrumenten in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB)

De **missies in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB)** zullen ook optimaal worden benut om externe bedreigingen voor de interne veiligheid van de EU beter in kaart te brengen en aan te pakken, in overeenstemming met hun door de Raad vastgestelde mandaten. Om de capaciteiten van derde landen op te bouwen, zullen de hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid en de Commissie acties in het kader van het gemeenschappelijk veiligheids- en defensiebeleid ondersteunen met specifieke financieringsinstrumenten en alle geschikte financieringsmogelijkheden onderzoeken.

Beperkende maatregelen van de EU zijn een beproefd GBVB-instrument, dat ook wordt gebruikt in de strijd tegen terrorisme. Op basis van suggesties van de hoge vertegenwoordiger voor buitenlandse zaken en veiligheidsbeleid, de lidstaten of de Commissie zou de Raad kunnen beoordelen hoe de bestaande autonome beperkende maatregelen van de EU (terroristenlijst van de EU) doeltreffender, operationeler en flexibeler kunnen worden gemaakt. Bovendien zouden zij kunnen overwegen aanvullende beperkende maatregelen tegen criminele netwerken te onderzoeken, in overeenstemming met de doelstellingen van het gemeenschappelijk buitenlands en veiligheidsbeleid.

Visumbeleid en informatie-uitwisseling

Het visumbeleid van de EU is een belangrijk instrument om met derde landen samen te werken en onze grenzen te beveiligen door de toegang tot de EU te controleren en de voorwaarden daarvoor vast te stellen. De Commissie zal **veiligheidsoverwegingen volledig opnemen in het visumbeleid van de EU** via een komende EU-visumbeleidsstrategie. De Commissie zal met de medewetgevers samenwerken om het voorstel tot herziening en stroomlijning van het opschortingsmechanisme goed te keuren, met name voor specifieke gevallen van misbruik van de visumvrije regeling[87]. Derde landen zullen worden aangemoedigd om informatie uit te

[86] Besluit (EU) 2021/1312 van de Raad van 19 juli 2021 en Besluit (EU) 2021/1313 van de Raad van 19 juli 2021.
[87] COM (2023) 642.

wisselen over personen die een bedreiging voor de veiligheid kunnen vormen, die in de informatiesystemen en gegevensbanken van de EU zal worden ingevoerd.

Om tot beleidscoördinatie en inspanningen aan de bron te komen en een efficiëntere, snellere en soepelere samenwerking tot stand te brengen, zal de Commissie werken aan het vaststellen van **regelingen voor gegevensstromen** en zal zij nagaan hoe de **informatie-uitwisseling** voor rechtshandhaving en grensbeheer met betrouwbare derde landen kan worden **verbeterd**, met inachtneming van de grondrechten en de regels inzake gegevensbescherming.

Kernacties

De Commissie zal:

- **internationale overeenkomsten sluiten tussen de EU en prioritaire derde landen inzake samenwerking met Europol en Eurojust;**
- **de deelname van partnerlanden aan Empact aanmoedigen om georganiseerde misdaad en terrorisme te bestrijden;**
- **EU-agentschappen en -organen ondersteunen bij het opzetten en versterken van werkafspraken met partnerlanden;**
- **veiligheidsoverwegingen verder in aanmerking nemen in het visumbeleid van de EU via de komende visumstrategie;**
- **de informatie-uitwisseling met betrouwbare derde landen met het oog op rechtshandhaving en grensbeheer versterken.**

De Commissie zal, in samenwerking met de hoge vertegenwoordiger voor buitenlandse zaken:

- **civiele missies in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) optimaal benutten;**
- **uiterlijk in 2027 gezamenlijke inspecties in havens van derde landen coördineren.**

De Commissie zal, in samenwerking met de hoge vertegenwoordiger voor buitenlandse zaken en de lidstaten:

- **verbindingsnetwerken en samenwerking in het kader van een Team-Europa-aanpak versterken;**
- **vanaf 2025 gezamenlijke operationele teams en fusiecentra in derde landen opzetten.**

Het Europees Parlement en de Raad worden aangespoord om:

- **de onderhandelingen over de herziening van het opschortingsmechanisme voor de vrijstelling van de visumplicht af te ronden.**

8. Conclusie

In een wereld van onzekerheid moet het vermogen van de Unie om op veiligheidsdreigingen te anticiperen, deze te voorkomen en erop te reageren, worden verbeterd.

Het volstaat niet om pas op crises te reageren wanneer deze zich voordoen. Wij moeten onze bewustwording vergroten met een volledig beeld van de veranderende dreigingen. Ook moeten wij ervoor zorgen dat onze instrumenten en capaciteiten tegen de taak opgewassen zijn.

De uitgebreide reeks maatregelen die in deze strategie worden beschreven, zal helpen een sterkere Unie in de wereld tot stand te brengen: een Unie die in staat is te anticiperen op, plannen te maken voor en te voorzien in haar eigen veiligheidsbehoeften, die op doeltreffende wijze kan

reageren op dreigingen voor haar interne veiligheid en daders ter verantwoording kan roepen, en die haar open, vrije en welvarende samenlevingen en democratieën beschermt.

Hiervoor is een mentaliteitsverandering op het gebied van interne veiligheid nodig. Wij zullen werken aan de bevordering van een nieuwe veiligheidscultuur in de EU, waarin veiligheidsoverwegingen in al onze wetgeving, beleidsmaatregelen en programma's, van aanvang tot uitvoering, in aanmerking worden genomen. En waar samenwerking tussen beleidsterreinen ons in staat stelt om nieuwe terreinen te verkennen.

Dit is niet de taak van slechts één instelling, regering of actor. Het is een gezamenlijke inspanning van Europa.