Raad van de
Europese Unie

Brussel, 18 oktober 2023
(OR. en)

**14372/23**

| | |
|---|---|
| **JAI 1332** | **COPEN 363** |
| **COSI 179** | **FREMP 292** |
| **ENFOPOL 431** | **JAIEX 66** |
| **ENFOCUSTOM 110** | **CFSP/PESC 1410** |
| **IXIM 194** | **COPS 489** |
| **CT 155** | **HYBRID 73** |
| **CRIMORG 137** | **DISINFO 85** |
| **FRONT 327** | **TELECOM 306** |
| **ASIM 92** | **DIGIT 223** |
| **VISA 208** | **COMPET 1008** |
| **CYBER 247** | **RECH 456** |
| **DATAPROTECT 278** | **CULT 122** |
| **CATS 58** | **COTER 185** |
| **DROIPEN 151** | **CORDROGUE 94** |

**BEGELEIDENDE NOTA**

| | |
|---|---|
| van: | de secretaris-generaal van de Europese Commissie, ondertekend door mevrouw Martine DEPREZ, directeur |
| ingekomen: | 18 oktober 2023 |
| aan: | mevrouw Thérèse BLANCHET, secretaris-generaal van de Raad van de Europese Unie |
| nr. Comdoc.: | COM(2023) 665 final |
| Betreft: | MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD over het zesde voortgangsverslag over de uitvoering van de EU-strategie inzake de veiligheidsunie |

Hierbij gaat voor de delegaties document COM(2023) 665 final.

Bijlage: COM(2023) 665 final

EUROPESE
COMMISSIE

Brussel, 18.10.2023
COM(2023) 665 final

# MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

## over het zesde voortgangsverslag over de uitvoering van de EU-strategie inzake de veiligheidsunie

# I. Inleiding

Drie jaar geleden heeft de Commissie de strategie voor de veiligheidsunie 2020-2025[1] vastgesteld waarin de hoofdprioriteiten voor de Unie op het gebied van de beveiliging werden gedefinieerd. Sindsdien hebben we grote vooruitgang geboekt bij alle vier de pijlers van de strategie, met baanbrekende wetgeving op alle gebieden, van bescherming van kritieke entiteiten tot vergroting van de cyberweerbaarheid. Ondertussen blijft het landschap van veiligheidsbedreigingen in Europa en onze buurlanden echter evolueren. De recente terroristische aanslagen in een van onze scholen in Frankrijk en in de straten van Brussel herinneren ons nog maar eens aan de urgentie en noodzaak om onze beveiligingsarchitectuur te blijven aanpassen en versterken. Het gevaar van cyberaanvallen blijft toenemen, ook omdat kwaadwillige actoren partij kiezen in de lopende conflicten. Hybride bedreigingen, waaronder desinformatie, blijven zich verveelvoudigen. Europol heeft de Russische aanvalsoorlog tegen Oekraïne aangewezen als de oorzaak van een aanzienlijke toename in de cyberaanvallen tegen EU-doelen, waarbij grote aanvallen politiek gemotiveerd zijn en gecoördineerd worden door pro-Russische hackersgroepen[2]. Dit heeft geleid tot de blokkering van de internettoegang en onderbreking van essentiële diensten zoals energienetwerken[3].

De strategie voor de veiligheidsunie werd ontworpen om de EU beter te wapenen tegen een veranderend dreigingslandschap. Toen we werden geconfronteerd met de crises die de pandemie en oorlog met zich meebrachten, hebben de gebeurtenissen het belang aangetoond van de aanpak waarvoor in de strategie is gekozen: onze vastberadenheid om de punten binnen het hele veiligheidsecosysteem van de EU met elkaar te verbinden en de silo's tussen de cyber- en fysieke dimensies van de beveiliging te doorbreken, waaronder de aanpak van georganiseerde criminaliteit en terrorisme en de bestrijding van radicalisering.

Waakzaamheid vereist echter dat we voortdurend onderzoeken wat er ontbreekt bij onze inspanningen om onze burgers veilig te houden. In de strategie zijn prioritaire gebieden vastgesteld waarop de Unie een toegevoegde waarde kan bieden teneinde de lidstaten te ondersteunen bij het bevorderen van de veiligheid voor alle mensen die in Europa wonen. Sinds de vaststelling ervan zijn alle voorgenomen acties uitgevoerd en zijn er nieuwe in opgenomen om te reageren op de voortdurende veiligheidsuitdagingen.

In totaal heeft de Commissie 36 wetgevingsinitiatieven in het kader van de strategie voor de veiligheidsunie gepresenteerd. Voor meer dan de helft van deze voorstellen zijn de interinstitutionele onderhandelingen reeds met solide nieuwe wetgeving afgesloten, zoals beschreven in de tabel in de bijlage. Over verschillende belangrijke initiatieven die de Commissie heeft voorgesteld, wordt echter nog steeds onderhandeld door het Europees Parlement en de Raad. Nu de huidige parlementaire zittingsperiode ten einde loopt en in juni 2024 Europese verkiezingen zullen worden gehouden, moet er spoed worden gezet achter deze lopende dossiers, zodat de burgers ten volle van de veiligheidsunie kunnen profiteren. In dit zesde voortgangsverslag over de veiligheidsunie ligt daarom de nadruk op deze door de

[1] COM(2020) 605 final.

[2] DDoS-aanvallen (Distributed Denial of Service attacks): zie het Spotlight Report "Cyber-attacks: the apex of crime-as-a-service" van Europol van 13 september 2023.

[3] Tijdens het conflict in Oekraïne is op grote schaal gebruik gemaakt van "malware wipers" om gegevens en systemen te vernietigen, waardoor bijvoorbeeld de internettoegang van duizenden abonnees in de EU werd verstoord en een groot Duits energiebedrijf de toegang tot monitoring op afstand van meer dan 5 800 windturbines verloor. "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict", studie van het Europees Parlement, september 2023 — PE 702.594.

Commissie goedgekeurde, cruciale wetgevings- en niet-wetgevingsdossiers met betrekking tot de veiligheidsunie waarvoor meer zal moeten worden gedaan om deze af te ronden en op doeltreffende wijze uit te voeren.

Van de voordelen van EU-wetgeving waarover reeds overeenstemming is bereikt, zal men pas wat merken wanneer deze in de praktijk zijn gebracht. De werkzaamheden zullen zich moeten toespitsen op de correcte en volledige omzetting, uitvoering en toepassing ervan door de lidstaten. In 2023 is de Commissie erop blijven toezien dat de EU-strategie voor de veiligheidsunie ook wordt waargemaakt, waarvoor zij gebruik heeft gemaakt van haar institutionele bevoegdheden om inbreukprocedures in te leiden wanneer lidstaten EU-wetgeving niet of onjuist hadden omgezet.

In dit verslag wordt ook samengevat wanneer de actie van lidstaten en/of EU-instanties cruciaal is voor dit resultaat. EU-instanties spelen een cruciale rol bij ondersteuning van de uitvoering van de initiatieven voor de veiligheidsunie, en hun verantwoordelijkheden zijn de afgelopen jaren toegenomen. In het verslag worden enkele van de belangrijkste nieuwe taken beschreven die hen zijn toegewezen om de lidstaten beter te ondersteunen bij de uitvoering van belangrijke initiatieven in het kader van de veiligheidsunie.

Daarnaast heeft de geopolitieke situatie het belang van de externe veiligheid voor onze interne veiligheid benadrukt. Een sterker intern EU-kader op het gebied van de veiligheid is onlosmakelijk verbonden met sterkere partnerschappen en samenwerking met derde landen. De EU moet actief blijven onderzoeken hoe wereldwijde betrokkenheid kan helpen om de veiligheid van de burgers thuis te waarborgen.

## II. Een toekomstbestendige veiligheidsomgeving

### *Cyberbeveiliging en weerbaarheid van kritieke infrastructuur*

In het kader van de veiligheidsunie wil de Unie ervoor zorgen dat alle Europese burgers en bedrijven online en offline goed worden beschermd, en streeft zij een open, veilige en stabiele cyberspace na. De toenemende omvang, frequentie en impact van cyberbeveiligingsincidenten vormen een grote bedreiging voor de werking van zowel netwerk- en informatiesystemen als de interne markt. De aanvalsoorlog van Rusland tegen Oekraïne heeft deze dreiging nog verergerd en de huidige geopolitieke spanningen worden nog eens versterkt door interventies van een veelheid van aan staten gelieerde, criminele en hacktivistische actoren. De sabotage aan de Nord Stream-pijpleidingen van vorig najaar heeft duidelijk gemaakt hoezeer essentiële sectoren zoals energie, digitale infrastructuur, vervoer en ruimtevaart afhankelijk zijn van een weerbare kritieke infrastructuur. Het recente incident met een onderzeese gaspijpleiding en datakabel tussen Estland en Finland illustreert de noodzaak van een hoog niveau van paraatheid om dit soort situaties het hoofd te kunnen bieden. Hoewel de oorzaak van de schade onduidelijk blijft en de onderzoeken nog lopen, is de uitwisseling van informatie op verschillende niveaus tussen lidstaten en de Commissie bemoedigend geweest. De onderbrekingen hadden geen onmiddellijke gevolgen voor de internetconnectiviteit of de continuïteit van de gasvoorziening op Europees of lokaal niveau. Dit illustreert de geboekte vooruitgang en de versterkte paraatheidsinspanningen van de afgelopen maanden.

Een duidelijk en robuust rechtskader is daarom van essentieel belang voor de waarborging van de bescherming en weerbaarheid van deze kritieke infrastructuren. In dit verband is een cruciale doorbraak bereikt met de gelijktijdige goedkeuring van de herziene richtlijn betreffende

maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie[4] (NIS 2) en de richtlijn betreffende de weerbaarheid van kritieke entiteiten[5] (CER), die beide op 16 januari 2023 in werking zijn getreden. De lidstaten worden nu aangespoord om deze fundamentele stukken wetgeving snel en volledig om te zetten, maar uiterlijk op 17 oktober 2024, teneinde een robuust Uniekader op te zetten ter bescherming van kritieke infrastructuur van de Unie tegen fysieke en cyberdreigingen.

In juli 2023 heeft de Commissie in een gedelegeerde verordening essentiële diensten vastgesteld in de elf sectoren die onder de CER-richtlijn[6] vallen. De volgende stap is dat de lidstaten risicobeoordelingen uitvoeren voor deze diensten. Naar aanleiding van de aanbeveling van de Raad[7] van 8 december 2022 wordt er intensiever gewerkt aan stresstests voor kritieke infrastructuur, waaronder om te beginnen de energiesector, en aan de versterking van de samenwerking met de NAVO en belangrijke partnerlanden. Deze werkzaamheden hebben in juni 2023 geleid tot een verslag van de taskforce van de EU en NAVO over de weerbaarheid van kritieke infrastructuur, waarin de huidige beveiligingsuitdagingen voor de kritieke infrastructuur in vier belangrijke sectoren (energie, vervoer, digitale infrastructuur en ruimte) in kaart zijn gebracht en aanbevelingen worden gedaan om de weerbaarheid te vergroten. De aanbevelingen, onder meer over meer coördinatie, informatie-uitwisseling en oefeningen, worden door de personeelsleden van de EU en de NAVO uitgevoerd in het kader van de gestructureerde dialoog over weerbaarheid.

Daarnaast heeft de Commissie op 6 september 2023 een voorstel[8] goedgekeurd voor een aanbeveling van de Raad over een blauwdruk ter verbetering van de coördinatie op EU-niveau in reactie op pogingen om kritieke infrastructuur van aanzienlijk grensoverschrijdend belang te verstoren. Op 4 oktober 2023 werd een oefening georganiseerd in de vorm van een op scenario's gebaseerde discussie over de blauwdruk, om te testen hoe deze in de praktijk zou worden toegepast en om informatie te verschaffen voor de lopende onderhandelingen over het voorstel in de Raad.

Naar aanleiding van oproepen van de Raad[9] hebben de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep risicobeoordelingen uitgevoerd en risicoscenario's opgesteld vanuit een oogpunt van cyberbeveiliging. Dit werk is in eerste instantie gericht op de sectoren telecommunicatie en elektriciteit. De betrokkenheid van alle relevante instanties en netwerken, zowel civiel als militair, heeft voor het eerst geleid tot een uitgebreide en inclusieve beoordeling voor de hele Unie. Deze vormt een verdere aanvulling op de gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens in het kader van NIS 2, evenals de risicobeoordelingen en stresstests van kritieke infrastructuur in de sectoren energie, digitale infrastructuur, communicatie, vervoer en ruimtevaart. In het belang van de coördinatie en samenhang zouden deze activiteiten op elkaar moeten voortbouwen om tot een standaardaanpak te komen, en zouden deze als leidraad moeten dienen voor de ontwikkeling van toekomstige

---

4 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).

5 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.

6 COM(2023) 4878 final.

7 Aanbeveling van de Raad van 8 december 2022 betreffende een Uniebrede gecoördineerde aanpak om de weerbaarheid van kritieke infrastructuur te versterken.

8 COM(2023) 526 final.

9 Conclusies van de Raad van 23 mei 2022 over de ontwikkeling van de cyberstrategie van de Europese Unie en de oproep van Nevers van 9 maart 2022 om de cyberbeveiligingscapaciteiten van de EU te versterken.

oefeningen. Het succes van deze acties zal nu afhangen van de actieve betrokkenheid van de lidstaten.

Het functioneren van economieën en samenlevingen is in toenemende mate afhankelijk van ruimtegerelateerde diensten en gegevens, vooral op het gebied van veiligheid en defensie. De ruimte is een strategisch domein dat door een steeds intensievere concurrentie wordt gekenmerkt en het belang ervan voor de veiligheid is vooral toegenomen in de nasleep van de Russische invasie in Oekraïne. De ruimtestrategie voor veiligheid en defensie van de Europese Unie is in maart 2023 aangenomen ter versterking van onze strategische positie en autonomie in de ruimte. Als belangrijkste actie die uit deze strategie is voortgevloeid, zal de Europese Commissie in 2024 een EU-ruimtewet voorstellen die de veiligheid, duurzaamheid en veerkracht/veiligheid van ruimteactiviteiten in de EU zal regelen.

Wat de externe dimensie betreft, ondersteunt een veilige infrastructuur de veerkracht van de wereldeconomie en de toeleveringsketens[10], en om die reden omvat de Global Gateway-strategie van de EU een sterke veiligheidsdimensie. Gezien de onderlinge verbindingen tussen de infrastructuur van de EU en partnerlanden is verdere internationale samenwerking evenzeer van essentieel belang voor de versterking van de mondiale cyberweerbaarheid en ondersteuning van een vrije, open, veilige en beveiligde cyberspace.

***Verordening cyberweerbaarheid***

Het is van cruciaal belang voor de Europese cyberbeveiliging dat consumenten en bedrijven kunnen vertrouwen op veilige digitale producten. Met haar voorstel voor een verordening cyberweerbaarheid[11], dat op 15 september 2022 is vastgesteld, wil de Commissie in deze behoefte voorzien. De verordening zou verplichte horizontale cyberbeveiligingsvereisten invoeren waaraan producten met digitale elementen gedurende vijf jaar of hun hele levenscyclus (afhankelijk van wat korter is) zouden moeten voldoen. In de verordening zouden de voorwaarden worden geschept voor het ontwerp en de ontwikkeling van veilige producten met digitale elementen, door ervoor te zorgen dat hardware- en softwareproducten met zo weinig mogelijk kwetsbaarheden op de markt worden gebracht. Dit zou een belangrijke mijlpaal zijn bij de verhoging van de Europese cyberbeveiligingsnormen op alle gebieden en waarschijnlijk een internationaal referentiepunt worden, wat de cyberbeveiligingsbranche van de Unie duidelijke voordelen op de wereldmarkten oplevert. Het Europees Parlement en de Raad hebben hun respectieve standpunten in juli 2023 vastgesteld en de onderhandelingen zouden snel moeten kunnen vorderen.

Cyberbeveiligingscertificering speelt ook een cruciale rol bij de vergroting van het vertrouwen in ICT-producten en -diensten, en stelt consumenten, bedrijven en overheden in staat om weloverwogen keuzes te maken met een passend niveau van cyberbeveiliging. De werkzaamheden aan de cyberbeveiligingscertificering zijn gaande, en bevinden zich momenteel in de fase waarin de Europese op gemeenschappelijke criteria gebaseerde cyberbeveiligingscertificeringsregeling wordt beoordeeld in de comitéprocedure. Het agentschap van de Europese Unie voor cyberbeveiliging (Enisa) bereidt momenteel een potentiële EU-certificeringsregeling voor cloudbeveiliging (EUCS) voor die wordt besproken in de Europese Groep voor cyberbeveiligingscertificering. De intensieve samenwerking met deskundigen uit verschillende sectoren, consumenten en leveranciers moet leiden tot een degelijke juridische en technische aanpak die de nodige veiligheidsgaranties biedt in overeenstemming met het recht van de Unie, internationale verbintenissen en WHO-verplichtingen. Daarnaast bereidt Enisa de potentiële EU5G-regeling en de Europese

[10] JOIN(2021) 30 final.
[11] COM(2022) 454 final.

portemonnees voor digitale identiteit (EUIDW) voor. Voor de verbetering van de totale veiligheid van ICT-producten, ICT-diensten en ICT-processen zijn gecoördineerde inspanningen van alle lidstaten essentieel.

***Verordeningen inzake informatie- en cyberbeveiliging voor instellingen, organen en instanties van de EU***

De voorgestelde verordeningen voor de regeling van de cyberbeveiliging en informatiebeveiliging voor de eigen instellingen van de Unie, die in maart 2022 samen werden voorgesteld, hebben een verschillend ontwikkelingstempo doorgemaakt. Afgelopen juni werd een politiek akkoord bereikt over de cyberbeveiligingsverordening, waarmee alle EU-instellingen, -organen en -instanties hun cyberbeveiligingsstrategie kunnen versterken, en waaruit blijkt dat de EU veel belang hecht aan een snelle uitvoering van dit voorstel. In deze situatie is het bijzonder zorgwekkend dat er bij het parallelle voorstel over informatiebeveiliging, dat essentieel is voor de completering van een solide wetgevingskader voor instellingen, organen en instanties, onverwacht trage vorderingen worden gemaakt. Beide voorstellen zouden voor de Europese parlementsverkiezingen moeten worden aangenomen om het Europese bestuur geloofwaardig en veerkrachtig te maken in de huidige geopolitieke context. Een minimumpakket van voorschriften en normen voor informatiebeveiliging voor alle instellingen, organen en instanties van de EU zou alle betrokken partijen zekerheid bieden en zorgen voor een consistente bescherming tegen zich ontwikkelende bedreigingen voor hun gerubriceerde en niet-gerubriceerde gegevens. Samen zouden deze nieuwe voorschriften een stabiele basis vormen voor een veilige uitwisseling van informatie tussen instellingen, organen en instanties en met lidstaten, met gestandaardiseerde praktijken en maatregelen ter bescherming van de informatiestromen. Als zodanig komen zij tegemoet aan meerdere oproepen van de Raad om de veerkracht van de instellingen, organen en instanties te vergroten en het besluitvormingsproces van de Unie beter tegen kwaadwillige inmenging te beschermen.

***Verordening cybersolidariteit***

Het op 18 april 2023 door de Commissie goedgekeurde voorstel voor een verordening cybersolidariteit[12], waarin wordt voortgebouwd op het reeds bestaande sterke strategische beleids- en wetgevingskader, zou de opsporing van cyberdreigingen, de weerbaarheid en de paraatheid op alle niveaus van het cyberbeveiligingsecosysteem van de Unie verder verbeteren. Deze doelstellingen zouden worden uitgevoerd via drie hoofdacties:

(1) De invoering van een ***Europees cyberschild*** om gemeenschappelijke capaciteiten op het gebied van opsporing en situationeel bewustzijn op te bouwen en te versterken. Het cyberschild zou bestaan uit alle nationale centra voor beveiligingsoperaties ("nationale SOC's") en landsgrensoverschrijdende centra voor beveiligingsoperaties ("landsgrensoverschrijdende SOC's").
(2) De instelling van een ***cybernoodmechanisme*** om de lidstaten te ondersteunen bij de voorbereiding en respons op, en het onmiddellijke herstel van significante en grootschalige cyberbeveiligingsincidenten. Tot de steun voor respons bij incidenten zou de EU-cyberbeveiligingsreserve behoren, die ook beschikbaar zou zijn voor Europese instellingen, organen en instanties van de Unie, en voor derde landen die geassocieerd zijn met het programma Digitaal Europa, mits hun associatieovereenkomst met het programma Digitaal Europa daarin voorziet.
(3) De instelling van een ***Europees evaluatiemechanisme voor cyberbeveiligingsincidenten*** om specifieke significante of grootschalige incidenten te

[12] COM(2023) 209 final.

evalueren en te beoordelen. Het verslag van de post-incidentenevaluatie zou worden gecoördineerd en opgesteld door Enisa.

De besprekingen in de Raad en het Europees Parlement zijn gestart. Afronding van de onderhandelingen vóór het einde van het huidige mandaat van het Europees Parlement zou een belangrijke impuls geven aan de inspanningen ter bescherming van burgers en bedrijven in de hele Unie.

***Academie voor cyberbeveiligingsvaardigheden***

Omdat cyberdreigingen toenemen, heeft de EU dringend behoefte aan professionals met de vaardigheden en competenties om cyberaanvallen te voorkomen, op te sporen, af te schrikken en de EU te verdedigen tegen dergelijke aanvallen. De behoefte aan arbeidskrachten op het gebied van cyberbeveiliging wordt momenteel geschat op 883 000 professionals, terwijl het aantal onvervulde vacatures in 2022 tussen de 260 000 en 500 000 lag. Alle geledingen van de maatschappij moeten worden aangemoedigd om deze lacune te helpen dichten, maar met name in 2022 vertegenwoordigden vrouwen slechts 20 % van de afgestudeerden in cyberbeveiliging en 19 % van de specialisten in informatie- en communicatietechnologie. In het kader van het Europees Jaar van de Vaardigheden in 2023 heeft de Commissie op 18 april 2023[13] een door de lidstaten verwelkomd initiatief goedgekeurd[14] om een Academie voor cyberbeveiligingsvaardigheden op te richten teneinde het tekort aan cyberbeveiligingsprofessionals weg te werken. De Academie voor cyberbeveiligingsvaardigheden zou bestaande initiatieven op het gebied van cyberbeveiligingsvaardigheden bij elkaar brengen en de coördinatie verbeteren. De Commissie moedigt lidstaten, regionale en lokale autoriteiten, evenals Europese openbare instanties aan om specifieke strategieën of initiatieven op het gebied van de cyberbeveiligingsvaardigheden vast te stellen of om cyberbeveiligingsvaardigheden te integreren in relevante strategieën of initiatieven met een breder toepassingsgebied (bv. cyberbeveiliging, digitale vaardigheden, werkgelegenheid enz.) Ook de betrokkenheid van particuliere belanghebbenden zal van essentieel belang zijn voor het opvullen van de lacunes op het gebied van cyberbeveiligingsvaardigheden en het verkleinen van het daarmee samenhangende tekort aan arbeidskrachten in Europa.

***Drones***

Een andere toenemende bedreiging voor openbare ruimten en kritieke infrastructuren is het kwaadwillige gebruik van drones. Incidenten met drones komen steeds vaker voor, zowel binnen als buiten de Unie, en antidrone-oplossingen zijn een belangrijk instrument voor rechtshandhaving en andere openbare instanties in de Unie, evenals voor particuliere exploitanten van kritieke infrastructuur. Tegelijkertijd levert het legitieme gebruik van drones een belangrijke bijdrage aan de groene en de digitale transitie[15]. Zoals werd aangekondigd in de Drone-strategie 2.0 die in november 2022 werd goedgekeurd, stelt de Commissie nu een mededeling vast over de wijze waarop potentiële dreigingen van drones kunnen worden tegengegaan, welke wijze wordt ondersteund door twee handboeken met praktische richtsnoeren over belangrijke technische aspecten[16]. Het initiatief is bedoeld om een alomvattend en geharmoniseerd beleidskader te bieden, met een gemeenschappelijke interpretatie van de voorschriften die van kracht zijn om mogelijke dreigingen van drones te bestrijden en waar nodig aan te passen aan snelle technologische ontwikkelingen. Lidstaten en

[13] COM(2023) 207 final.
[14] Conclusies van de Raad van 22 mei 2023 met betrekking tot het EU-beleid op het gebied van cyberdefensie.
[15] COM(2022) 652 final.
[16] COM(2023) 659 final.

relevante particuliere marktdeelnemers worden uitgenodigd nauw met de Commissie samen te werken om de volledige uitvoering ervan te waarborgen.

***Beveiliging van de lucht- en scheepvaart***

Illegale activiteiten, zoals piraterij, gewapende overvallen op zee, smokkel van migranten, mensen-, wapen- en drugshandel, evenals terrorisme, vormen nog altijd een uitdaging voor de maritieme veiligheid en worden nog eens verergerd door evoluerende dreigingen, waaronder hybride en cyberaanvallen. De Commissie en de hoge vertegenwoordiger hebben op 10 maart 2023 een gezamenlijke mededeling aangenomen, waarin de EU-strategie voor maritieme veiligheid[17] wordt geactualiseerd en die nu moet worden uitgevoerd overeenkomstig het geactualiseerde actieplan.

Op het gebied van beveiliging van de luchtvaart heeft de Commissie op 2 februari 2023 een werkdocument van de diensten van de Commissie met de titel "Working towards an enhanced and more resilient aviation security policy"[18] goedgekeurd, dat een ambitieus programma bevat om 1) de regelgevingsstructuur voor de beveiliging van de luchtvaart te moderniseren, 2) de ontwikkeling en toepassing van meer innovatieve oplossingen te bevorderen en 3) het basisniveau van de beveiliging van de luchtvaart te actualiseren, zodat luchthavens in de Unie ten volle kunnen profiteren van nieuwe en geavanceerde technologieën om de grootste prioritaire bedreigingen aan te pakken. Er moeten binnen twee jaar 14 kenacties worden uitgevoerd.

De Commissie roept het Europees Parlement en de Raad op om de onderhandelingen over de volgende dossiers met spoed af te ronden, in ieder geval vóór het einde van het mandaat van het huidige Europees Parlement:

- het voorstel voor een verordening cyberweerbaarheid;
- het voorstel voor een verordening cybersolidariteit;
- de voorgestelde verordening inzake informatiebeveiliging voor instellingen, organen en instanties.

De Commissie roept de lidstaten op om:

- de omzetting van de richtlijn betreffende de weerbaarheid van kritieke entiteiten en de stresstests van kritieke infrastructuur in de energiesector prioriteit te geven;
- de aanbeveling van de Raad betreffende een blauwdruk voor het coördineren van de respons op verstoringen van kritieke infrastructuur van aanzienlijk grensoverschrijdend belang goed te keuren;
- de NIS 2-richtlijn volledig en met spoed om te zetten om de cyberbeveiliging van essentiële en belangrijke entiteiten te verbeteren;
- zich actief bezig te houden met het uitvoeren van risicobeoordelingen op het gebied van cyberbeveiliging en het opstellen van risicoscenario's voor kritieke infrastructuur en toeleveringsketens;
- met een sterke betrokkenheid op Europees niveau opvolging te geven aan de Academie voor cyberbeveiligingsvaardigheden en specifieke nationale strategieën of initiatieven op het gebied van cyberbeveiligingsvaardigheden, en hierbij belangrijke belanghebbenden, waaronder regionale en lokale overheden, te betrekken;

[17] JOIN(2023) 8 final.
[18] SWD(2023) 37 final.

- samen te werken met relevante particuliere exploitanten en de Commissie om te zorgen voor uitvoering van alle acties die worden genoemd in de mededeling over het bestrijden van potentiële dreigingen die van drones uitgaan;
- het actieplan van de EU-strategie voor maritieme beveiliging uit te voeren en regelmatig verslag uit te brengen over de resultaten;
- de 14 geïdentificeerde kernacties voor verbetering van de beveiliging van de luchtvaart uit te voeren.

## III. Aanpak van veranderende dreigingen

Nieuwe geopolitieke spanningen hebben sterk aangetoond dat de veiligheidsuitdaging voor de EU niet alleen toeneemt, maar ook steeds volatieler wordt en geaccentueerd wordt door het hybride karakter van veel dreigingen. Verder moet beveiliging ook inspelen op maatschappelijke en technologische veranderingen. De COVID-19-pandemie leidde tot nieuwe mogelijkheden voor cybercriminelen en in het bijzonder tot een verhoogde dreiging van onlinemateriaal betreffende seksueel misbruik van kinderen. Criminelen en kwaadwillende actoren staan altijd klaar om technologische ontwikkelingen uit te buiten. In het licht van dergelijke vaak complexe en multidimensionale bedreigingen is een krachtig en consistent optreden van de EU vereist.

***Verordening ter bestrijding van online seksueel misbruik van kinderen***

Uit de dreigingsevaluatie van de georganiseerde internetcriminaliteit van Europol is gebleken dat in 2022 zowel de frequentie als de ernst van seksuele uitbuiting en seksueel misbruik van kinderen verder was toegenomen, waarbij daders blijven profiteren van technische mogelijkheden om hun daden en identiteit te maskeren[19]. Het huidige systeem dat gebaseerd is op vrijwillige opsporing en rapportage door bedrijven, is ontoereikend gebleken om kinderen te beschermen. Een tussentijdse verordening staat vrijwillige opsporing en rapportage door bedrijven toe, mits dit rechtmatig is op grond van de algemene verordening gegevensbescherming (AVG). Deze verordening zal in augustus 2024 vervallen. In mei 2022 heeft de Commissie een verordening[20] voorgesteld om het misbruik van onlinediensten voor seksueel misbruik van kinderen aan te pakken. Het voorgestelde kader legt sterk de nadruk op preventie. Bedrijven zouden verplicht worden om het risico op seksueel misbruik van kinderen via hun systemen te beoordelen en preventieve maatregelen te nemen. Alleen in geval van een aanzienlijk risico kunnen nationale rechtbanken of onafhankelijke administratieve autoriteiten als laatste redmiddel gerichte opsporingsbevelen tegen dienstverleners uitvaardigen. Een nieuw onafhankelijk EU-centrum zou de inspanningen van dienstenaanbieders vergemakkelijken door als expertiseknooppunt te fungeren, betrouwbare informatie over geïdentificeerd materiaal te verstrekken, online rapportages van seksueel misbruik van kinderen door aanbieders te ontvangen en te analyseren om foutieve meldingen op te sporen alsmede slachtoffers te ondersteunen. Het is van essentieel belang dat de nieuwe voorschriften zo snel mogelijk worden aangenomen en uitgevoerd om kinderen tegen verder misbruik te beschermen, te voorkomen dat materiaal opnieuw online verschijnt en daders voor het gerecht te brengen. De

[19] Internet Organised Crime Threat Assessment (Iocta) 2023, Europol (2023).
[20] COM(2022) 209 final.

onderhandelingen in de Raad en het Parlement zijn gaande en het streven is dat zij voor het einde van de zittingsperiode van dit Parlement een akkoord over dit dossier bereiken

***Richtlijn ter bestrijding van geweld tegen vrouwen en huiselijk geweld***

Vrouwen krijgen, onder meer in de context van huiselijk geweld, intussen ook te maken met cybergeweld via internet en IT-hulpmiddelen, over de grenzen van de lidstaten heen. In maart 2022 heeft de Commissie een richtlijn voorgesteld voor de aanpak van geweld tegen vrouwen en huiselijk geweld, met specifieke voorschriften voor cybergeweld en maatregelen voor opvulling van de lacunes in de bescherming, toegang tot de rechter en preventie. Een snelle goedkeuring en uitvoering zou de lidstaten extra instrumenten geven voor het bestrijden van deze vorm van criminaliteit. De medewetgevers zijn in juli 2023 begonnen met interinstitutionele onderhandelingen en streven ernaar om de onderhandelingen voor het einde van het huidige mandaat van het Europees Parlement af te ronden.

***5G-cyberbeveiliging***

De beveiliging van 5G-netwerken is een belangrijke prioriteit voor de Commissie en een essentieel onderdeel van haar strategie voor de veiligheidsunie. 5G-netwerken zijn een centrale infrastructuur die de basis vormt voor een breed scala aan diensten die essentieel zijn voor het functioneren van de interne markt en voor vitale maatschappelijke en economische functies. Op 15 juni 2023 hebben de autoriteiten van de EU-lidstaten die in de NIS-samenwerkingsgroep vertegenwoordigd zijn, met steun van de Commissie en Enisa, een tweede voortgangsverslag gepubliceerd over de uitvoering van de EU-toolbox inzake 5G-cyberbeveiliging. Volgens het verslag hebben 24 lidstaten wetgevende maatregelen goedgekeurd of in voorbereiding die nationale autoriteiten de bevoegdheid geven om een beoordeling van leveranciers uit te voeren en beperkingen op te leggen, en hebben 10 lidstaten daadwerkelijk dergelijke beperkingen opgelegd. Er is echter verdere actie nodig ter voorkoming van kwetsbaarheden voor de Unie als geheel, met mogelijk ernstige negatieve gevolgen voor de beveiliging van individuele gebruikers en bedrijven in de hele Unie en de kritieke infrastructuur van de Unie. Alle lidstaten moeten de toolbox onverwijld invoeren. Op dezelfde dag heeft de Commissie een mededeling aangenomen over de uitvoering van de toolbox door de lidstaten en over de eigen interne communicatie van de Commissie en de financieringsactiviteiten van de Unie. Hierin werd de grote bezorgdheid benadrukt over de risico's voor de beveiliging van de EU die leveranciers van mobiele netwerkcommunicatieapparatuur Huawei en ZTE met zich meebrengen. In deze context neemt de Commissie maatregelen om te voorkomen dat haar interne communicatie wordt blootgesteld aan mobiele netwerken die Huawei en ZTE als leveranciers gebruiken. Bij aanbestedingen zullen nieuwe connectiviteitsdiensten die berusten op apparatuur van die leveranciers worden uitgesloten, en de Commissie zal met de lidstaten en telecomexploitanten samenwerken om ervoor te zorgen dat die leveranciers geleidelijk worden verwijderd uit de bestaande connectiviteitsdiensten van de sites van de Commissie. De Commissie onderzoekt ook hoe dit besluit in de relevante financieringsprogramma's en -instrumenten van de Unie en in volledige overeenstemming met het Unierecht kan worden weerspiegeld.

***Toegang tot gegevens voor doeltreffende rechtshandhaving***

In het huidige digitale tijdperk heeft bijna elk strafbaar feit een digitale component. Technologieën en instrumenten worden ook gebruikt voor criminele doeleinden, ook technologieën en instrumenten die nodig zijn om de cyberbeveiliging, gegevensbescherming en privacy in onze samenleving te waarborgen. Hierdoor wordt het steeds moeilijker om voor een effectieve rechtshandhaving in de hele EU te zorgen om de openbare veiligheid te waarborgen en criminaliteit te voorkomen, op te sporen, te onderzoeken en te vervolgen, en hoewel er op het niveau van de Unie en op nationaal niveau aanzienlijke inspanningen zijn

geleverd, onder andere door middel van wetgeving en met behulp van initiatieven op het gebied van capaciteitsopbouw en innovatie, zijn er nog steeds juridische en technische uitdagingen. Met betrekking tot de toegang tot gegevens voor een doeltreffende rechtshandhaving heeft de Commissie, met medewerking van het voorzitterschap van de Raad, een groep op hoog niveau opgericht om een samenwerkingsplatform te bieden voor een breed scala aan belanghebbenden en deskundigen die onderzoek zullen doen naar de uitdagingen waarmee misdaadbestrijdingsautoriteiten worden geconfronteerd (bv. encryptie, bewaring van gegevens, 5G en normalisatie). De Commissie heeft de groep op hoog niveau gevraagd om tegen juni 2024 evenwichtige, solide en haalbare aanbevelingen te formuleren, die de complexiteit van deze kwesties weerspiegelen, mede vanuit het oogpunt van cyberbeveiliging en gegevensbescherming. De lidstaten en deelnemende deskundigen worden daarom aangemoedigd om actief deel te nemen aan dit proces en aan doeltreffende, wettige en algemeen aanvaarde oplossingen te werken.

***Hybride bedreigingen***

In een geopolitieke context waarin hybride dreigingen steeds complexer en geraffineerder worden, biedt het strategisch kompas voor veiligheid en defensie van de EU[21] ("strategisch kompas") een gedeelde beoordeling van de dreigingen en uitdagingen waarmee de Unie wordt geconfronteerd, evenals een strategisch actieplan. De toename van kwaadwillig gedrag in cyberspace door staten en niet-statelijke actoren, waaronder in de context van de oorlog tegen Oekraïne, heeft nog eens extra benadrukt dat cyberspace een gebied voor buitenlands en veiligheidsbeleid is geworden. De potentiële risico's van kwaadwillige acties en desinformatie vragen om bijzondere waakzaamheid in verkiezingsperiodes, zoals in aanloop naar de Europese verkiezingen in 2024.

Gezien de grote risico's van overloopeffecten is de EU doorgegaan met activiteiten voor ontwikkeling van capaciteitsopbouw op het gebied van de cyberbeveiliging en bevordering van partnerschappen met derde landen, onder meer via specifieke cyberdialogen, om actief bij te dragen aan haar algehele weerbaarheid. Er is een aantal instrumenten ontwikkeld, herzien en versterkt om de Unie beter in staat te stellen hybride bedreigingen doeltreffend aan te pakken, zoals beschreven in het zevende voortgangsverslag over hybride bedreigingen, dat op 14 september 2023[22] is gepubliceerd. Hierbij gaat het onder meer om:

- de EU-toolbox tegen hybride dreigingen waarmee een kader moet worden geboden voor een gecoördineerde en goed geïnformeerde reactie op hybride dreigingen en campagnes;
- de lopende werkzaamheden voor het opzetten van snellereactieteams bij hybride dreigingen van de EU voor op maat gesneden ondersteuning op korte termijn voor lidstaten, partnerlanden en missies en operaties in het kader van het gemeenschappelijk veiligheids- en defensiebeleid (GVDB);
- het herziene EU-protocol voor de bestrijding van hybride bedreigingen ("EU-draaiboek")[23], waarin de processen en structuren van de Unie voor de aanpak van hybride bedreigingen en campagnes worden beschreven;
- de herziene uitvoeringsrichtsnoeren van het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten[24] ("instrumentarium voor cyberdiplomatie") waarmee de ontwikkeling van duurzame, op maat gesneden,

[21] Document van de Raad nr. 7371/22.
[22] SWD(2023) 315 final.
[23] SWD(2023) 116 final.
[24] 10289/23 van 8 juni 2023.

samenhangende en gecoördineerde strategieën tegen actoren van persistente cyberbedreigingen mogelijk wordt gemaakt;
- de toolbox voor de aanpak van buitenlandse informatiemanipulatie en inmenging (FIMI), ter versterking van het bestaande instrumentarium van de Unie om FIMI te voorkomen, te ontmoedigen en aan te pakken;
- het EU-beleid op het gebied van cyberdefensie[25], ter vergroting van de cyberdefensiecapaciteiten van de EU, verbetering van het situationeel bewustzijn en coördinatie van het hele scala aan beschikbare defensieve opties, teneinde de weerbaarheid te versterken, te reageren op cyberaanvallen en solidariteit en wederzijdse bijstand te waarborgen.

De lidstaten worden daarom aangemoedigd hun samenwerking op dit gebied voort te zetten en te versterken, door te zorgen voor een doeltreffende uitvoering van bovengenoemd instrumentarium, onder meer door regelmatige oefeningen, en door overeenstemming te bereiken over het concept van snellereactieteams bij hybride bedreigingen, als basis voor richtsnoeren voor verdere stappen in de richting van de totstandbrenging van deze teams.

### *AI in de context van rechtshandhaving*

Artificiële intelligentie (AI) is snel gemeengoed geworden in het dagelijks leven. De effecten van het gebruik van AI op cybercriminaliteit en cyberbeveiliging zijn nog niet volledig bekend, maar zullen duidelijk nieuwe uitdagingen met zich meebrengen. Hoewel AI voordelen kan bieden als het op een veilige en gecontroleerde manier wordt gebruikt, kan het in de handen van kwaadwilligen gevaarlijke mogelijkheden hebben, bijvoorbeeld door criminelen te helpen hun identiteit te verbergen bij misdaden zoals terrorisme en seksueel misbruik van kinderen. Het is daarom van cruciaal belang dat de autoriteiten op de hoogte blijven van de ontwikkelingen om misbruik te voorkomen en hierop te reageren[26]. De onderhandelingen over de voorgestelde verordening artificiële intelligentie hebben tot doel deze kwesties aan te pakken en zijn beland in een cruciale fase waarin medewetgevers nu technische en politieke kwesties bespreken die de interacties met deze technologie in de komende jaren zullen bepalen. Het is essentieel dat er evenwichtige oplossingen worden gevonden, vooral met betrekking tot toepassingen met een hoog risico, waaronder op het gebied van rechtshandhaving.

De Commissie roept het Europees Parlement en de Raad op om de interinstitutionele onderhandelingen over de volgende lopende dossiers met spoed af te ronden, in ieder geval vóór het einde van het mandaat van het huidige Europees Parlement:

- voorstel voor een verordening ter bestrijding van online seksueel misbruik van kinderen;
- voorstel voor een richtlijn ter bestrijding van geweld tegen vrouwen en huiselijk geweld;
- voorstel voor een verordening tot vaststelling van geharmoniseerde voorschriften inzake artificiële intelligentie (AI-verordening).

De Commissie roept de lidstaten op om:

- de EU-toolbox voor 5G-cyberbeveiliging onverwijld volledig uit te voeren;
- de werkzaamheden van de groep op hoog niveau inzake toegang tot gegevens voor een doeltreffende rechtshandhaving te ondersteunen, teneinde duidelijke, solide en

[25] JOIN(2022) 49 final.

[26] Zie bijvoorbeeld het verslag van Europol dat op 17 april 2023 werd gepubliceerd: ChatGPT — the impact of Large Language Models on Law Enforcement.

haalbare aanbevelingen te formuleren voor een proportionele aanpak van bestaande en verwachte uitdagingen;

- in samenwerking met de hoge vertegenwoordiger maatregelen te nemen om ervoor te zorgen dat de EU-toolbox tegen hybride dreigingen, het herziene instrumentarium voor cyberdiplomatie en de toolbox voor de aanpak van buitenlandse informatiemanipulatie en inmenging daadwerkelijk worden uitgevoerd, onder meer door regelmatig oefeningen te houden en rekening te houden met de mondiale dynamiek;
- overeenstemming te bereiken over het concept van snellereactieteams bij hybride bedreigingen.

## IV. Bescherming van Europeanen tegen terrorisme en georganiseerde criminaliteit

Het risico dat mondiale of lokale gebeurtenissen nieuwe uitbraken van terrorisme veroorzaken, is altijd aanwezig. Parallel daaraan behoren georganiseerde criminaliteit en drugshandel tot de ernstigste bedreigingen voor de veiligheid van de EU. Om de collectieve inspanningen van de Unie in de strijd tegen deze bedreigingen op te voeren, wordt collectief gewerkt aan de uitvoering van de EU-strategie voor de aanpak van georganiseerde criminaliteit[27], de EU-strategie voor de bestrijding van mensenhandel[28], de EU-agenda en het EU-actieplan inzake drugs[29] en de EU-agenda voor terrorismebestrijding[30]. Om de zorgwekkend verslechterende situatie op het gebied van de georganiseerde criminaliteit en drugshandel het hoofd te bieden, moeten de lidstaten en de EU hun werkzaamheden echter verder intensiveren om onze collectieve respons op criminele netwerken te versterken en slachtoffers van misdrijven beter te beschermen, en wordt tegelijk met dit verslag een EU-routekaart ter bestrijding van drugshandel en georganiseerde criminaliteit gepubliceerd[31].

Op het gebied van terrorismebestrijding versterkt de EU ook haar externe instrumentarium[32] door ten volle gebruik te maken van de dialogen op hoog niveau over terrorismebestrijding, het netwerk van terrorismebestrijdings-/beveiligingsdeskundigen in EU-delegaties, evenals door haar betrokkenheid bij multilaterale fora, onder meer als medevoorzitter van het Mondiaal Forum Terrorismebestrijding (GCTF).

### *Drugshandel*

Met het nieuwe mandaat van het EU-drugsagentschap dat vanaf juli 2024 in werking treedt, zal de EU beter toegerust zijn om een complex veiligheids- en gezondheidsprobleem aan te pakken dat miljoenen mensen in de EU en wereldwijd treft. Verder is de Commissie bezig met een

[27] COM(2021) 170 final.
[28] COM(2021) 171 final.
[29] COM(2020) 606 final.
[30] COM(2020) 795 final.
[31] COM(2023) 641 final.
[32] Zoals waartoe wordt opgeroepen in het strategisch kompas en in de conclusies van de Raad over de aanpak van de externe dimensie van een voortdurend evoluerende terroristische en gewelddadige extremistische dreiging, die in juni 2022 zijn aangenomen.

herziening[33] van de verordeningen inzake drugsprecursoren[34] teneinde de belangrijkste uitdagingen aan te pakken die in de evaluatie van 2020[35] zijn vastgesteld, en waarin werd benadrukt dat de door designerprecursoren[36] gestelde uitdagingen moeten worden aangepakt om het aanbod van illegale drugs te verminderen.

In het licht van de ongekende toename van illegale drugs die in Europa beschikbaar zijn, moet de strijd tegen drugshandel echter worden opgevoerd, in samenwerking met internationale partners. Er zijn extra maatregelen van de lidstaten en de EU nodig om criminele netwerken te ontmantelen en slachtoffers van criminaliteit beter te beschermen. De Commissie presenteert vandaag een EU-routekaart voor de bestrijding van drugshandel en georganiseerde criminaliteit. Deze bevat zeventien acties in vier prioriteitsgebieden: versterking van de weerbaarheid van logistieke knooppunten met een Europese havenalliantie, ontmanteling van criminele netwerken, opvoering van de preventie-inspanningen en versterking van de samenwerking met internationale partners. Deze acties moeten in 2024 en 2025 worden uitgevoerd.

***Vuurwapens***

De handel in vuurwapens voedt de georganiseerde criminaliteit in de EU en in haar buurlanden. Naar schatting zijn er in de EU 35 miljoen illegale vuurwapens in het bezit van burgers. Ongeveer 630 000 vuurwapens zijn als gestolen of verloren in het Schengeninformatiesysteem opgenomen. Door snelle pakjesdiensten en het gebruik van nieuwe technologie, zoals 3D-printen, ontsnapt de illegale handel in vuurwapens tegenwoordig vaker aan controles. Ook de Russische aanvalsoorlog tegen Oekraïne heeft het risico op de verspreiding van vuurwapens vergroot. In oktober 2022 heeft de Commissie een voorstel aangenomen om de bestaande wetgeving inzake de invoer, uitvoer en doorvoer van civiele vuurwapens te actualiseren, zodat mazen in de bestaande voorschriften waardoor het aantal naar de EU gesmokkelde en omgeleide vuurwapens kan toenemen, worden gedicht[37]. Op middellange termijn zullen de nieuwe voorschriften helpen om het risico van de omzeiling van embargo's op de uitvoer van vuurwapens voor civiel gebruik te verminderen en om de invoer van dit soort vuurwapens uit niet-EU-landen strenger te controleren. Beide medewetgevers moeten hun standpunten over dit dossier nog bepalen en het streven is dat zij voor het einde van de zittingsperiode van dit Parlement een akkoord over dit dossier bereiken.

***Mensenhandel***

Mensenhandel is een bijzonder ernstige vorm van georganiseerde criminaliteit en een ernstige schending van de grondrechten. Slachtoffers worden binnen de EU verhandeld, voornamelijk voor seksuele en arbeidsuitbuiting, maar ook voor gedwongen bedelarij, criminaliteit en andere vormen. De Commissie heeft in december 2022 voorgesteld om de richtlijn ter bestrijding van mensenhandel[38] te wijzigen met geactualiseerde voorschriften om tekortkomingen in het bestaande rechtskader aan te pakken. Als de herziene richtlijn eenmaal is goedgekeurd, zouden met name gedwongen huwelijken en illegale adoptie aan het toepassingsgebied van de richtlijn worden toegevoegd en zou expliciet naar de online dimensie van mensenhandel worden verwezen. Verder zou deze een verplichte sanctieregeling voor daders omvatten en de

[33] Drugsprecursoren — EU-wetgeving (herziene regels) (europa.eu).

[34] Verordening (EG) nr. 273/2004 inzake drugsprecursoren en Verordening (EG) nr. 111/2005 van de Raad houdende voorschriften voor het toezicht op de handel tussen de Gemeenschap en derde landen in drugsprecursoren.

[35] COM(2020) 768 final.

[36] Actie 23 van het actieplan inzake drugs, COM(2020) 606 final.

[37] COM(2022) 480 final.

[38] COM(2022) 732 final.

oprichting van nationale verwijzingsmechanismen formaliseren om vroegtijdige identificatie en grensoverschrijdende doorverwijzing voor hulp en steun aan slachtoffers te verbeteren. Het willens en wetens gebruikmaken van diensten van slachtoffers van mensenhandel zou strafbaar worden en het zou verplicht worden om jaarlijks gegevens over mensenhandel te verzamelen, voor publicatie door Eurostat. De Raad heeft in juni 2023 zijn algemene oriëntatie vastgesteld, terwijl het Europees Parlement zijn standpunt nog moet bepalen. Er zal snel actie moeten worden ondernomen om voor het einde van het mandaat van het huidige Parlement een akkoord te bereiken.

***Milieucriminaliteit***

Milieucriminaliteit is een wereldwijde bedreiging geworden en groeit met naar schatting 5 tot 7 % per jaar. De aanzienlijke winsten die hiermee kunnen worden behaald, de mazen in de wetgeving van lidstaten en de lage pakkans trekken alle georganiseerde criminaliteit aan. Volgens Europol zijn er aanwijzingen dat de opbrengsten van deze activiteiten worden gebruikt om terrorisme te financieren. In december 2021 heeft de Commissie een voorstel aangenomen om de richtlijn van 2008 inzake de bescherming van het milieu door middel van het strafrecht te vervangen. Het voorstel is gericht op het verfijnen en actualiseren van de definities van categorieën van milieucriminaliteit en het definiëren van doeltreffende, afschrikkende en evenredige soorten en niveaus van sancties voor natuurlijke en rechtspersonen. Tot de nieuwe strafbare feiten behoren delicten in verband met illegale ontbossing, schendingen van de EU-wetgeving inzake chemische stoffen, illegale winning van oppervlakte- of grondwater en illegale scheepsrecycling. Het voorstel heeft tot doel de rechtshandhavingsketen en de grensoverschrijdende samenwerking tussen de autoriteiten van de lidstaten en de instanties en organen van de EU aanzienlijk te versterken. Het Europees Parlement en de Raad hebben hun respectieve standpunten over het voorstel vastgesteld en bevinden zich in een onderhandelingsproces dat zij tegen het einde van het jaar zouden moeten kunnen afronden. Een herzien actieplan[39] tegen de handel in wilde dieren moet worden uitgevoerd om de preventie en handhaving verder te versterken.

***Ontneming en confiscatie van vermogensbestanddelen***

Criminelen hun illegale inkomsten ontnemen, is de sleutel tot het ontwrichten van de georganiseerde criminaliteit. Daarom heeft de Commissie, in aanvulling op het voorstel om rechtshandhavingsinstanties toegang te geven tot bankgegevens in de hele EU[40] (waarover in juni 2023 een politiek akkoord is bereikt), in mei 2022 een voorstel ingediend over de ontneming en confiscatie van vermogensbestanddelen[41], om vermogensbestanddelen beter te kunnen opsporen, identificeren, bevriezen, confisqueren en beheren. De belangrijkste bepalingen van het voorstel hebben betrekking op de vereisten voor financiële onderzoeken en aanvullende bevoegdheden en instrumenten van bureaus voor de ontneming van vermogensbestanddelen, evenals effectievere bevriezings- en confiscatiemaatregelen voor een bredere reeks delicten. Een van de nieuwe strafbare feiten waarvoor deze maatregelen zouden gelden, is de schending van beperkende maatregelen van de Unie. In december 2022 heeft de Commissie een afzonderlijk voorstel aangenomen voor het harmoniseren van de strafrechtelijke definities van en sancties voor de schending van beperkende maatregelen van de Unie. De doeltreffende uitvoering en handhaving van de beperkende maatregelen van de Unie blijft een topprioriteit voor de Commissie, en worden versterkt door het werk van de "Freeze and Seize"-taskforce die door de Commissie is opgezet als reactie op de Russische aanvalsoorlog tegen

[39] COM(2022) 581 final.
[40] COM(2021) 429 final.
[41] COM(2022) 245 final.

Oekraïne. Met betrekking tot beide voorstellen hebben het Europees Parlement en de Raad hun standpunt bepaald en wordt ernaar gestreefd om tegen het einde van dit jaar tot een akkoord te komen.

***Antiwitwaspakket***

Het witwassen van geld is verbonden met vrijwel alle criminele activiteiten die criminele opbrengsten genereren in de EU[42] en is dus een belangrijke hefboom voor de aanpak van criminaliteit in de EU. In juli 2021 heeft de Commissie ambitieuze voorstellen gedaan om de maatregelen van de EU ter voorkoming van het witwassen van geld en de financiering van terrorisme te versterken[43], met vier wetgevingsvoorstellen ter versterking van de preventie en opsporing van pogingen van criminelen om illegale opbrengsten wit te wassen of terroristische activiteiten te financieren via het financiële stelsel. Een van de vier initiatieven van het pakket, namelijk het voorstel om te zorgen voor traceerbaarheid van overdrachten van cryptoactiva, werd in mei 2023 door de medewetgevers aangenomen[44]. Deze verordening treedt op 30 december 2024 in werking, op welke datum alle aanbieders van cryptoactivadiensten informatie moeten verzamelen en bewaren over de initiator en begunstigde van overdrachten van cryptoactiva. De overige drie voorstellen zijn gericht op i) de oprichting van een nieuwe EU-Autoriteit voor de bestrijding van witwassen die moet zorgen voor een consistent en kwalitatief hoogwaardig toezicht op de hele interne markt, met inbegrip van de meest risicovolle grensoverschrijdende entiteiten, en die de werkzaamheden van de financiële-inlichtingeneenheden moet ondersteunen en coördineren, ii) de vaststelling van geharmoniseerde voorschriften voor de particuliere sector, waaronder de invoering van een EU-brede limiet van 10 000 EUR voor grote contante betalingen in ruil voor diensten en goederen, en iii) de versterking van de bevoegdheden en samenwerkingsinstrumenten voor bevoegde autoriteiten. Dit pakket zal het vermogen van de EU om het witwassen van geld te bestrijden en EU-burgers te beschermen tegen terrorisme en georganiseerde criminaliteit naar verwachting aanzienlijk vergroten. De medewetgevers onderhandelen momenteel over de drie openstaande voorstellen, en het streven is dat zij voor het einde van de zittingsperiode van dit Parlement een akkoord over dit dossier bereiken.

De Commissie roept het Europees Parlement en de Raad op om de interinstitutionele onderhandelingen over de volgende lopende dossiers met spoed af te ronden, in ieder geval vóór het einde van het mandaat van het huidige Europees Parlement:

- voorstel voor een richtlijn betreffende ontneming en confiscatie van vermogensbestanddelen;
- voorstel voor een richtlijn betreffende de definitie van strafbare feiten en sancties voor de schending van beperkende maatregelen van de Unie;
- voorstel voor een richtlijn ter bestrijding van mensenhandel;
- voorstel voor een richtlijn ter verbetering van de milieubescherming door middel van het strafrecht;
- voorstel voor een antiwitwaspakket;

[42] Europol, "Ondernemende criminelen — Europa's strijd tegen de wereldwijde netwerken van financiële en economische criminaliteit", 2020.

[43] COM(2021) 420 final.

[44] Verordening (EU) 2023/1113 van het Europees Parlement en de Raad van 31 mei 2023 betreffende bij geldovermakingen en overdrachten van bepaalde cryptoactiva te voegen informatie en tot wijziging van Richtlijn (EU) 2015/849.

- voorstel voor het actualiseren van bestaande wetgeving inzake de invoer, uitvoer en doorvoer van civiele vuurwapens.

De Commissie roept de lidstaten en de instanties en organen van de EU op:
- samen te werken aan de uitvoering van de 17 acties van de EU-routekaart voor de bestrijding van drugshandel en georganiseerde criminaliteit in 2023 en 2024.

## V. Een krachtig Europees veiligheidsecosysteem

De laatste jaren zijn de bedreigingen voor de veiligheid steeds meer grensoverschrijdend van aard geworden, wat vraagt om verdere synergieën en nauwere samenwerking op alle niveaus. Sinds de vaststelling van de strategie voor de veiligheidsunie zijn belangrijke initiatieven genomen om de grensoverschrijdende samenwerking te maximaliseren, de beschikbare instrumenten en procedures aan de buitengrenzen en binnen het Schengengebied te stroomlijnen en te verbeteren, en de uitwisseling van informatie tussen rechtshandhavings- en justitiële autoriteiten te verbeteren voor een betere bestrijding van de georganiseerde criminaliteit. Tegen deze achtergrond is de doeltreffende uitvoering van het interoperabiliteitskader voor gegevensuitwisseling een belangrijke pijler voor het verbeteren van de veiligheid en een doeltreffende Europese reactie op grensoverschrijdende bedreigingen, terwijl tegelijkertijd het vrije verkeer binnen de EU wordt gewaarborgd.

### *Verbeterde uitwisseling van informatie binnen het Schengengebied: vooraf te verstrekken passagiersgegevens (API), persoonsgegevens van passagiers (PNR) en Prüm II*

De twee API-voorstellen die de Commissie in december 2022 heeft goedgekeurd[45] zouden de interne veiligheid van de Unie vergroten door de rechtshandhavingsinstanties van de lidstaten extra instrumenten te geven om zware criminaliteit en terrorisme te bestrijden. In het bijzonder zouden vooraf te verstrekken passagiersgegevens op vluchten binnen de EU in combinatie met PNR-gegevens van luchtreizigers het de rechtshandhavingsinstanties van lidstaten aanzienlijk makkelijker maken om de efficiëntie van hun onderzoeken te verhogen door gerichter op te treden. Het is belangrijk dat de voorgestelde voorschriften zo snel mogelijk worden aangenomen: dit zou niet alleen de strijd tegen de georganiseerde criminaliteit en terrorisme ondersteunen, maar ook de noodzaak om alle reizigers systematisch te controleren aanzienlijk verminderen in geval van een tijdelijke herinvoering van grenscontroles aan de binnengrenzen, waardoor vliegreizen en het vrij verkeer worden vergemakkelijkt. De Commissie heeft op 6 september 2023 de Raad aanbevolen een machtiging te verlenen voor het openen van onderhandelingen met Zwitserland, IJsland en Noorwegen over overeenkomsten inzake de doorgifte van PNR-gegevens. De goedkeuring van deze drie aanbevelingen zou een consistente en doeltreffende externe EU-strategie voor doorgifte van PNR-gegevens ondersteunen.

Binnen het Prümkader wisselt de politie dagelijks gegevens uit om georganiseerde criminaliteit, drugs, terrorisme, seksuele uitbuiting en mensenhandel te bestrijden. Met het voorstel voor een verordening over geautomatiseerde gegevensuitwisseling voor politiële samenwerking ("Prüm II")[46] wordt het bestaande Prümkader herzien om lacunes in de informatie te dichten en het voorkomen, opsporen en onderzoeken van strafbare feiten in de EU te verbeteren. De

[45] COM(2022) 729 final en COM(2022) 73 final.
[46] COM(2021) 784 final.

herziene voorschriften voor geautomatiseerde gegevensuitwisseling voor politiële samenwerking vervolledigen de voorstellen voor de politiële samenwerking in dit mandaat, naast de reeds goedgekeurde aanbeveling van de Raad ter versterking van de operationele grensoverschrijdende samenwerking en de richtlijn over de uitwisseling van informatie tussen rechtshandhavingsinstanties. Een snelle goedkeuring en uitvoering van deze gerelateerde instrumenten zou de gegevensuitwisseling tussen rechtshandhavingsinstanties verbeteren, vergemakkelijken en versnellen, en zou helpen bij het identificeren van criminelen.

***Volledig interoperabel grensbeheersysteem voor een veilig, sterk, digitaal en verenigd Schengengebied***

Een goed functionerend Schengengebied zonder binnengrenzen berust op wederzijds vertrouwen tussen de lidstaten. Dit berust op zijn beurt op efficiënte controles, zowel aan de buitengrenzen van de Unie als door middel van alternatieve maatregelen op het grondgebied van de lidstaten. In de door de Commissie voorgestelde wijziging van de Schengengrenscode[47] wordt uiteengezet hoe de lidstaten beter gebruik kunnen maken van alternatieven voor binnengrenstoezicht, die een hoog veiligheidsniveau kunnen bieden. Het is belangrijk dat de wijziging van de Schengengrenscode wordt aangenomen en volledig wordt uitgevoerd om voor een hoog en evenredig veiligheidsniveau binnen het Schengengebied te zorgen. Momenteel wordt nog steeds gewerkt aan de nieuwe architectuur voor de informatiesystemen van de EU om betere ondersteuning te geven aan de werkzaamheden van de nationale autoriteiten die voor veiligheid en grensbeheer moeten zorgen. Deze nieuwe architectuur omvat het vernieuwde Schengeninformatiesysteem, het Europees systeem voor reisinformatie en -autorisatie, het inreis-uitreissysteem, de actualisering van het visuminformatiesysteem en het interoperabiliteitskader om systemen volledig veilig aan elkaar te koppelen. Als de nieuwe architectuur eenmaal volledig voltooid is, zou deze de nationale autoriteiten uitgebreidere en betrouwbaardere veiligheidsinformatie verschaffen. Alle onderdelen van het interoperabiliteitskader zijn essentieel, wat betekent dat een vertraging in één aspect of in één lidstaat voor iedereen tot een vertraagde uitrol leidt. Vertragingen bij de technische ontwikkeling van het inreis-uitreissysteem moeten tot een minimum worden beperkt, zodat het inreis-uitreissysteem zo snel mogelijk in gebruik kan worden genomen en alle belangrijke elementen van het interoperabiliteitskader kunnen worden ingevoerd.

Het screeningsvoorstel[48] zou de veiligheid binnen het Schengengebied vergroten door uniforme voorschriften vast te stellen voor de identificatie van onderdanen van derde landen die niet voldoen aan de inreisvoorwaarden als bedoeld in de Schengengrenscode, en hen aan de buitengrenzen te onderwerpen aan de gezondheids- en veiligheidscontroles. Het voorgestelde Eurodac-systeem zou deze doelstellingen ondersteunen door aan te geven wanneer na screening blijkt dat een persoon een bedreiging voor de interne veiligheid kan vormen. Dit zou op zijn beurt de uitvoering van de voorgestelde verordening betreffende asiel- en migratiebeheer vergemakkelijken. De Commissie moedigt de medewetgevers aan om de onderhandelingen over deze dossiers vóór het einde van de huidige zittingsperiode snel af te ronden.

***Corruptiebestrijding***

Corruptie is zeer schadelijk voor onze democratieën, voor de economie en voor onze veiligheid, omdat zij als katalysator fungeert voor de georganiseerde criminaliteit en vijandige buitenlandse inmenging. Het is van essentieel belang dat corruptie met succes wordt voorkomen en bestreden, zowel om de waarden van de EU en de doeltreffendheid van het EU-beleid te

[47] COM(2021) 891 final.
[48] COM(2020) 612 final.

waarborgen als om de rechtsstaat en het vertrouwen in bestuurders en openbare instellingen te handhaven. Zoals door voorzitter Von der Leyen in de toespraak over de Staat van de Unie van 2022 werd aangekondigd, heeft de Commissie op 3 mei 2023 een pakket anticorruptiemaatregelen[49] goedgekeurd. Het voorstel van de Commissie voor een richtlijn betreffende de bestrijding van corruptie omvat aangescherpte voorschriften voor het strafbaar stellen van corruptiedelicten en het harmoniseren van straffen in de hele EU. Met behulp van het voorstel worden ook effectieve onderzoeken en vervolgingen mogelijk gemaakt en wordt sterk de nadruk gelegd op preventie en het creëren van een cultuur van integriteit waarin corruptie niet wordt getolereerd. De besprekingen over dit voorstel in het Europees Parlement en de Raad zijn inmiddels begonnen. Daarnaast worden de lidstaten opgeroepen om de aanbevelingen uit te voeren die voortvloeien uit de pijler corruptiebestrijding van het verslag over de rechtsstaat van 2023, dat op 5 juli 2023 is aangenomen. In een voorstel van de hoge vertegenwoordiger, dat gesteund wordt door de Commissie, wordt ook voorgesteld om een specifieke sanctieregeling voor het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) vast te stellen om wereldwijd ernstige vormen van corruptie aan te pakken.

***Versterking van de rechten van slachtoffers***

Op 12 juli 2023 heeft de Commissie wijzigingen van de richtlijn slachtofferrechten voorgesteld, om de toegang van slachtoffers tot informatie, ondersteuning en bescherming, deelname aan strafprocedures en toegang tot schadevergoeding te verbeteren. Een van de algemene doelstellingen van de herziening is bij te dragen aan een hoog niveau van veiligheid door een veiligere omgeving voor slachtoffers te creëren teneinde het melden van strafbare feiten aan te moedigen en de angst voor represailles te verminderen.

De Commissie roept het Europees Parlement en de Raad op om de interinstitutionele onderhandelingen over de volgende lopende dossiers met spoed af te ronden, in ieder geval vóór het einde van het mandaat van het huidige Europees Parlement:

- voorstel inzake de Prüm II-verordening;
- voorstellen betreffende vooraf te verstrekken passagiersgegevens (API);
- voorstellen inzake corruptiebestrijding en met name instelling van een speciale sanctieregeling in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB);
- voorstel voor een wijziging van de verordening van de Schengengrenscode;
- voorstel voor een richtlijn slachtofferrechten;
- voorstel inzake screening.

De Commissie roept de lidstaten op om:

- ervoor te zorgen dat het inreis-uitreissysteem zo snel mogelijk in werking treedt teneinde de uitvoering van de EU-architectuur voor informatie-uitwisseling te voltooien.

## VI. Uitvoering

De waarborging van de veiligheid van Europa als geheel is een gedeelde verantwoordelijkheid waarbij elke actor zijn rol moet vervullen, van de Commissie en de medewetgevers die nieuwe, krachtige, uitgebreide en praktische voorschriften vaststellen, tot de tijdige omzetting, uitvoering en toepassing van die voorschriften door de lidstaten, en de operationele

[49] COM(2023) 234 final.

werkzaamheden die in het veld worden verricht door verschillende autoriteiten, organisaties en belanghebbenden. Ook EU-instanties op het gebied van justitie, binnenlandse zaken en cyberbeveiliging spelen een belangrijke rol, die door recente uitbreidingen van hun verantwoordelijkheden nog eens is toegenomen.

***Verbeterde screening van begunstigden van EU-financiering***

Bij de uitvoering van de EU-begroting heeft de Commissie de verantwoordelijkheid om ervoor te zorgen dat begunstigden van EU-financiering de EU-waarden respecteren. De mechanismen en controlesystemen die bepalen wie in aanmerking komt voor EU-financiering zijn al robuust en de lopende onderhandelingen over de herziening van het Financieel Reglement zijn ook bedoeld om de Commissie sterkere juridische middelen te geven om indien nodig op te treden. Daarnaast werkt de Commissie momenteel aan manieren om de screening van huidige en potentiële toekomstige begunstigden van EU-financiering verder te verbeteren door de richtsnoeren inzake de verplichtingen ten aanzien van de eerbiediging van de EU-waarden en de gevolgen van een schending van de EU-waarden te verbeteren. Dit zal de verantwoordelijkheden van zowel de begunstigden als de uitvoerders van controles op EU-niveau verduidelijken en kan dienen als inspiratiebron voor het nationale niveau. In geval van schending van de financieringsvoorwaarden zal de Commissie niet aarzelen om de samenwerking met de begunstigden van het betrokken project stop te zetten en zo nodig middelen terug te vorderen. Het is belangrijk dat lidstaten proactief informatie delen met de Commissie wanneer zij op de hoogte zijn van mogelijke risico's met betrekking tot organisaties die EU-financiering aanvragen.

***Inbreuken***

Op het gebied van de veiligheid heeft de Commissie veel inbreukprocedures gevoerd. Zo werd in 2023 een groot aantal inbreukprocedures ingeleid wegens niet-nakoming van de verplichtingen uit hoofde van de verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud van 2021 (16 lidstaten)[50], en ontvingen in de loop van 2022 en 2023 20 lidstaten aanvullende ingebrekestellingen wegens de onjuiste uitvoering van de richtlijn ter bestrijding van seksueel misbruik van kinderen van 2011[51]. Er loopt nog een aanzienlijk aantal inbreukprocedures wegens non-conformiteit van nationale wetgeving met de richtlijn inzake terrorismebestrijding[52] van 2017 en wegens niet-omzetting van voorschriften die het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten vergemakkelijken[53]. Andere gebieden waarop inbreukprocedures lopen, zijn onder andere de vuurwapenwetgeving; de voorschriften inzake psychoactieve stoffen die in drugs worden gebruikt, de bestrijding van fraude en vervalsing van niet-contante betaalmiddelen, de bestrijding van het witwassen, de uitwisseling van strafregisters tussen de EU-lidstaten en de richtlijn slachtofferrechten. Er is (technische en financiële) steun beschikbaar gesteld aan lidstaten die overeengekomen initiatieven en acties uitvoeren en de Commissie blijft beschikbaar om met de lidstaten samen te werken om de uitvoering te optimaliseren.

---

50 Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online-inhoud.

51 Richtlijn 2011/93/EU ter bestrijding van seksueel misbruik van kinderen.

52 Richtlijn (EU) 2017/541 van het Europees Parlement en de Raad van 15 maart 2017 inzake terrorismebestrijding en ter vervanging van Kaderbesluit 2002/475/JBZ van de Raad en tot wijziging van Besluit 2005/671/JBZ van de Raad.

53 Richtlijn (EU) 2019/1153 van het Europees Parlement en de Raad van 20 juni 2019 tot vaststelling van regels ter vergemakkelijking van het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten, en tot intrekking van Besluit 2000/642/JBZ van de Raad.

***Monitoring via Schengenevaluaties en het nieuwe governancesysteem ervan***

Het evaluatie- en toezichtmechanisme van Schengen is blijven bijdragen tot de doeltreffende uitvoering van de Schengenregels die de veiligheid in het gebied zonder interne controles moeten vergroten. In 2023 zijn de eerste evaluaties op grond van het versterkte Schengenevaluatie- en -toezichtmechanisme uitgevoerd, waardoor strategische kwetsbaarheden met grensoverschrijdende gevolgen voor de veiligheid binnen de EU tijdig konden worden vastgesteld en verholpen. Bovendien heeft de Commissie in 2023 een thematische Schengenevaluatie gestart voor het beoordelen van de praktijken van lidstaten die voor vergelijkbare uitdagingen staan bij de bestrijding van drugssmokkel naar de EU, waarbij de aandacht met name uitgaat naar omvangrijke drugssmokkel. Met deze evaluaties werd de aandacht voor de veiligheidsaspecten van Schengen versterkt en uitgebreid. Op basis van de resultaten van de periodieke, thematische en onaangekondigde Schengenevaluaties heeft de Raad in juni 2023 de prioriteiten voor de Schengencyclus voor 2023-2024 vastgesteld. Hierbij zijn aandachtsgebieden aangegeven die een extra impuls nodig hebben voor een veiliger en sterker Schengengebied. Een doeltreffende en snelle uitvoering van deze prioriteiten in combinatie met een intensievere beleidscoördinatie van de Schengenraad zal de strijd tegen de georganiseerde criminaliteit verder versterken en de grensoverschrijdende operationele samenwerking maximaliseren.

***Rol van EU-instanties en -organen***

Voor de uitvoering van de initiatieven in het kader van de veiligheidsunie is partnerschap van cruciaal belang, aangezien het werk van verschillende nationale en Europese autoriteiten en organen nodig is om concrete resultaten te boeken. Zo maakt Empact (het Europees multidisciplinair platform tegen criminaliteitsdreiging) gestructureerde multidisciplinaire samenwerking van lidstaten mogelijk, ondersteund door alle EU-instellingen, -organen en -instanties (zoals Europol, Frontex, Eurojust, Cepol, OLAF en eu-LISA). De operaties die door Empact worden uitgevoerd, onder meer via speciale operationele taskforces (OTF's), coördineren de inspanningen van de lidstaten en operationele partners bij de strijd tegen criminele netwerken en zware criminaliteit. Alleen al in 2022 resulteerde Empact in een totaal van 9 922 arrestaties, meer dan 180 miljoen EUR aan in beslag genomen activa en geld, 9 263 gestarte onderzoeken, 4 019 geïdentificeerde slachtoffers, meer dan 62 ton in beslag genomen drugs, 51 geïdentificeerde en 12 gearresteerde High Value Targets (HVT's), operaties in de context van de aanvalsoorlog tegen Oekraïne, met name om mensenhandel en vuurwapengerelateerde bedreigingen aan te pakken[54].

Frontex, het Europees Agentschap voor maritieme veiligheid (EMSA) en het Europees Bureau voor visserijcontrole (EFCA) blijven hun samenwerking op het gebied van kustwachttaken versterken om de nationale autoriteiten te ondersteunen bij het vergroten van de veiligheid en beveiliging op zee. Deze instanties zullen een belangrijke bijdrage leveren aan de uitvoering van de EU-strategie voor maritieme veiligheid.

Verscheidene initiatieven van de veiligheidsunie hebben nieuwe verantwoordelijkheden en taken voor de relevante instanties met zich meegebracht, soms met gevolgen voor de personele middelen.

[54] Factsheets over resultaten Empact in 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

*Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)*

Wat betreft de paraatheid voor en respons op incidenten ter verbetering van de cyberbeveiliging heeft de Commissie een kortetermijnactie opgezet ter ondersteuning van de lidstaten door financiering van het programma Digitaal Europa (DEP) over te hevelen naar het **Agentschap van de Europese Unie voor cyberbeveiliging (Enisa)** om de paraatheid en capaciteit voor respons op grote cyberincidenten te versterken. Het voorstel voor de verordening cybersolidariteit dat in april 2023 is aangenomen, bouwt voort op deze actie en kan, zodra het door de medewetgevers is aangenomen, Enisa belasten met aanvullende taken zoals het beheer van de toekomstige cyberbeveiligingsreserve van de Unie of het opstellen van een evaluatieverslag na grootschalige cyberbeveiligingsincidenten. Op grond van de voorgestelde verordening cyberweerbaarheid zou het Enisa meldingen moeten ontvangen van fabrikanten over kwetsbaarheden in producten met digitale elementen, en van incidenten die gevolgen hebben voor de beveiliging van die producten, die het Enisa naar de relevante CSIRT's of de relevante centrale contactpunten van de lidstaten zou moeten doorsturen. Van het Enisa wordt ook verwacht dat het een tweejaarlijks technisch verslag opstelt over opkomende trends met betrekking tot cyberbeveiligingsrisico's in producten met digitale elementen en dit bij de NIS-samenwerkingsgroep indient.

*Europees Kenniscentrum voor cyberbeveiliging*

Het **Europees kenniscentrum voor cyberbeveiliging (ECCC)** is samen met het netwerk van nationale coördinatiecentra (NCC's) het nieuwe orgaan van de Unie ter ondersteuning van innovatie en industriebeleid op het gebied van cyberbeveiliging. Dit ecosysteem zal de capaciteiten van de gemeenschap op het gebied van de cyberbeveiligingstechnologie versterken, de kwaliteit van onderzoek in stand houden en het concurrentievermogen van de industrie van de Unie op dit gebied te versterken. Het ECCC en de NCC's zullen strategische investeringsbeslissingen nemen en middelen van de Unie, haar lidstaten en, indirect, de industrie bundelen om de technologie en industriële cyberbeveiligingscapaciteiten te verbeteren en versterken. Het ECCC speelt daarom een sleutelrol bij de verwezenlijking van de ambitieuze doelstellingen op het gebied van cyberbeveiliging van de programma's Digitaal Europa en Horizon Europa.

Het ECCC heeft meer dan de helft van zijn personeel aangeworven en zal binnenkort een uitvoerend directeur aanwerven. Er wordt inmiddels al gewerkt aan onder andere het cyberbeveiligingsonderdeel van het DIGITAL-programma en een nieuwe strategische agenda[55] voor technologieontwikkeling en -implementatie, waarin prioritaire acties zijn opgenomen om kmo's te ondersteunen bij de ontwikkeling en het gebruik van strategische cyberbeveiligingstechnologieën, -diensten en -processen; de pool van professionele arbeidskrachten te ondersteunen en te laten groeien; en de expertise op het gebied van onderzoek, ontwikkeling en innovatie in het bredere Europese cyberbeveiligingsecosysteem te versterken.

*Europol*

Met een gloednieuw mandaat zal **Europol** beter toegerust zijn om de lidstaten te ondersteunen in de strijd tegen de georganiseerde criminaliteit. De strijd tegen de drugshandel is een topprioriteit gezien het toenemende belang en de toenemende negatieve gevolgen ervan voor de veiligheid van de EU-burgers. Na de autorisatie van de Raad van de Europese Unie op 15 mei 2023 heeft de Commissie actief gewerkt aan de afsluiting van internationale overeenkomsten

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_en

met Bolivia, Brazilië, Ecuador, Mexico en Peru over de uitwisseling van persoonsgegevens met Europol met het oog op het voorkomen en bestrijden van ernstige criminaliteit en terrorisme.

*Eurojust*

Met meer dan twintig jaar ervaring met het bieden van justitiële ondersteuning aan nationale autoriteiten bij de bestrijding van een breed scala aan ernstige en complexe grensoverschrijdende criminaliteit, heeft **Eurojust** zijn positie op het gebied van vrijheid, veiligheid en rechtvaardigheid in de EU verstevigd. Om de samenwerking over de hele linie te versterken, is de Commissie in onderhandeling over internationale overeenkomsten ter vergemakkelijking van de samenwerking tussen Eurojust en dertien derde landen met het oog op de uitwisseling van persoonsgegevens ten behoeve van de strijd tegen georganiseerde criminaliteit en terrorisme[56]. Onderhandelingen met Armenië en Libanon zijn reeds afgerond, die met Algerije en Colombia zijn gaande en die met Bosnië en Herzegovina zijn gestart. De Commissie moedigt het Europees Parlement en de Raad aan om de sluiting van overeenkomsten met deze landen vóór het einde van de zittingsperiode af te ronden, teneinde de transnationale justitiële samenwerking te versterken en de strijd tegen grensoverschrijdende criminaliteit te verbreden.

*EOM*

Sinds het begin van zijn operationele activiteiten in juni 2021 is het **Europees openbaar ministerie (EOM)** een krachtig instrument gebleken in het instrumentarium van de Unie voor het onderzoeken en vervolgen van strafbare feiten die de begroting van de Unie schaden, met inbegrip van strafbare feiten die verband houden met de deelname aan een criminele organisatie, waarbij de nadruk ligt op misdaden tegen de begroting van de Unie. De Commissie moedigt de lidstaten die nog niet deelnemen aan de nauwere samenwerking van het EOM aan om dit zo snel mogelijk te doen, zodat het EOM zijn volledige potentieel voor de bescherming van het geld van de Europese belastingbetaler kan verwezenlijken.

*EUDA*

Met een nieuw mandaat dat in juni 2023 door de medewetgevers is goedgekeurd, verandert het bestaande Europees Waarnemingscentrum voor drugs en drugsverslaving (EWDD) in een volwaardig agentschap — het **Drugsagentschap van de Europese Unie (EUDA)** — met een versterkte rol. Het agentschap zal de door illegale drugs gestelde nieuwe gezondheids- en veiligheidsuitdagingen uitvoeriger kunnen beoordelen en effectiever kunnen bijdragen aan de werkzaamheden op het niveau van de lidstaten en op internationaal niveau. Het verzamelen, analyseren en verspreiden van gegevens zal de belangrijkste taak van het agentschap blijven, maar het uitgebreide mandaat zal het agentschap ook in staat stellen om een algemene capaciteit voor het beoordelen van gezondheids- en veiligheidsbedreigingen te ontwikkelen om opkomende bedreigingen te identificeren, waaronder het gebruik van polysubstanties, de samenwerking via nationale knooppunten te versterken, en een netwerk van laboratoria op te zetten dat het agentschap van forensische en toxicologische informatie voorziet. Dit zal het agentschap helpen om waarschuwingen af te geven wanneer er bijzonder gevaarlijke stoffen op de markt verschijnen en om het bewustzijn te vergroten.

[56] Algerije, Argentinië, Armenië, Bosnië en Herzegovina, Brazilië, Colombia, Egypte, Israël, Jordanië, Libanon, Marokko, Tunesië en Turkije.

De Commissie roept het Europees Parlement en de Raad op om de interinstitutionele onderhandelingen over de volgende lopende dossiers met spoed af te ronden, in ieder geval vóór het einde van het mandaat van het huidige Europees Parlement:

- voorstel inzake de herschikking van het Financieel Reglement.

De Commissie roept de lidstaten op om:

- proactief informatie met de Commissie te delen wanneer zij op de hoogte zijn van mogelijke risico's met betrekking tot organisaties die EU-financiering aanvragen;
- de prioriteiten van de Schengencyclus voor 2023-2024 snel uit te voeren voor een veiliger en sterker Schengengebied;
- de tegen hen lopende inbreukprocedures aan te pakken om voor een correcte omzetting van de desbetreffende wetgeving te zorgen.

## VII. Conclusie

De afgelopen drie jaar stonden in het teken van een constante en vastberaden inspanning om de ambitie van totstandbrenging van een veiligheidsunie voor de EU leven in te blazen. Binnen het hele spectrum van het veiligheidsbeleid is enorme vooruitgang geboekt. De realiteit van voortdurend veranderende bedreigingen vraagt nu om voortdurende inspanningen met hernieuwde motivatie. De werkzaamheden aan het wetgevingskader moeten tijdig worden afgerond, vóór het einde van de zittingsperiode in het voorjaar van 2024. Op de lidstaten rusten constant verantwoordelijkheden om nieuwe wetten om te zetten, uit te voeren en toe te passen. Voor de uitvoering zijn gezamenlijke inspanningen nodig, ook met de steun van de EU-instanties, en heel vaak een steeds sterkere samenwerking met onze internationale partners.

Alleen met de collectieve en vastberaden inspanningen van alle betrokkenen zullen we de veiligheids- en beveiligingsniveaus in de EU bereiken die burgers verwachten, en in de actuele omstandigheden zou het voor elke actor een prioriteit moeten zijn om zijn rol bij het versterken van de beveiliging van de EU te spelen.