EUROPESE
COMMISSIE

Brussel, 13.12.2022
COM(2022) 745 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

betreffende het vijfde voortgangsverslag over de uitvoering van de EU-strategie voor de veiligheidsunie

1. INLEIDING

In juli 2020 heeft de Commissie de alomvattende strategie voor de veiligheidsunie vastgesteld[1]. Sindsdien is het dreigingsklimaat aanzienlijk geëvolueerd. Door de COVID-19-crisis zijn enkele kwetsbaarheden sterker uitgelicht, met name doordat veel activiteiten online moesten plaatsvinden. Aanvallen op de cyberbeveiliging zijn in omvang blijven toenemen en hebben nieuwe vormen aangenomen[2]. De gevolgen van de aanvalsoorlog van Rusland tegen Oekraïne waren voelbaar in de interne veiligheid van de EU, waar het risico van mensenhandel, de dreiging van chemische en nucleaire incidenten en het illegale verkeer van vuurwapens toenamen. De oorlog heeft ook het gebruik van buitenlandse desinformatie en inmenging aangewakkerd. De recente sabotage van de Nord Stream-pijpleidingen heeft duidelijk gemaakt hoezeer essentiële sectoren zoals energie, digitale infrastructuur, vervoer en ruimtevaart afhankelijk zijn van weerbare kritieke infrastructuur. Daaruit is eens te meer gebleken dat fysieke en digitale veiligheid nauw met elkaar vervlochten zijn en samen moeten worden beschermd.

Met dit voortgangsverslag over de veiligheidsunie wordt een tussentijds overzicht gegeven van de uitvoering van de strategie, waarbij wordt gewezen op wat reeds bereikt is en wat nog moet worden gedaan voordat het mandaat van deze Commissie ten einde loopt. Sinds juli 2020 heeft de EU grote stappen genomen naar de voltooiing van de maatregelen op de belangrijkste gebieden die onder de vier pijlers van de strategie vallen[3]. Uit dit verslag blijkt dat de overgrote meerderheid van de in de strategie opgesomde maatregelen ter hand zijn genomen[4]. Er moeten echter nog inspanningen worden geleverd opdat de burgers alle effecten van de strategie voor de veiligheidsunie kunnen ondervinden: het Europees Parlement en de Raad moeten met name de openstaande wetsvoorstellen nog aannemen en de lidstaten moeten de overeengekomen wetgeving nog uitvoeren. De doelstellingen van de veiligheidsunie kunnen ook het beste worden bereikt aan de hand van nauwe samenwerking met verbonden EU-initiatieven op gebieden zoals de energiezekerheid, de Europese gezondheidsunie en het Europees actieplan voor democratie. De Commissie blijft hieraan bijdragen met onder meer drie samen met dit verslag vastgestelde voorstellen betreffende de illegale handel in cultuurgoederen, de essentiële inlichtingen afkomstig van vooraf te verstrekken passagiersgegevens[5] en een voorstel om mensenhandel aan te pakken[6].

---

1 COM(2020) 605.

2 Enisa Threat landscape 2022.

3 1) Een toekomstbestendige veiligheidsomgeving, 2) een aanpak van veranderende dreigingen, 3) de Europeanen beschermen tegen terrorisme en georganiseerde misdaad, 4) een krachtig Europees veiligheidsecosysteem.

4 Een tabel als bijlage biedt een overzicht van de wetgevings- en niet-wetgevingsmaatregelen sinds de invoering van de strategie voor de veiligheidsunie.

5 Een actieplan tegen de illegale handel in cultuurgoederen (COM(2022) 800 en twee voorstellen inzake de herziening van de richtlijn vooraf te verstrekken passagiersgegevens (COM(2022) 729 en 731).

6 Naar verwachting zullen een voorstel voor een herziene richtlijn tegen mensenhandel (COM(2022) 732) en het vierde voortgangsverslag over mensenhandel op 19 december 2022 worden vastgesteld.

2. FYSIEKE EN DIGITALE INFRASTRUCTUUR BESCHERMEN TEGEN FYSIEKE, CYBER- EN HYBRIDE AANVALLEN

Kritieke infrastructuur in de EU beschermen tegen fysieke en digitale aanvallen

Nog vóór de recente aanvallen op kritieke infrastructuur was de EU haar weerbaarheid aan het opbouwen met behulp van twee verbonden initiatieven: de herziene richtlijn[7] betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie **(*Network Infrastructure Security* — "NIS2-richtlijn")[8]** en een nieuwe richtlijn betreffende de veerkracht van kritieke entiteiten **(*Resilience of Critical Entities* – "CER-richtlijn")**[9]. Deze twee richtlijnen vormen samen een kader voor de aanpak van actuele en toekomstige online en offline risico's, van cyberaanvallen tot natuurrampen. De medewetgevers hebben een akkoord bereikt over deze richtlijnen die de komende weken in werking zullen treden. Met de **NIS2-richtlijn** wordt het toepassingsgebied uitgebreid naar middelgrote en grote entiteiten in een scala aan sleutelsectoren[10]. De richtlijn bevat aangescherpte beveiligingseisen voor onder meer incidentrespons en crisisbeheer, beveiliging van de toeleveringsketen, de respons op en het bekendmaken van kwetsbaarheden, het testen van de cyberbeveiliging en het effectieve gebruik van encryptie. Met de richtlijn worden ook de verplichtingen in verband met het melden van incidenten gestroomlijnd, strengere toezichtsmaatregelen ingevoerd en wordt er werk gemaakt van de harmonisatie van de sanctieregelingen in de lidstaten[11]. De **CER-richtlijn** behandelt de fysieke weerbaarheid van kritieke entiteiten tegen zowel natuurrampen als rampen die door de mens worden veroorzaakt. Zij geldt voor elf sectoren en is een belangrijke stap waarmee kritieke entiteiten die essentiële diensten verlenen, beter in staat worden gesteld incidenten te voorkomen, te weerstaan, te verzachten, op te vangen, er bescherming tegen te bieden, erop te reageren, zich eraan aan te passen en ervan te herstellen.

In de **financiële** sector werd tevens de wet digitale operationele veerkracht (*Digital Operational Resilience Act* — DORA) vastgesteld[12], als onderdeel van het pakket digitaal geldwezen. Na de uitvoering van DORA zal de digitale operationele veerkracht van de financiële sector in de EU versterkt zijn dankzij de stroomlijning en verbetering van de bestaande regels, door de invoering van nieuwe vereisten waar dat nodig is.

Om **kritieke infrastructuur** nog beter **tegen grootschalige cyberaanvallen** te beschermen, zijn de Commissie, de hoge vertegenwoordiger en de NIS-samenwerkingsgroep[13] **risicoscenario's** aan het opstellen met betrekking tot de cyberbeveiliging in de sectoren energie, telecommunicatie, vervoer en ruimtevaart. Daarnaast zijn ook werkzaamheden aan de gang in verband met maatregelen voor de verbetering van het collectieve beschermingsniveau en de cyberveerkracht van ruimtecommunicatiesystemen en -diensten[14]. Bovendien wordt er

---

7 Voorstel tot herziening van Richtlijn (EU) 2016/1148.

8 COM(2020) 823.

9 COM(2020) 829.

10 De volgende sectoren vallen binnen het toepassingsgebied van de NIS2- en de CER-richtlijn: energie, vervoer, bankwezen, financiëlemarktinfrastructuren, digitale infrastructuur, gezondheidszorg, drinkwater, afvalwater, openbaar bestuur, ruimtevaart en voedselproductie, -verwerking en -distributie.

11 Momenteel is tussen nationale deskundigen in de NIS-samenwerkingsgroep overleg aan de gang in verband met ondersteuning aan de lidstaten bij de omzetting en uitvoering van de NIS2-richtlijn.

12 COM (2020) 595. Politiek akkoord bereikt in mei 2022.

13 De groep bestaat uit vertegenwoordigers van de lidstaten, de Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), ter ondersteuning en facilitering van de strategische samenwerking tussen de lidstaten betreffende de beveiliging van netwerk- en informatiesystemen.

14 Conclusies van de Raad over de ontwikkeling van de cyberstrategie van de Europese Unie, 23 mei 2022.

gewerkt aan gerichte cyberbeveiligingsrisicobeoordelingen voor communicatie-infrastructuur en -netwerken in de EU (met inbegrip van vaste en mobiele infrastructuur, satellieten, onderzeese kabels en internetrouting)[15]. De Commissie heeft tevens een initiatief opgestart voor het uitwerken van scenario's in verband met **natuurrampen die te maken hebben met bedreigingen van de veiligheid** zoals cyberaanvallen of terrorisme, om de rampenpreventie, -paraatheid en -respons te verbeteren.

De sabotage van de Nord Stream-gaspijpleidingen en andere recente incidenten hebben duidelijk gemaakt dat **kritieke infrastructuur van de EU** wordt bedreigd en dat maatregelen dringend nodig zijn. Op het kader van de CER- en de NIS2-richtlijn wordt dan ook vooruitgelopen zodat de maatregelen voor de versterking van de weerbaarheid van kritieke infrastructuur en de verbetering van de paraatheid en respons in sleutelsectoren sneller kunnen worden genomen. Een en ander werd samengebracht in een **aanbeveling van de Raad**[16] waarmee de effectieve uitvoering van de richtlijnen kan worden versneld. Zij voorziet in een gemeenschappelijke aanpak voor het uitvoeren van **stresstests** bij entiteiten die kritieke infrastructuur exploiteren, te beginnen in de energiesector, volgens gezamenlijk overeengekomen beginselen. De werkzaamheden met betrekking tot de stresstests gaan onmiddellijk van start zodat zij voor het einde van 2023 voltooid kunnen zijn; in april 2023 zal er dan een balans van de vorderingen worden opgemaakt. De Commissie zal, in samenwerking met de Raad en voortbouwend op de ondersteuning en de bijdragen van de relevante agentschappen van de Unie, een blauwdruk opstellen die bedoeld is om een gecoördineerde respons op EU-niveau te waarborgen wanneer zich aanzienlijke verstoringen van kritieke infrastructuur voordoen.

In de **energiesector** werkt de Commissie momenteel aan een netcode voor de cyberbeveiliging van grensoverschrijdende elektriciteitsstromen[17], met inbegrip van regels voor risicobeoordelingen, gemeenschappelijke minimumeisen, planning, toezicht, verslaglegging en crisisbeheersing, die volledig zal samenhangen met het NIS2-kader. In een afzonderlijke maatregel als reactie op de agressie van Rusland tegen Oekraïne werden de elektriciteitsnetten van Oekraïne en Moldavië in maart 2022 gesynchroniseerd met het net van continentaal Europa, in aanvulling op risicobeperkende maatregelen, onder meer op het gebied van cyberbeveiliging.

In de **vervoerssector** werkt de Commissie samen met de lidstaten, het Agentschap van de Europese Unie voor de veiligheid van de luchtvaart (EASA) en het Inlichtingen- en situatiecentrum van de Europese Unie (EU-Intcen) aan regelmatige beoordelingen van het risico- en dreigingsniveau voor de EU-burgerluchtvaart in conflictgebieden. Het EU-waarschuwingssysteem voor conflictgebieden wordt genoemd als een goede praktijk op internationaal niveau[18]. Maatregelen omvatten een heropstart van de werkstroom inzake risicobeoordelingen in verband met luchtvracht, een eerste risicobeoordeling op EU-niveau om de dreigingen voor passagiersschepen te evalueren, een alomvattende exercitie om de

[15] Overeenkomstig de oproep van Nevers om de EU-capaciteiten op het gebied van cyberbeveiliging te versterken, waarover een akkoord werd bereikt tijdens de informele bijeenkomst van de EU-ministers voor telecommunicatie op 9 maart 2022.

[16] Voorstel COM(2022) 551 van de Commissie werd gevolgd door de goedkeuring van een aanbeveling van de Raad op 8 december 2022.

[17] Dit is vereist bij Verordening (EU) 2019/943, de elektriciteitsverordening.

[18] Internationale Burgerluchtvaartorganisatie (doc. 10084 getiteld "Risk Assessment Manual for Civil Aircraft Operations Over or Near Conflict Zones" 2018).

luchtvaartbeveiliging in kaart te brengen en de beoordeling van dreigingen voor de burgerluchtvaart te actualiseren.

Kritieke maritieme infrastructuur krijgt eveneens speciale aandacht[19]. De gemeenschappelijke gegevensuitwisselingsstructuur voor het maritieme domein wordt momenteel ontwikkeld en zal eind 2023 volledig operationeel zijn en de maritieme bewakingsautoriteiten op vrijwillige basis onderling verbinden voor de bijna realtime uitwisseling van informatie. Ook het European Coast Guard Functions Forum heeft zijn bewakingscapaciteit tegen cyberaanvallen versterkt.

Verscheidene onderzoeksprojecten in het kader van **Horizon Europa** zijn eveneens gericht op het veiliger maken van onze digitale infrastructuur en het opbouwen van capaciteit om cyberaanvallen te voorkomen en af te slaan[20].

De cyberbeveiliging van de EU verbeteren

Op 16 december 2020 stelden de Commissie en de hoge vertegenwoordiger een nieuwe **EU-strategie inzake cyberbeveiliging voor het digitale tijdperk**[21] voor, om de gezamenlijke weerbaarheid van Europa tegen cyberdreigingen te versterken en ervoor te zorgen dat burgers en bedrijven hun voordeel kunnen doen met betrouwbare en veilige diensten en digitale instrumenten. De strategie is nagenoeg volledig uitgevoerd.

In de NIS2-richtlijn wordt voorzien in de oprichting van een **Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe)**[22] om het gecoördineerde beheer van grootschalige cyberbeveiligingsincidenten en -crises op operationeel niveau te ondersteunen. Het zal de regelmatige uitwisseling van relevante informatie tussen de lidstaten en instellingen, organen en instanties van de EU garanderen. De Commissie ontwikkelt momenteel een **situatie- en analysecentrum voor cyberbeveiliging** om haar interne capaciteit op te drijven. De Commissie werkt samen met de lidstaten aan een **gezamenlijke cybereenheid**[23] om een gecoördineerde respons van de EU op grootschalige cyberincidenten te waarborgen — ook in het kader van de follow-up voor haar aanbeveling ter zake. Daarnaast waren de Commissie en de hoge vertegenwoordiger actief betrokken bij cyberoefeningen die in 2022 door de lidstaten werden georganiseerd[24].

Netwerken en computersystemen vereisen onafgebroken monitoring en analyse opdat onbevoegde toegang en anomalieën in real time kunnen worden opgespoord. De Commissie heeft voorgesteld om in de hele EU een netwerk van centra voor beveiligingsoperaties (***Security Operations Centres* —** SOC's) op te zetten om communicatienetwerken te monitoren en verdachte gebeurtenissen te identificeren. De collectieve opsporingsvermogens zullen worden versterkt door bestaande SOC's op te schalen, nieuwe centra op te richten en

---

19 Onder meer door de uitvoering van PESCO-vermogensprojecten en Horizon 2020-projecten.

20 EU-CIP, voor een Europese kennishub en een proefbank voor beleid inzake de bescherming van kritieke infrastructuur, en ATLANTIS — *The Atlantic Testing Platform for Maritime Robotics: New Frontiers for Inspection and Maintenance of Offshore Energy Infrastructures*.

21 JOIN(2020) 18.

22 EU-CyCLONe bestaat uit de vertegenwoordigers van de autoriteiten voor crisisbeheer van de lidstaten, met deelname van de Commissie wanneer een mogelijk of actueel grootschalig cyberbeveiligingsincident aanzienlijke effecten heeft of kan hebben op de in de richtlijn bepaalde diensten en activiteiten.

23 COM (2021) 4520.

24 Voorbeelden zijn onder meer de *Blueprint Operational Level Exercise (Blue OLEx)*, georganiseerd door Litouwen en Enisa, en de *EU Cyber Crisis Linking Exercise on Solidarity (EU CyCLES*), georganiseerd door het Franse voorzitterschap.

SOC's in verschillende lidstaten met elkaar te verbinden. Daarbij zou ook gebruik kunnen worden gemaakt van de recentste artificiële intelligentie (AI) en data-analyse om civiele communicatienetwerken te beschermen en de opsporing van cyberaanvallen te versnellen[25].

Ter versterking van de paraatheid voor en de respons op ernstige cyberincidenten heeft de Commissie tevens een kortlopend programma opgezet om de lidstaten, via aanvullende financiering aan Enisa, te ondersteunen bij onder meer penetratietesten van kritieke entiteiten zodat kwetsbaarheden in kaart kunnen worden gebracht. Dit kan de lidstaten ook helpen bij hun incidentrespons, via Enisa met de steun van betrouwbare cyberbeveiligingsaanbieders uit de particuliere sector, na een ernstig incident waarbij kritieke entiteiten betrokken zijn. In een volgende stap zal ervoor worden gezorgd dat de lidstaten ten volle gebruik maken van deze mogelijkheden.

Zowel hardware als software worden steeds meer het mikpunt van **cyberaanvallen**. Er doen zich steeds meer cyberaanvallen voor, die bovendien steeds gesofisticeerder zijn in het uitbuiten van de zwakke punten van software. Bij twee derde van alle incidenten die in het kader van de NIS werden gerapporteerd, werd van dergelijke kwetsbaarheden van de software geprofiteerd. De gevolgen voor burgers, infrastructuur of bedrijven zijn ook steeds groter[26]. Bij twee derde van alle incidenten die in het kader van de NIS werden gerapporteerd, werd van dergelijke kwetsbaarheden van de software geprofiteerd. In september 2022 heeft de Commissie de **wet inzake cyberweerbaarheid**[27] voorgesteld, die erop gericht is producten met digitale elementen minder kwetsbaar te maken en te zorgen voor de snelle beschikbaarheid van patches en risicobeperkende maatregelen. Volgens het voorstel zouden producten met digitale elementen (hardware en software) uitsluitend in de handel mogen worden gebracht als zij voldoen aan specifieke essentiële cyberbeveiligingsvereisten[28]. Fabrikanten en ontwikkelaars zouden de cyberbeveiliging van hun producten gedurende vijf jaar moeten garanderen en de consumenten transparante informatie verstrekken over de cyberbeveiliging van hun producten. Dit zal aanzienlijk bijdragen aan de veiligheid van de toeleveringsketen[29].

Certificering speelt een cruciale rol bij de toename van het vertrouwen in en de beveiliging van belangrijke producten en diensten voor de digitale wereld. Met de wet inzake cyberweerbaarheid[30] wordt een Europees cyberbeveiligingscertificeringskader opgezet waarin de Commissie Enisa kan vragen certificeringsregelingen te ontwikkelen. Op basis van gemeenschappelijke criteria werd een Europese cyberbeveiligingscertificeringsregeling

---

[25] Een eerste fase werd gestart met een in november 2022 gepubliceerde oproep tot het indienen van voorstellen voor de capaciteitsopbouw van centra voor beveiligingsoperaties en een oproep tot indiening van blijken van belangstelling voor een gezamenlijke aanbesteding voor instrumenten en infrastructuren met het Europees Kenniscentrum voor cyberbeveiliging (ECCC), waarvoor in totaal 110 miljoen EUR aan EU-financiering uit het programma Digitaal Europa wordt gereserveerd.

[26] Enisa Threat landscape 2022.

[27] COM(2022) 454.

[28] Inmiddels heeft de Commissie in oktober 2021 in het kader van de richtlijn radioapparatuur een gedelegeerde verordening vastgesteld waarbij de fabrikanten van radioapparatuur verplicht zijn hun cyberbeveiliging, de bescherming van de privacy van gebruikers en de bescherming tegen fraude op te drijven.

[29] Overeenkomstig de conclusies van de Raad inzake de beveiliging van ICT-toeleveringsketens, 17 oktober 2022.

[30] Bij Verordening 2018/881 werd een EU-breed cyberbeveiligingscertificeringskader voor ICT-producten, -diensten en -processen ingevoerd.

ontwikkeld en regelingen voor clouddiensten en 5G-beveiliging worden momenteel voorbereid.

De Commissie zet haar werkzaamheden in verband met de veiligheid en weerbaarheid van **5G-netwerken** samen met de lidstaten voort en blijft de uitvoering van het EU-instrumentarium voor 5G op nationaal en EU-niveau van zeer nabij volgen. Hoewel de overgrote meerderheid van de lidstaten de beveiligingseisen voor 5G-netwerken reeds heeft versterkt of daarmee aan de slag is, moeten alle lidstaten nu dringend de uitvoering van de instrumentariummaatregelen voltooien[31]. Zij moeten met name beperkingen op leveranciers met een hoog risico vaststellen, aangezien tijdverlies de kwetsbaarheid van de netwerken in de Unie kan vergroten, en ook de fysieke en niet-fysieke bescherming van kritieke en gevoelige onderdelen van 5G-netwerken versterken, onder meer met behulp van strenge toegangscontrole.

Om de EU en de lidstaten te helpen bij een proactieve, strategische aanpak van het cyberbeveiligingsbeleid voor de industrie, zal het **Europees kenniscentrum voor cyberbeveiliging** met nationale coördinatiecentra samenwerken aan de ondersteuning van innovatie in cyberbeveiliging en de versterking van de capaciteiten van de gemeenschap die zich bezighoudt met cyberbeveiligingstechnologie[32].

In september 2022 heeft Enisa formeel een **Europees kader voor cyberbeveiligingsvaardigheden** in het leven geroepen, waarin de noodzakelijkste functieprofielen op dat gebied worden aangewezen en een gemeenschappelijke Europese grondslag wordt gelegd voor de bevordering van de erkenning van vaardigheden en de ontwikkeling van opleidingen op het gebied van cyberbeveiliging. Dit kader zal dienen als bouwsteen voor de **Academie voor vaardigheden op het gebied van cyberbeveiliging** die in het kader van het werkprogramma 2023 van de Commissie werd voorgesteld en die een alomvattende aanpak zal bieden om de toenemende behoefte aan cyberbeveiligingsspecialisten in Europa in te vullen.

Gezien de gevoelige gerubriceerde en niet-gerubriceerde EU-informatie die door **instellingen, organen en instanties van de EU** wordt behandeld, is het belangrijk dat deze goed tegen cyberaanvallen wordt beschermd. In maart 2022 kwam de Commissie met een voorstel voor een verordening betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in deze organen[33], waarin zij de beginselen die aan de NIS2-richtlijn ten grondslag liggen, toepaste op de instellingen van de EU. Het voorstel omvat een nieuwe interinstitutionele raad voor cyberbeveiliging en een versterkt cyberbeveiligingscentrum (CERT-EU)[34] die moeten zorgen voor correcte informatie-uitwisseling en voor samenwerking met de autoriteiten van de lidstaten, bijvoorbeeld via het netwerk van Cyber Security Incident Response Teams (CSIRT's). Parallel daarmee heeft de Commissie een voorstel voor een verordening betreffende informatiebeveiliging in de instellingen, organen en instanties van de

---

31 De lidstaten hebben eerder dit jaar, met de steun van de Commissie en Enisa, een verslag gepubliceerd over de cyberbeveiliging van open radiotoegangsnetwerken die, wanneer zij rijper zullen zijn, een andere manier zullen bieden om het onderdeel radiotoegang van 5G-netwerken uit te rollen op basis van open interfaces.

32 De raad van bestuur van het ECCC is samengesteld en heeft op 20 oktober 2022 zijn vierde vergadering gehouden.

33 COM(2022) 122.

34 CERT-EU heeft bovendien aanzienlijk geïnvesteerd in de verdere verbetering van zijn bestaande dienstverlening aan instellingen, organen en instanties van de EU en in de toevoeging van nieuwe diensten voor een betere preventie en opsporing van en respons op cyberaanvallen.

Unie[35] vastgesteld, om de weerbaarheid tegen cyber- en hybride dreigingen te versterken door een gemeenschappelijke reeks voorschriften inzake informatiebeveiliging voor alle instellingen en organen van de Unie in het leven te roepen. Het is van essentieel belang dat de Raad spoed zet achter zijn werkzaamheden in verband met dit voorstel, gezien de talrijke oproepen van de lidstaten aan de Commissie om werk te maken van maatregelen die het besluitvormingsproces van de EU beter beschermen tegen kwaadwillige activiteiten van allerlei aard. CERT-EU en Enisa hebben tevens een nieuw type cyberoefening ontworpen en getest dat is toegesneden op EU-agentschappen, zoals werd aanbevolen door de Europese Rekenkamer.

Voorbeelden van belangrijke resultaten

De Europese maand van de cyberbeveiliging: dit initiatief, dat bestaat uit workshops, socialemediacampagnes en lezingen, is van 184 activiteiten in 2014 gegroeid naar 500 activiteiten in oktober 2022. Dankzij deze activiteiten kunnen gebruikers online beter reageren wanneer zij worden geconfronteerd met een cyberbeveiligingsdreiging (zoals gerapporteerd door 73 % van de lidstaten tijdens een enquête in 2021).

De Cybersecurity Higher Education Database (CyberHEAD): Met ongeveer 70 000 bezoeken per jaar is CyberHEAD de webpagina van Enisa die de afgelopen twee jaar het meest werd bezocht. Jonge talenten krijgen via de webpagina een overzicht van het scala aan mogelijkheden voor een hogere opleiding in cyberbeveiliging en kunnen dan met kennis van zaken besluiten welke mogelijkheid zij zullen aangrijpen. De webpagina helpt universiteiten bij het aantrekken van studenten die sterk gemotiveerd zijn om te werken aan de cyberbeveiliging van Europa.

Hybride bedreigingen afwenden, buitenlandse inmenging bestrijden en de cyberdefensie van de EU verbeteren

In het **strategisch kompas** voor veiligheid en defensie **van de EU** wordt een ambitieus actieplan uiteengezet om de EU beter in staat te stellen om op te treden, de weerbaarheid te versterken en beter te investeren in de defensievermogens van de EU.

Hoewel het afwenden van **hybride bedreigingen** in hoofdzaak onder de verantwoordelijkheid van de lidstaten valt, vult de EU het nationale optreden aan door de coördinatie te ondersteunen, het situationeel bewustzijn te verbeteren, de samenwerking met gelijkgestemde landen en internationale organisaties te bevorderen, en te voorzien in mogelijkheden voor een gezamenlijke respons. Tijdens het afgelopen decennium werden meer dan tweehonderd maatregelen genomen om de weerbaarheid te verbeteren en hybride dreigingen op EU-niveau af te wenden. De fusiecel voor analyse van hybride dreigingen, EU-Intcen, draagt bij aan de besluitvorming van de EU en is het centrale orgaan voor alomvattend situationeel bewustzijn en strategische prognoses, dat informatie uit alle bronnen samenbrengt en inlichtingen over hybride dreigingen analyseert. In het strategisch kompas werd de oprichting van EU-teams voor snelle reactie op hybride dreigingen aangekondigd. De werkzaamheden in verband hiermee zijn van start gegaan. Deze teams zullen de lidstaten, GVDB-missies en -operaties en partnerlanden ondersteunen bij de bestrijding van hybride dreigingen door op korte termijn gebruik te maken van de betreffende expertise van de lidstaten en de EU, zo nodig expertise op militair gebied. Momenteel wordt een EU-toolbox tegen hybride dreigingen ontwikkeld die een kader zal vormen voor een gecoördineerde respons op hybride campagnes die de EU en haar lidstaten treffen, waarin de externe en interne dimensie naadloos zijn samengebracht

35 COM(2022) 119.

en zowel de nationale als EU-brede overwegingen in aanmerking worden genomen. Er is ook aanzienlijke vooruitgang geboekt met de verbetering van de weerbaarheid tegen en de bestrijding van hybride dreigingen door te inventariseren hoe goed sectoren momenteel bestand zijn tegen die dreigingen[36]. De Commissie heeft voorts het analytische onderzoek over de opbouw van weerbaarheid tegen hybride dreigingen[37] voortgezet en de integratie van overwegingen inzake hybride dreigingen in de beleidsvorming voltooid.

Uit de COVID-19-pandemie en de oorlog van Rusland tegen Oekraïne is gebleken hoe manipulatie van de informatieomgeving van invloed kan zijn op de EU en partners overal ter wereld. **Buitenlandse desinformatie en inmenging** gericht op het ondergraven van het vertrouwen in de EU en de op regels gebaseerde internationale orde maakt ook een steeds groter deel uit van hybride aanvallen. Voortbouwend op het Europees actieplan voor democratie heeft de Commissie een reeks tastbare maatregelen en structuren ingevoerd om informatiemanipulatie en desinformatie aan te pakken, onder meer de herziene gedragscode inzake desinformatie, de wet inzake digitale diensten en het voorstel betreffende transparantie en gerichte politieke reclame waarover momenteel interinstitutionele onderhandelingen gaande zijn. Dit zou uitmonden in nieuwe verplichtingen voor platformen en een eerste wettelijk bindend toezichtskader. Daarnaast is de EDEO, zoals aangekondigd in het strategisch kompas, in nauwe samenwerking met de Commissie en de lidstaten, bezig met de verdere ontwikkeling van een **EU-instrumentarium voor het aanpakken en tegengaan van buitenlandse desinformatie en inmenging**, om een gecoördineerde respons op manipulatief gedrag van buitenlandse actoren te stimuleren[38]. De EDEO is tevens de samenwerking met internationale partners zoals de NAVO en het snellereactiemechanisme van de G7 blijven versterken.

De Commissie veroordeelt elke buitenlandse inmenging op het soevereine grondgebied van de EU-lidstaten en maakt zich zorgen over de meldingen betreffende Chinese buitenlandse politiebureaus in de EU, die, als ze waar zijn, volstrekt onaanvaardbaar zouden zijn. Hoewel het tot de bevoegdheid van de autoriteiten van de lidstaten behoort om deze beweringen te onderzoeken, staat de Commissie klaar om, met de steun van Europol, de uitwisseling van informatie tussen de lidstaten te vergemakkelijken. De Commissie heeft deze kwestie ter sprake gebracht tijdens de Raad Justitie en Binnenlandse Zaken van december 2022.

In november 2022 hebben de Commissie en de hoge vertegenwoordiger een nieuw EU-beleid op het gebied van **cyberdefensie**[39] gepresenteerd, waarin wordt uiteengezet hoe de samenwerking en investeringen in cyberdefensie kunnen worden versterkt om een betere bescherming tegen cyberaanvallen te waarborgen. Het beleid heeft tot doel de belangen van de EU in cyberspace te verdedigen aan de hand van een betere samenwerking tussen cyberdefensieactoren in de EU door mechanismen te ontwikkelen om vermogens op EU-niveau te benutten, onder meer in het kader van GVDB-missies en -operaties. Met het beleid

[36] SWD(2022) 21.

[37] *Hybrid threats: a comprehensive resilience ecosystem*, JRC130097.

[38] Momenteel wordt gewerkt aan de in het strategisch kompas genoemde taken om een dataruimte te creëren voor het systematisch vergaren van gegevens over incidenten in verband met buitenlandse desinformatie en inmenging en de GVDB-missies en -operaties te voorzien van vermogens en middelen om de betreffende instrumenten van deze toolbox in te zetten. De EDEO blijft het open-source situationeel bewustzijn verbeteren via het systeem voor snelle waarschuwingen van de EU, zorgt voor een grotere bewustwording, met name aan de hand van de campagne EUvsDisinfo, en heeft zijn samenwerking met belanghebbenden zoals de NAVO en het snellereactiemechanisme van de G7 verder verbeterd.

[39] JOIN(2022) 49.

zal de ontwikkeling van een volledig spectrum van cyberdefensievermogens een nieuwe impuls krijgen en zal de samenwerking tussen de militaire en civiele cybergemeenschappen van de EU worden versterkt, doordat het situationeel bewustzijn, de crisiscoördinatie en de opleiding, ook met de particuliere sector, worden verbeterd. Met het beleid zullen tevens de strategische afhankelijkheden op het gebied van kritieke cybertechnologieën worden verminderd aan de hand van de ontwikkeling van een strategische routekaart voor kritieke cyberbeveiligings- en cyberdefensietechnologieën, en zal de Europese technologische en industriële defensiebasis worden versterkt.

In het strategisch kompas wordt de **ruimte** aangeduid als vijfde operationele domein voor oorlogsvoering (naast land, zee, lucht en cyberspace) en worden de Commissie en de hoge vertegenwoordiger verzocht de eerste ruimtestrategie voor veiligheid en defensie te ontwikkelen. In die strategie zullen maatregelen worden voorgesteld om het collectieve beschermings- en weerbaarheidsniveau van ruimtesystemen en -diensten te verbeteren en alle dreigingen, ook cyberdreigingen, voor gevoelige ruimtesystemen en -diensten in de EU af te wenden en erop te reageren.

3. BESTRIJDING VAN TERRORISME EN RADICALISERING

Nagenoeg alle belangrijke initiatieven die in de EU-veiligheidsstrategie zijn voorgesteld om de lidstaten te ondersteunen bij de bestrijding van terrorisme en radicalisering zijn goedgekeurd. De bescherming tegen onlinedreigingen vormde daarbij een bijzonder thema. In een volgende stap moet worden gewaarborgd dat deze initiatieven hun volledige effect sorteren.

Bestrijding van terrorisme

De agenda inzake terrorismebestrijding voor de EU[40] heeft, sinds de vaststelling ervan in december 2020, de EU de middelen in handen gegeven om beter te anticiperen op terroristische dreigingen, deze dreigingen te voorkomen, ertegen te beschermen en erop te reageren. Specifieke geografische initiatieven hebben ook geholpen bij de reactie op de evoluerende situatie inzake bedreigingen. In het licht van ontwikkelingen in Afghanistan heeft de EU-coördinator voor terrorismebestrijding in samenspraak met de Commissie, de hoge vertegenwoordiger, het voorzitterschap en belangrijke EU-agentschappen een **actieplan inzake terrorismebestrijding voor Afghanistan**[41] opgesteld, dat in oktober 2021 door de lidstaten werd bekrachtigd. Een duidelijke verwezenlijking van dit actieplan was een vrijwillige procedure voor strengere veiligheidscontroles op mensen die uit Afghanistan afkomstig zijn.

Voorrang wordt gegeven aan het afweren van de dreiging die uitgaat van **terugkerende buitenlandse terroristische strijders** die zich momenteel in Syrië en Irak bevinden. Hoewel de primaire verantwoordelijkheid bij de lidstaten ligt, helpt samenwerking op EU-niveau de lidstaten bij de aanpak van gemeenschappelijke uitdagingen zoals het vervolgen van personen die terreurdaden hebben begaan, het voorkomen van onopgemerkte binnenkomst in het Schengengebied en de re-integratie en rehabilitatie van teruggekeerde buitenlandse terroristische strijders. De Commissie blijft nauw samenwerken met de lidstaten en belangrijke partnerlanden om ervoor te zorgen dat van het slagveld afkomstig bewijsmateriaal

[40] COM (2020) 795.

[41] *Afghanistan: Counter-Terrorism Action Plan*, 29 september 2021.

wordt ingevoerd in EU-databanken en -informatiesystemen. De EU-coördinator voor terrorismebestrijding is in overleg met de lidstaten en in nauwe samenwerking met de hoge vertegenwoordiger en de Commissie aan het onderzoeken hoe verbeterde levensomstandigheden in gevangenissen en kampen in Noordoost-Syrië kunnen worden aangewend om radicalisering te helpen bestrijden.

De EU-wetgeving inzake de bestrijding van terrorisme werd geactualiseerd. **De richtlijn inzake terrorismebestrijding** die in 2017 werd vastgesteld, wordt momenteel door alle lidstaten uitgevoerd[42] om gedrag zoals het volgen van een opleiding of het ondernemen van een reis met terroristisch oogmerk en de financiering van terrorisme strafbaar te stellen. De onjuiste omzetting van de richtlijn in een aantal lidstaten moet nog altijd worden aangepakt.

Terroristen de middelen ontnemen om een aanval uit te voeren is van cruciaal belang in de strijd tegen terrorisme. Nagenoeg alle lidstaten hebben momenteel de geactualiseerde wetgeving inzake vuurwapens[43] in nationaal recht omgezet. In februari 2021 trad nieuwe wetgeving in werking die gericht is op de beperking van de toegang tot precursoren voor explosieven die terroristen zouden kunnen gebruiken om bommen te vervaardigen. Op basis van de aanpak die wordt gehanteerd om de toegang tot precursoren voor explosieven te reguleren, onderzoekt de Commissie hoe de toegang kan worden beperkt tot bepaalde gevaarlijke chemische stoffen die kunnen worden gebruikt om aanslagen te plegen.

Openbare ruimten zijn herhaaldelijk het mikpunt van terroristische aanslagen geweest. De Commissie heeft een handboek uitgegeven voor de bevordering van de beveiliging door ontwerp van openbare ruimten[44]. Dit volgt op uitvoerige technische richtsnoeren[45], instrumenten voor de beoordeling van de kwetsbaarheid van openbare ruimten[46] en alomvattende ondersteuning voor belangrijke belanghebbenden[47], evenals een aanbeveling inzake vrijwillig in acht te nemen prestatie-eisen voor röntgenapparatuur voor gebruik in openbare ruimten (met uitzondering van de luchtvaart)[48]. In 2022 heeft het Fonds voor interne veiligheid ook 14,5 miljoen EUR gefinancierd voor projecten ter verbetering van de bescherming van openbare ruimten, waaronder gebedshuizen. **Drones** zijn zeer innovatieve instrumenten die kunnen worden ingezet voor legitieme doeleinden, maar ook met kwaadwillige bedoelingen, zoals aanvallen op openbare ruimten, personen en kritieke infrastructuur. In november 2022 heeft de Commissie een **dronestrategie 2.0** vastgesteld[49], die in 2023 zal worden gevolgd door een uitvoeriger EU-aanpak voor de bestrijding van het kwaadwillige gebruik van drones.

---

42 COM (2021) 701. De lidstaten moesten deze uiterlijk op 8 september 2018 in nationaal recht hebben omgezet.

43 COM(2015) 750.

44 SWD(2022) 398.

45 *Guideline — Building Perimeter Protection, EUR 30346 EN.*

46 http://counterterrorism.jrc.ec.europa.eu

47 Zie met name: *EU Digital Autumn School* (JRC127168) en *Terrorism and Extremism Database — User Guide* (JRC130461).

48 In deze handeling wordt aan de lidstaten de aanbeveling gegeven om aan de EU-prestatie-eisen te voldoen in aanbestedingen voor röntgenapparatuur die in openbare ruimten wordt gebruikt om dreigingen op te sporen (C(2022) 4179).

49 COM(2022) 652.

Bestrijding van radicalisering die leidt tot gewelddadig extremisme en terrorisme online en offline

Radicalisering voorkomen en bestrijden is van cruciaal belang voor een doeltreffend terrorismebestrijdingsbeleid. De Commissie ondersteunt de lidstaten met het netwerk voor voorlichting over radicalisering waarin 6 000 deskundigen zijn samengebracht die actief zijn in preventieve werkzaamheden. Tot de belangrijkste gebieden voor ondersteuning van de lidstaten behoren onder meer de bestrijding van gewelddadige extremistische ideologieën en de polarisatie die leidt tot radicalisering; radicalisering online en het misbruik van nieuwe technologieën; en het beheren en voorbereiden van de integratie van vrijgekomen daders. Verbanden tussen gewelddadige extremistische groepen en ideologieën en haatzaaiende uitlatingen worden aangepakt met behulp van de EU-gedragscode om de verspreiding van illegale haatuitingen op internet tegen te gaan[50].

De EU werkt momenteel ook aan het voorkomen van buitenlandse beïnvloeding en financiering van steun voor radicale/extremistische standpunten in de lidstaten. De Commissie van haar kant blijft waakzaam om te voorkomen dat EU-middelen projecten ondersteunen die niet verenigbaar zijn met de Europese waarden of die een illegale agenda proberen uit te voeren. In dit verband worden door de Commissie beheerde projecten sinds eind 2021 op een uniek platform, het financierings- en aanbestedingenportaal, gepubliceerd zodra de subsidieovereenkomst ondertekend is. Het is van essentieel belang dat de lidstaten dit venster gebruiken voor hun eigen screening van de begunstigden en de Commissie eventuele aanvullende informatie verstrekken waarover zij beschikken. In dit verband omvat het voorstel van de Commissie voor een herziening van het Financieel Reglement de toevoeging van een veroordeling voor het aanzetten tot haat als reden voor uitsluiting van EU-financiering. De Commissie roept het Europees Parlement en de Raad op deze kwestie in de definitieve tekst doeltreffend aan te pakken. Daarnaast treft de Commissie momenteel maatregelen om het interne bewustzijn te vergroten en ontwikkelt zij interne werkmethoden om de toetsing bij de selectie van projecten aan te scherpen.

Het voorkomen van radicalisering online is een ander belangrijk aandachtspunt. De **verordening inzake het tegengaan van de verspreiding van terroristische online-inhoud**[51] werd van toepassing in juni 2022. Sindsdien kunnen nationale bevoegde autoriteiten eisen dat terroristische inhoud uiterlijk één uur na een officieel verwijderingsbevel wordt verwijderd. Aanbieders van onlinediensten die aan terroristische inhoud worden blootgesteld, moeten specifieke maatregelen treffen om hun platformen tegen misbruik te beschermen. Dit vormt een aanvulling op de werkzaamheden van het **EU-internetforum**, dat de Commissie heeft opgestart om de lidstaten, internetondernemingen en maatschappelijke organisaties samen te brengen zodat zij de verspreiding van gewelddadige extremistische en terroristische inhoud via internet kunnen voorkomen. Recente ondersteuning van het EU-internetforum aan de inhoudsmoderatie van techbedrijven en aanbieders van internetinfrastructuur omvat een adresboek van door terroristen geëxploiteerde websites en een jaarlijks geactualiseerd kennispakket over gewelddadige rechts-extremistische groepen, symbolen en manifesten[52].

---

50 https://ec.europa.eu/commission/presscorner/detail/nl/IP_16_1937

51 Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud, PB L 172 van 17.5.2021, blz. 79.

52 Andere resultaten zijn onder meer: een actualisering van het EU-crisisprotocol; handboeken met richtsnoeren betreffende het kwaadwillige gebruik van “borderline” inhoud en videospellen (die dus op het randje van de

Sinds 2019 houdt dit forum zich ook bezig met het voorkomen van seksueel misbruik van kinderen op internet.

Voorbeelden van belangrijke resultaten

Hoe samenwerking met Eurojust ertoe leidde dat een buitenlandse strijder werd veroordeeld voor terrorisme: het belangrijkste doelwit van een onderzoek in verband met terrorisme werd in 2021 veroordeeld tot een gevangenisstraf van vier jaar voor deelname aan een terroristische organisatie nadat de Italiaanse autoriteiten het register voor terrorismebestrijding hadden gebruikt om verbanden vast te stellen tussen een verdachte buitenlandse strijder en andere terrorismezaken. Eurojust bracht de nationale autoriteiten bij elkaar, wat leidde tot de uitvoering van Europese onderzoeksbevelen en verzoeken om wederzijdse rechtshulp.

Coördinatie van Europol tegen op internet beschikbare handleidingen voor het maken van bommen: in een reeks regelmatige gezamenlijke initiatieven werden tijdens een actiedag in februari 2022, ondersteund door Europol en met deelname van acht lidstaten en het Verenigd Koninkrijk, op internet honderden items gevonden met instructies voor het maken van bommen met behulp van precursoren en voor het gebruik ervan tijdens terroristische aanvallen. De informatie werd doorgegeven aan de aanbieders van onlinediensten.

4. BESTRIJDING VAN GEORGANISEERDE MISDAAD

In het landschap van de georganiseerde misdaad in Europa verandert de samenwerking tussen misdadigers voortdurend. Criminele netwerken kunnen betrokken zijn bij uiteenlopende criminele activiteiten, waarbij zij drugshandel combineren met georganiseerde vermogensdelicten, fraude, migrantensmokkel en mensenhandel[53]. Het toegenomen gebruik van internet en onlinediensten heeft de cybercriminaliteit en het gendergerelateerd cybergeweld verder gestimuleerd. Het toegenomen gebruik van versleutelde communicatietechnologieën beschermt weliswaar de privacy en de grondrechten, maar stelt de rechtshandhaving voor extra uitdagingen[54]. Intussen heeft de verstoring ten gevolge van de Russische aanvalsoorlog tegen Oekraïne nieuwe mogelijkheden gecreëerd, die snel worden uitgebuit door misdaadorganisaties.

In april 2021 heeft de Commissie de **EU-strategie voor de aanpak van georganiseerde criminaliteit 2021-2025**[55] vastgesteld. In de strategie wordt benadrukt dat het belangrijk is de structuren van de georganiseerde criminaliteit te ontmantelen en de aandacht toe te spitsen op groepen die een groter risico voor de veiligheid van Europa vormen en op personen in de hogere echelons van misdaadorganisaties. De uitvoering van de strategie is momenteel al goed gevorderd, want verschillende acties zijn reeds goedgekeurd en uitgevoerd. De Commissie heeft ook financiële steun verleend aan de lidstaten voor de bestrijding van de criminele dreigingen waarmee de EU wordt geconfronteerd[56].

---

illegaliteit zitten) en die leiden tot radicalisering; en een onderzoek naar de effecten van algoritmische versterking op het traject van de gebruiker naar radicalisering.

53 Europol (2021), *European Union serious and organised crime threat assessment, a corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Bureau voor publicaties van deEuropese Unie, Luxemburg.*

54 *Internet Organised Crime Threat Assessment (IOCTA)*, 2021.

55 COM(2021) 170.

56 In juli 2022 heeft de Commissie via het Fonds voor interne veiligheid 15,7 miljoen EUR toegewezen aan de lidstaten voor de ondersteuning van langetermijnprojecten en -activiteiten in het kader van het Europees

Cybercriminaliteit

Door de versnelde digitalisering tijdens de COVID-19-pandemie werd de verspreiding van cyberdreigingen zoals gijzelsoftware gestimuleerd[57]. **Gijzelsoftware** vormt een aanzienlijk cyberbeveiligingsrisico voor kritieke infrastructuur en de openbare veiligheid. Het Centrum voor de bestrijding van cybercriminaliteit van Europol heeft onlangs, samen met de gezamenlijke cybercrime-taskforce, het *International Ransomware Response Model* ontwikkeld om een alomvattende respons van de rechtshandhavingsinstanties te operationaliseren. De EU heeft deelgenomen aan de top van het Counter Ransomware Initiative van 2022 om de internationale samenwerking inzake gijzelsoftware te versterken. Tijdens de top kwamen 36 landen en de EU met elkaar overeen dat zij een internationale taskforce in verband met de bestrijding van gijzelsoftware zouden opzetten om de activiteiten in verband met de weerbaarheid tegen en de ontwrichting en bestrijding van illegale financieringsactiviteiten te coördineren[58]. De Commissie en Europol hebben samen een decryptieplatform[59] opgezet, zodat de forensische toegang tot digitaal bewijsmateriaal minder tijd vergt en versleutelde communicatienetwerken van criminelen kunnen worden ontcijferd, wat de georganiseerde misdaad zware slagen zal toebrengen.

De EU speelde een belangrijke rol in het welslagen van de onderhandelingen over het tweede aanvullend protocol bij het **Verdrag van Boedapest inzake cybercriminaliteit** in mei 2022. Daarin zijn broodnodige instrumenten opgenomen voor grensoverschrijdende samenwerking bij het onderzoeken en vervolgen van cybercriminaliteit, evenals uitvoerige voorwaarden en waarborgen voor gegevensbescherming. Alle lidstaten dienen het tweede aanvullend protocol snel te ondertekenen en het Europees Parlement wordt verzocht zijn goedkeuring te geven zodat snelle ratificatie mogelijk wordt. De Commissie is namens de EU tevens betrokken bij onderhandelingen over een nieuw cybercriminaliteitsverdrag van de Verenigde Naties.

Seksueel misbruik van kinderen is verontrustend alomtegenwoordig. Alleen al in 2021 werden wereldwijd 85 miljoen foto's en video's van seksueel misbruik van kinderen gemeld en nog veel meer beelden blijven ongemeld. Omdat kinderen meer tijd doorbrengen op internet, zijn ze vatbaarder voor grooming, wat leidt tot een toename aan door henzelf gemaakt uitbuitingsmateriaal. Overeenkomstig de in juli 2020 vastgestelde EU-strategie voor doeltreffendere bestrijding van seksueel misbruik van kinderen[60] en de alomvattende EU-strategie voor de rechten van het kind van maart 2021[61] heeft de Commissie in mei 2022 een voorstel goedgekeurd tot vaststelling van regels ter voorkoming en bestrijding van online seksueel misbruik van kinderen[62], met nieuwe verplichtingen voor aanbieders van onlinediensten. Wanneer een aanzienlijk risico niet kan worden beperkt met behulp van preventie, zouden aanbieders verplicht kunnen worden om online seksueel misbruik op te sporen, te melden, te verwijderen en te blokkeren. Het voorstel houdt tevens de oprichting in van een EU-centrum ter voorkoming en bestrijding van seksueel misbruik van kinderen om de uitvoering te vergemakkelijken. In de zomer van 2024 vervalt tijdelijke wetgeving die in

multidisciplinair platform tegen criminaliteitsdreiging (Empact), dat de tien EU-prioriteiten inzake misdaad aanpakt die de Raad voor de periode 2022-2025 heeft vastgesteld.

57 *Internet Organised Crime Threat Assessment Report (IOCTA)*.

58 International Counter Ransomware Initiative 2022, Washington DC, 1 november 2022.

59 Het decryptieplatform van Europol wordt gehost door het Gemeenschappelijk Centrum voor onderzoek van de Europese Commissie in Ispra.

60 COM(2020) 607.

61 COM(2021) 142.

62 COM(2022) 209.

augustus 2021 werd aangenomen om aanbieders van onlinediensten in staat te stellen hun vrijwillige opsporing en melding van online seksueel misbruik van kinderen voort te zetten[63]. Het is dan ook van cruciaal belang dat het Europees Parlement en de Raad snel tot een akkoord komen over de voorgestelde verordening. Begin volgend jaar zal dit initiatief worden aangevuld met een voorstel tot actualisering van de richtlijn ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie die dateert van 2011[64].

Cybergeweld tegen vrouwen en kinderen is een opkomende nieuwe dimensie van gendergerelateerd cybergeweld. In 2020 werd naar schatting één op twee jonge vrouwen met deze vorm van geweld geconfronteerd[65]. In haar voorstel voor een richtlijn ter bestrijding van geweld tegen vrouwen en huiselijk geweld[66], dat in maart 2022 werd vastgesteld, presenteerde de Commissie doelgerichte voorschriften inzake online en offline gendergerelateerd geweld tegen vrouwen[67].

Georganiseerde criminaliteit

Mensenhandel is een kernactiviteit van de georganiseerde misdaad in de EU[68]. In de strategie voor de veiligheidsunie werd mensenhandel reeds als een prioriteit aangewezen, maar desondanks hebben misdadigers de COVID-19-pandemie aangegrepen om aanzienlijke winsten te boeken en hun criminele activiteiten op te voeren. De snelle coördinatie op EU-niveau helpt bij het voorkomen van de intensievere dreiging van mensenhandel na de aanvalsoorlog van Rusland tegen Oekraïne. De EU-coördinator voor de bestrijding van mensenhandel heeft een **gemeenschappelijk plan ter bestrijding van mensenhandel**[69] ontwikkeld om de werkzaamheden van de Commissie met de lidstaten, EU-agentschappen en de Europese Dienst voor extern optreden samen te brengen, en zo de risico's van mensenhandel aan te pakken en potentiële slachtoffers te ondersteunen. Deze inspanningen hebben ertoe bijgedragen dat het aantal bevestigde gevallen van mensenhandel beperkt is gebleven, ook al blijft de dreiging nog steeds groot.

In april 2021 voorzag de EU-strategie voor de bestrijding van mensenhandel 2021-2025 in een alomvattend intern en extern kader voor actie[70]. De Commissie geeft momenteel gevolg aan deze strategie door binnenkort een voorstel tot wijziging van de **richtlijn inzake de voorkoming en bestrijding van mensenhandel**[71] voor te stellen waarin de tekortkomingen van het huidige wettelijke kader worden aangepakt en dit kader wordt geactualiseerd om rekening te houden met de onlinedimensie en te streven naar een terugdringing van de vraag.

---

63 COM(2020) 568.

64 Richtlijn 2011/93/EU van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, PB L 335 van 17.12.2011, blz. 1.

65 Onderzoeksdienst van het Europees Parlement (EPRS), *Combating gender-based violence: Cyberviolence, European added value assessment*, 2021.

66 COM(2022) 105.

67 Het voorstel omvat de strafbaarstelling op EU-niveau van het zonder instemming delen van intiem materiaal, cyberstalking, cyberintimidatie en het online aanzetten tot haat of geweld. Dit zou worden aangevuld met een nieuw kader voor samenwerking tussen internetplatformen om de veiligheid van vrouwen online beter te beschermen.

68 Dreigingsevaluatie van de ernstige en georganiseerde criminaliteit (SOCTA) 2021.

69 Plan ter bestrijding van mensenhandel om mensen te beschermen die de oorlog in Oekraïne ontvluchten (alleen in het Engels beschikbaar).

70 COM(2021) 171.

71 Het vierde voortgangsverslag inzake mensenhandel dat naast dit voorstel zal worden vastgesteld, bevat uitgebreide informatie over de uitvoering van de EU-strategie van 2019 tot en met 2022 evenals kerngegevens en statistieken.

In september 2022 was een gezamenlijke actiedag van Empact gericht op criminele netwerken die gebruik maken van websites en sociale media om slachtoffers te rekruteren met het oog op seksuele uitbuiting. Tijdens deze dag werd voor het eerst een EU-brede hackathon tegen mensenhandel gehouden, ondersteund door Europol en Eurojust, waaraan rechtshandhavingsinstanties uit twintig landen deelnamen. Er werden elf verdachten van mensenhandel en 45 mogelijke slachtoffers geïdentificeerd[72].

In tegenstelling tot wat bij mensenhandel het geval is, betalen mensen die de EU op irreguliere wijze proberen binnen te komen de smokkelaars uit eigen beweging. De activiteit van de smokkelaars is echter van criminele aard, brengt vaak mensenlevens in gevaar en kan leiden tot bijkomende veiligheidsrisico's voor de EU. Het voorkomen en bestrijden van **migrantensmokkel** is een belangrijke doelstelling van de EU-strategie voor de veiligheidsunie, de EU-strategie voor de aanpak van georganiseerde criminaliteit en het nieuwe migratie- en asielpact[73]. Het vergt onafgebroken internationale samenwerking en coördinatie op alle niveaus. De uitvoering van het EU-actieplan tegen migrantensmokkel 2021-2025[74] vordert, aangezien er momenteel operationele partnerschappen tegen migrantensmokkel worden ontwikkeld met Marokko, Niger en de Westelijke Balkan, ondersteund door instellingen, instanties en organen van de EU en met financiering van de EU.

De markt voor **illegale drugs** blijft, met een kleinhandelswaarde die op minimaal 30 miljard EUR per jaar wordt geraamd, de grootste criminele markt in de EU en vormt een belangrijke inkomstenbron voor misdaadorganisaties, evenals een bedreiging voor de maatschappelijke stabiliteit en de volksgezondheid. In 2021 hebben maatregelen en samenwerking van de EU ertoe geleid dat drugs ter waarde van 7 miljard EUR van de straat werden gehaald[75]. In de **EU-agenda en het EU-actieplan inzake drugs voor 2021-2025**[76] van juli 2020 worden concrete maatregelen vastgesteld om de actie op EU-niveau op te voeren, zoals de omvorming van het Europees Waarnemingscentrum voor drugs en drugsverslaving tot het Drugsagentschap van de Europese Unie. Volgens het herziene mandaat van dat agentschap, dat in januari 2022 werd voorgesteld,[77] zouden de capaciteiten van het agentschap op het gebied van monitoring en dreigingsevaluatie worden versterkt, evenals het vermogen van het agentschap om op nieuwe uitdagingen te reageren. De Raad heeft in juni 2022 een algemene aanpak vastgesteld en de werkzaamheden in het Europees Parlement lopen nog. De Commissie heeft ook samenwerking in het EU-internetforum opgezet om drugshandel op internet aan te pakken en een specifieke thematische Schengenevaluatie inzake de smokkel van cocaïne via EU-havens voorgesteld. De steun voor het Maritiem Analyse- en Operatiecentrum op het gebied van verdovende middelen werd opgetrokken. De EU zet daarnaast haar politieke dialogen met derde landen over drugs voort: in juni 2022 werd een nieuwe dialoog met Colombia opgestart en in juli 2022 vond een tweede dialoog met China plaats.

---

72 20 countries spin a web to catch human traffickers during a hackathon
73 COM(2020) 609.
74 COM(2021) 591.
75 Jaarverslag van Eurojust over 2021.
76 COM(2020) 606.
77 COM(2022) 18.

Volgens Europol ontsnapt nagenoeg 99 % van de criminele winsten aan **confiscatie** in de EU en blijven ze dus in de handen van de delinquenten[78]. De Commissie heeft in juli 2021 voorstellen gedaan ter versterking van de bestrijding van witwassen en de financiering van terrorisme waarmee momenteel vorderingen worden gemaakt in de behandeling door de Raad[79]. In mei 2022 heeft de Commissie voorgesteld de EU-regels betreffende de ontneming en confiscatie van vermogensbestanddelen te versterken en te moderniseren[80]. Het voorstel werd besproken in werkgroepen van de Raad waarbij op verschillende gebieden vooruitgang wordt geboekt.

Het **Europees Openbaar Ministerie** heeft nu zijn eerste volledige jaar werkzaamheden in verband met de bescherming van de financiële belangen van de EU afgerond. Het heeft 4 006 meldingen van misdaden ontvangen, 929 onderzoeken geopend en bevriezingsbeslissingen voor een totale waarde van 259 miljoen EUR afgegeven. De schade die de tijdens de eerste zeven maanden van zijn activiteit onderzochte zaken aan de Uniebegroting hadden kunnen toebrengen bedroeg naar schatting 5,4 miljard EUR[81].

De Commissie is momenteel ook bezig met de voorbereiding van de **EU-toolbox tegen namaakpraktijken**, zoals werd aangekondigd in het actieplan inzake intellectuele eigendom,[82] en werd benadrukt in de strategie voor de aanpak van de georganiseerde criminaliteit.

Corruptie is niet alleen schadelijk voor het vertrouwen tussen burger en overheid, maar vormt ook een bedreiging voor de veiligheid. Het is een belangrijk instrument voor de georganiseerde misdaad en vergemakkelijkt een breed scala aan criminele activiteiten. Het is een kernthema in het jaarlijkse verslag over de rechtsstaat[83]. Hoewel sommige lidstaten van de EU wereldwijd nog steeds behoren tot de landen die de beste prestaties leveren als het gaat om de bestrijding van corruptie, blijven er nog altijd uitdagingen bestaan, met name in verband met strafrechtelijke onderzoeken en vervolgingen en de toepassing van sancties voor corruptie. Veel lidstaten werken aan maatregelen ter versterking van de kaders voor corruptiepreventie en integriteit, waarbij de middelen die aan corruptiebestrijding worden toegewezen vaak tekortschieten. De Commissie werkt aan een corruptiebestrijdingspakket voor 2023 waarmee de wetgeving op dit gebied zal worden geactualiseerd en gestroomlijnd.

Het EU-actieplan 2020-2025 inzake **illegale vuurwapenhandel**[84] werd in juli 2020 vastgesteld, samen met de strategie voor de veiligheidsunie. Het werd in oktober 2022 gevolgd door een voorstel tot herziening van de regels voor de invoer, uitvoer en doorvoer van vuurwapens[85], met grotere aandacht voor digitalisering. Dit zou alles bij elkaar genomen

---

78 Europol, *Does crime still pay? Criminal Asset Recovery in the EU — Survey of statistical information 2010-2014, 2016*.

79 COM(2021) 421, COM(2021) 420, COM(2021) 423, COM(2021) 422. In juni 2022 is politieke overeenstemming bereikt over de verordening betreffende overmakingen van geld en in juni 2022 werd ook een gedeeltelijke algemene aanpak bereikt inzake de verordening tot oprichting van de Autoriteit voor de bestrijding van witwassen en terrorismefinanciering (met uitzondering van de bepalingen inzake middelen en zetel).

80 COM(2022) 245 final.

81 Eerste jaarverslag van het EOM, 2022.

82 COM(2020) 760.

83 De recentste editie van het verslag werd op 13 juli 2022 vastgesteld (COM (2022) 500).

84 COM(2020) 608 final.

85 COM(2022) 480.

de traceerbaarheid van civiele vuurwapens moeten verbeteren. Daarnaast wordt er ook gewerkt aan betere ondersteuning voor Oekraïne en Moldavië op het gebied van handvuurwapens en lichte wapens in het kader van de Russische agressie tegen Oekraïne.

De illegale verhandeling van cultuurobjecten is een lucratieve handel voor misdaadorganisaties, en in sommige gevallen voor conflictpartijen en terroristen[86]. Die handel vormt dan ook een stimulans voor de georganiseerde misdaad en heeft daarnaast schadelijke gevolgen voor het cultureel erfgoed. Misdadigers kunnen zelfs legaal aangekochte cultuurobjecten misbruiken voor witwassen, het ontduiken van sancties, belastingfraude of de financiering van terrorisme. Om de **bestrijding van de illegale handel in cultuurobjecten** te versterken, is de Commissie momenteel een actieplan aan het vaststellen[87].

Volgens Interpol en het Milieuprogramma van de Verenigde Naties is **milieucriminaliteit** de op drie na grootste criminele activiteit ter wereld, na drugshandel, mensenhandel en namaakpraktijken. Onderhandelingen betreffende ambitieuze voorstellen van de Commissie voor een nieuwe richtlijn milieucriminaliteit[88], een nieuwe verordening overbrenging van afvalstoffen[89] en een nieuwe verordening inzake ontbossing[90] zijn momenteel gaande. Zodra deze voorstellen zijn vastgesteld, zullen ze de handhavingsketen versterken en voorzien in strengere straffen en passende onderzoeksinstrumenten. Zij worden tevens aangevuld met een herzien actieplan tegen de illegale handel in wilde dieren en planten[91].

Voorbeelden van belangrijke resultaten

Encrochat: met de steun van Europol en Eurojust werkten justitie en rechtshandhavingsautoriteiten in België, Frankrijk en Nederland samen aan het blokkeren van het gebruik van versleutelde communicatie door grootschalige misdaadorganisaties. Op het ogenblik dat de dienst werd gesloten, had deze 60 000 abonnees, van wie naar schatting 90 % criminelen.

EU-samenwerking tussen justitie en politie leidde tot de ontmanteling van een grootschalige misdaadorganisatie ("operatie Pollino"): een gemeenschappelijk onderzoeksteam dat in 2016 werd opgericht door Italië, Duitsland en Nederland organiseerde een actiedag, gecoördineerd door Eurojust en ondersteund door Europol, die ertoe heeft geleid dat 34 personen werden veroordeeld tot in totaal meer dan 400 jaar gevangenis. Achteraf werden nog twaalf personen veroordeeld tot een gevangenisstraf van samen meer dan 173 jaar. In verschillende lidstaten lopen de procedures nog.

5. DE VEILIGHEID VAN ONZE GRENZEN WAARBORGEN EN SAMENWERKING TUSSEN RECHTSHANDHAVINGINSTANTIES EN JUSTITIE ONDERSTEUNEN

Een goed functionerend **Schengengebied** levert niet alleen economische en sociale voordelen op, maar is ook van cruciaal belang voor de veiligheid van de EU. Daarvoor is een doeltreffend beheer van de buitengrenzen van de EU noodzakelijk, in combinatie met versterkte samenwerking van de rechtshandhavingsinstanties. In juni 2021 heeft de

[86] Zie bijvoorbeeld de resoluties 2199 (2015), 2253 (2015), 2322 (2016), 2347 (2017), 2462 (2019) en 2617 (2021) van de VN-Veiligheidsraad; de Verklaring van Rome van de ministers van Cultuur van de G20 van 30 juli 2021.
[87] COM(2022) 800.
[88] COM(2021) 851.
[89] COM(2021) 709.
[90] COM(2021) 706.
[91] COM(2022) 581.

Commissie een strategie vastgesteld voor een volledig functionerend en veerkrachtig Schengengebied[92], waarin wordt uiteengezet hoe maatregelen op het gebied van veiligheid, politiële en justitiële samenwerking ervoor kunnen zorgen dat de EU sterk blijft staan tegen bedreigingen voor de veiligheid, zelfs zonder controles aan de binnengrenzen. De strategie wordt nu verder behandeld met behulp van een jaarlijkse Schengencyclus — een nieuw governancemodel voor het Schengengebied — waarbij de vorderingen worden besproken in het eerste verslag over de staat van Schengen dat in mei 2022 werd vastgesteld[93]. Een cruciale stap is een gewijzigde Schengengrenscode,[94] via het voorstel van de Commissie van december 2021, waarin nieuwe bepalingen zijn opgenomen ter ondersteuning van een doeltreffende samenwerking inzake veiligheid en stappen worden beschreven die nodig zijn voor een doeltreffender beheer van de buitengrenzen in crisissituaties. De Raad heeft in juni 2022 een algemene aanpak vastgesteld. Het is belangrijk dat het Europees Parlement en de Raad de onderhandelingen nu snel afronden. De Commissie heeft ook nadrukkelijk gewezen op de voordelen die ontstaan wanneer Bulgarije, Roemenië en Kroatië worden betrokken bij alle aspecten van Schengen, omdat daardoor de veiligheid en het wederzijdse vertrouwen in het Schengengebied worden versterkt[95]. In december 2022 heeft de Raad een besluit vastgesteld inzake de volledige toepassing van het Schengenacquis in Kroatië[96].

In een ruimte zonder controles aan de binnengrenzen zouden politiefunctionarissen in de ene lidstaat toegang moeten hebben tot dezelfde informatie als die waarover hun collega's in een andere lidstaat beschikken. Volledige en doeltreffende samenwerking moet de norm zijn. Daarom is een versterking van de instrumenten voor **informatie-uitwisseling en grensoverschrijdende samenwerking** waarover rechtshandhavingsinstanties en justitiële autoriteiten in de hele EU beschikken van cruciaal belang. Met het pakket betreffende politiële samenwerking van december 2021[97] wordt een belangrijke verbetering van de beschikbare instrumenten geboden. Over de **richtlijn informatie-uitwisseling** is nu tussen het Europees Parlement en de Raad een politiek akkoord bereikt, en in juni 2022 heeft de Raad een aanbeveling tot versterking van de werking van grensoverschrijdende politiële samenwerking vastgesteld. De onderhandelingen betreffende een verordening tot herziening van het Prümkader[98] worden voortgezet, met het oog op efficiëntere geautomatiseerde gegevensuitwisseling tussen rechtshandhavingsinstanties op specifieke gebieden zoals DNA-profielen, dactyloscopische gegevens en voertuigregistratiegegevens, en met toevoeging van de categorieën politiedossiers en gezichtsopnamen. Een snel akkoord over de **Prüm II-verordening** zou de rechtshandhavingsinstanties in de lidstaten een volledig scala aan nieuwe instrumenten voor informatie-uitwisseling in handen geven.

Om de grensoverschrijdende criminaliteit doeltreffender te bestrijden, moeten rechtshandhaving en justitie in de lidstaten samenwerken met de steun van EU-agentschappen zoals Europol en Eurojust. Het nieuwe mandaat van **Europol** is in juni 2022 in werking getreden en geeft Europol de toelating zijn deskundigheid en operationele vermogens op te voeren om de lidstaten beter te ondersteunen bij de bestrijding van zware en georganiseerde

[92] COM(2021) 277.
[93] COM(2022) 301.
[94] COM(2021) 891.
[95] COM(2022) 636.
[96] Vanaf 1 januari 2023 worden controles op personen aan de land- en zeebinnengrenzen tussen Kroatië en de andere landen in het Schengengebied opgeheven. Controles aan de luchtbinnengrenzen worden opgeheven vanaf 26 maart 2023.
[97] COM(2021) 782, COM (2021) 780.
[98] COM (2021) 784.

misdaad en terrorisme. Het mandaat versterkt tevens het gegevensbeschermingskader van Europol en het toezicht van de Europese Toezichthouder voor gegevensbescherming. Onderzoeksinstanties en rechtbanken van verschillende lidstaten moeten samenwerken en elkaar ondersteunen bij het onderzoeken en vervolgen van strafbare feiten, en moeten informatie en bewijsmateriaal veilig en snel kunnen uitwisselen. Het **pakket Digitale justitie**[99] dat in december 2021 werd vastgesteld, bestond uit praktische stappen om de digitale informatie-uitwisseling over grensoverschrijdende terrorismezaken te verbeteren, een samenwerkingsplatform op te zetten ter ondersteuning van de werking van gemeenschappelijke onderzoeksteams en de digitalisering van grensoverschrijdende justitiële samenwerking en de toegang tot de rechter in burgerlijke, handels- en strafzaken te verbeteren. Een snelle goedkeuring van dit pakket door het Europees Parlement en de Raad zou de informatie-uitwisseling tussen justitiële autoriteiten enorm vergemakkelijken.

Digitaal bewijsmateriaal maakt deel uit van bijna elk onderzoek. Het voorlopige politieke akkoord inzake **digitaal bewijsmateriaal**[100] dat in november 2022 werd bereikt, zal de veilige uitwisseling van bewijsmateriaal van cruciale waarde mogelijk maken voor de justitiële autoriteiten in de lidstaten zodat zij de misdaad doeltreffender kunnen bestrijden.

De **beveiliging van de buitengrenzen van de EU** is een gemeenschappelijke verantwoordelijkheid. De eerste teams van het permanent korps van de Europese grens- en kustwacht worden sinds januari 2021 met succes ingezet en het permanent korps telt nu ongeveer 4 800 Frontex- en nationale functionarissen.

Dit jaar namen de irreguliere aankomsten via de meeste migratieroutes toe, wat erop wijst dat het belangrijk is bij alle migranten die aan de buitengrenzen van de EU aankomen systematische identiteits- en veiligheidscontroles uit te voeren, evenals gezondheidscontroles die voldoen aan gemeenschappelijke normen. Veiligheid is een belangrijk onderwerp in het nieuwe migratie- en asielpact. De snelle kanalisering van migranten naar de juiste procedures in het kader van het **screeningvoorstel** zou bijdragen tot de toepassing van veiligheidscontroles, met volledige eerbiediging van alle verplichtingen inzake de grondrechten. Het is nog steeds wachten op een standpunt van het Europees Parlement in verband met dit voorstel.

De **instrumentalisering van migranten** voor politieke doeleinden door het regime van Belarus in de tweede helft van 2021 heeft nooit geziene wettelijke, operationele en menselijke uitdagingen met zich meegebracht, ook op het gebied van veiligheid. In het voorstel voor een Schengengrenscode wordt de kwestie van de instrumentalisering van migranten door derde landen voor politieke doeleinden eveneens behandeld. Lidstaten die met deze situatie worden geconfronteerd, zouden bijvoorbeeld het aantal grensovergangen kunnen beperken en de grensbewaking opvoeren.

Momenteel wordt er gewerkt aan een nieuwe architectuur van de **informatiesystemen** van de EU om betere ondersteuning te geven aan de werkzaamheden van de nationale autoriteiten die moeten zorgen voor de veiligheid en het grens- en migratiebeheer. Centraal hierin staat het hernieuwde Schengeninformatiesysteem, dat in maart 2023 operationeel moet zijn. Andere belangrijke instrumenten zijn het inreis-/uitreissysteem (werkzaamheden beginnen volgens planning in mei 2023), het Europees reisinformatie- en -autorisatiesysteem Etias (dat eind 2023 operationeel moet zijn) en de actualisering van het visuminformatiesysteem (VIS).

[99] COM (2021) 756, COM (2021) 757, COM (2021) 759.
[100] COM (2018) 225, COM (2018) 226.

Dankzij deze instrumenten zullen meer controles mogelijk zijn en worden de lacunes in de veiligheidsinformatie gedicht door betere informatie-uitwisseling tussen de lidstaten. Voor deze werkzaamheden is de interoperabiliteit van de systemen van cruciaal belang: eu-LISA en de lidstaten moeten zonder uitstel de nodige stappen zetten zodat dit ambitieuze project tegen eind 2024 volledig kan zijn uitgevoerd.

Controles op binnenkomende goederen moeten doeltreffend zijn om de risico's voor de EU en haar burgers te beperken en tegelijkertijd de concurrentiekracht van legitieme bedrijven in de EU te waarborgen. Veiligheidscontroles op deze goederen werden verbeterd aan de hand van een opgewaardeerd controlesysteem bij invoer in de EU[101] om doeltreffende, risicogebaseerde douanecontroles en maatregelen voor de bescherming van luchtvracht tegen terroristische dreigingen te ondersteunen. Met het Instrument voor financiële steun voor douanecontroleapparatuur[102] wordt ook financiering verstrekt voor het op transparante wijze aankopen, onderhouden en moderniseren van relevante, geavanceerde en betrouwbare douanecontroleapparatuur.

Op voorhand af te geven passagiersgegevens (API-gegevens) kunnen bijdragen aan de veiligheid, maar dat wordt belemmerd door voorschriften die achterhaald zijn en in ongelijke mate worden toegepast. Met de nieuwe voorstellen van de Commissie zou de huidige richtlijn inzake API-gegevens worden ingetrokken en zou het gebruik van API-gegevens voor zowel grensbeheer als rechtshandhaving worden bevorderd[103]. Het gebruik van API-gegevens zou worden uitgebreid naar bepaalde vluchten binnen de EU en een uitbreiding vormen van het instrumentarium dat beschikbaar is voor de rechtshandhavingsinstanties van de lidstaten binnen het Schengengebied. De externe dimensie van het EU-beleid inzake **persoonsgegevens van passagiers** (PNR-gegevens) wordt nog bekeken in het licht van het feit dat steeds meer derde landen de capaciteit ontwikkelen om deze gegevens te verwerken voor rechtshandhavings- en grensbeveiligingsdoeleinden. De Commissie werkt ook aan een wetgevingsvoorstel betreffende een kader voor het verlenen van wederzijdse toegang tot veiligheidsgerelateerde informatie voor eerstelijnsfunctionarissen in de EU en partnerlanden om criminelen en terroristen doeltreffend op te sporen.

Fraude met reisdocumenten vergemakkelijkt het illegale verkeer van criminelen en terroristen en speelt een sleutelrol bij mensenhandel en drugshandel. De aanpak van die fraude mag de noodzaak om legitieme reizigers vlotter te laten reizen echter niet in de weg staan. Sinds augustus 2021 zijn de lidstaten daarom begonnen met de afgifte van identiteitskaarten die aan geharmoniseerde beveiligingsnormen voldoen en een chip bevatten met biometrische kenmerken die door alle grensautoriteiten van de EU kan worden geverifieerd[104]. De Commissie bereidt momenteel nog een initiatief voor betreffende de digitalisering van reisdocumenten en de vergemakkelijking van reizen[105]. Dat initiatief zal de

[101] Het ICS2 (invoercontrolesysteem 2) zal operationeel zijn in drie releases (maart 2021, maart 2022 en maart 2023). Elke release heeft betrekking op andere marktdeelnemers en vervoerswijzen.

[102] Verordening (EU) 2021/1077 van 24 juni 2021 tot oprichting, in het kader van het Fonds voor geïntegreerd grensbeheer, van het Instrument voor financiële steun voor douanecontroleapparatuur.

[103] COM(2022) 729 en 731.

[104] Op basis van Verordening (EU) 2019/1157 van het Europees Parlement en de Raad van 20 juni 2019 betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten afgegeven aan burgers van de Unie en hun familieleden die hun recht van vrij verkeer uitoefenen (PB L 188 van 12.7.2019, blz. 67).

[105] Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordeningen (EG) nr. 767/2008, (EG) nr. 810/2009 en (EU) 2017/2226 van het Europees Parlement en de Raad, Verordeningen (EG) nr. 1683/95, (EG) nr. 333/2002, (EG) nr. 693/2003 en (EG) nr. 694/2003 van de Raad en de

beveiliging verhogen en reis- en grensprocedures versnellen dankzij geavanceerde papierloze communicatie van reis- en persoonsgegevens en biometrische controles aan de grenzen.

Rechtshandhaving en nieuwe technologieën

Technologieën zoals **artificiële intelligentie** of versleuteling kunnen toegevoegde waarde bieden voor rechtshandhavingsinstanties en justitiële autoriteiten, maar kunnen ook hun werk bemoeilijken. In haar mededeling betreffende artificiële intelligentie (AI) en in de verordening artificiële intelligentie[106] onderstreepte de Commissie dat AI aanzienlijk kan bijdragen aan de doelstellingen van de strategie voor de veiligheidsunie door actuele dreigingen tegen te gaan en te anticiperen op toekomstige risico's en kansen[107]. In het kader van Horizon Europa, het onderzoeks- en innovatieprogramma van de EU voor de periode 2021-2027, is er financiering beschikbaar voor **civiel beveiligingsonderzoek** en -innovatie, onder meer inzake AI of biometrie. Alleen al voor 2021 en 2022 werd reeds 413,8 miljoen EUR geprogrammeerd[108].

Voorbeeld van belangrijke resultaten

Gebruik van het Schengeninformatiesysteem (SIS): de lidstaten voerden in 2021 nagenoeg 7 miljard zoekopdrachten uit in het SIS. De autoriteiten van de lidstaten voerden dagelijks gemiddeld nagenoeg 20 miljoen zoekopdrachten uit in het systeem, die gemiddeld resulteerden in 600 treffers op buitenlandse signaleringen, hetgeen bijdroeg tot het oplossen van een even groot aantal zaken. Na een brutale dubbele moord in Roemenië in 2021 bijvoorbeeld, werd de dader slechts enkele dagen later opgespoord in Italië, dankzij een SIS-signalering met het oog op de aanhouding van de betrokkene, waardoor Italiaanse onderzoekers werden ingeseind, die de man daarna konden aanhouden in Rome.

6. DE NEXUS INTERNE-EXTERNE VEILIGHEID: VEILIGHEID IN HET NABUURSCHAP VAN DE EU EN IN DE PARTNERLANDEN

Gebeurtenissen buiten de grenzen van de EU en de veiligheid in Europa zijn nauw met elkaar verweven. Wij kunnen de interne veiligheid van de EU alleen maar verbeteren als wij onze buren en partners steunen en helpen bij de verbetering van hun eigen interne veiligheid en als wij samenwerken met onze bondgenoten en met internationale organisaties zoals de NAVO en de VN.

De Europese Dienst voor extern optreden (EDEO) en de diensten van de Commissie werken nauw samen met belangrijke partnerlanden en internationale organisaties, via regelmatige **dialogen over terrorismebestrijding**. Er lopen momenteel meer dan dertig dialogen over terrorismebestrijding met derde landen en internationale organisaties[109]. Parallel daarmee

Overeenkomst ter uitvoering van het Akkoord van Schengen wat betreft de digitalisering van de visumprocedure (COM(2022) 658 final).

[106] COM(2021) 206.

[107] COM(2021) 205.

[108] In het kader van Horizon Europa worden ook substantiële middelen geïnvesteerd in innovatieve technologieën die rechtshandhavingsinstanties kunnen benutten in de strijd tegen radicalisering, evenals projecten voor het opsporen van drugs en explosieven, de illegale handel in cultuurgoederen, migrantensmokkel, de beveiliging van openbare ruimten en identiteitsdiefstal.

[109] In 2022 vonden dialogen over terrorismebestrijding plaats met de VN, Israël en India; dialogen met Turkije, Qatar en de Verenigde Arabische Emiraten (VAR) gaan binnenkort van start. In 2023 zullen naar verwachting belangrijke dialogen plaatsvinden met Marokko, Tunesië, Egypte, Kenia, de VS, Saudi-Arabië en mogelijk ook met Algerije.

werd het deskundigennetwerk inzake terrorisme en veiligheid in de EU-delegaties in belangrijke derde landen versterkt.

Om interneveiligheidsdreigingen als gevolg van de aanvalsoorlog van Rusland tegen Oekraïne beter het hoofd te kunnen bieden, hebben de diensten van de Commissie en de EDEO, met de EU-coördinator voor terrorismebestrijding, een overeenkomst gesloten met **Oekraïne** om een onafgebroken, gestructureerde samenwerking op het gebied van veiligheid tot stand te brengen. Deze samenwerking heeft tot doel de operationele samenwerking, ook die met Europol en Frontex, te verbeteren en de informatie-uitwisseling over dreigingen voor de interne veiligheid te versterken. EU-agentschappen hebben onmiddellijk steun verleend om te reageren op de uitdagingen die zich na de invasie stelden. Momenteel hebben Frontex 277, Europol 15 en het Asielagentschap van de Europese Unie 60 medewerkers ingezet in de regio.

De rechtshandhavingsinstanties van de lidstaten en hun partners werken in het kader van het **Europees multidisciplinair platform tegen criminaliteitsdreiging (Empact)** samen aan de organisatie van operationele acties en gezamenlijke actiedagen tegen nieuwe of evoluerende criminaliteitsdreigingen die gekoppeld zijn aan de agressie van Rusland tegen Oekraïne.

De dialoog over cyberbeveiliging tussen de EU en Oekraïne is geïntensiveerd met gecoördineerde politieke, financiële en materiële steun van de EU om Oekraïne te helpen bij de versterking van zijn cyberweerbaarheid. Dankzij financiering voor een bedrag van in totaal 29 miljoen EUR kon Oekraïne zijn digitale en cyberweerbaarheid opvoeren met steun voor cyberbeveiligingsuitrusting en -software en een weerbare digitale transformatie.

Door zijn geografische ligging speelt **Moldavië** een belangrijke rol in de aanpak van de criminaliteits- en veiligheidseffecten van de Russische invasie van Oekraïne. In juli 2022 heeft de Commissie, in samenwerking met de EDEO, een EU-ondersteuningscentrum voor interne veiligheid en grensbeheer opgestart met Moldavië. De rol van dit centrum behelst voornamelijk de facilitering van samenwerking en operationele actie om het hoofd te bieden aan gedeelde veiligheidsdreigingen op zes prioriteitsgebieden die door de EU en Moldavië samen zijn aangewezen: illegale vuurwapenhandel, migrantensmokkel, mensenhandel, de preventie en bestrijding van terrorisme en gewelddadig extremisme, cybercriminaliteit en drugshandel. In maart 2022 heeft Moldavië een statusovereenkomst gesloten met Frontex, op grond van het versterkte mandaat van deze laatste.

De samenwerking tussen de rechtshandhavingsinstanties van de EU en de **landen van de Westelijke Balkan** — ook met de hulp van EU-agentschappen — is de voorbije drie jaar voortdurend intensiever geworden. Overeenkomstig de conclusies van de Raad in maart 2021 is de samenwerking met derde landen op het gebied van rechtshandhaving geïntegreerd in alle operationele actieplannen van het Europees multidisciplinair platform tegen criminaliteitsdreiging (Empact), waardoor de deelname van de Westelijke Balkan aan activiteiten van Empact een nieuwe impuls heeft gekregen. In het kader van het instrument voor pretoetredingssteun wordt nog steeds aanzienlijke financiering verstrekt voor de hervorming en prestaties van rechtshandhavingsinstanties, waarbij de EU-agentschappen tevens capaciteitsopbouw verstrekken aan veiligheidsactoren. Met het in 2018 ondertekende gezamenlijke actieplan inzake terrorismebestrijding worden goede vorderingen gemaakt, en in het geval van Noord-Macedonië en Albanië, waar de meeste acties voltooid zijn, werd in december 2022 een herziene en geactualiseerde versie van de respectieve bilaterale

overeenkomsten ondertekend om onze samenwerking op het gebied van terrorismebestrijding en het voorkomen en bestrijden van gewelddadig extremisme verder aan te scherpen.

Op 18 november 2022 heeft de Raad toestemming gegeven voor het openen van onderhandelingen betreffende **statusovereenkomsten met Frontex** tussen de EU en Albanië, Servië, Montenegro en Bosnië en Herzegovina[110]. Deze overeenkomsten zouden Frontex in staat stellen grensbeheerteams in te zetten voor het uitvoeren van grenscontroletaken, onder het commando van de relevante nationale autoriteiten. Dit zal van bijzonder belang zijn voor de bestrijding van migrantensmokkel. Noord-Macedonië heeft in oktober 2022 een statusovereenkomst met Frontex gesloten, op grond van het versterkte mandaat van deze laatste.

De **EU en de VS** hebben ook een lange geschiedenis van partnerschap en samenwerking inzake veiligheidsaangelegenheden, waarbij zij streven naar een meer systematische en tijdige uitwisseling van informatie over kwesties zoals terrorisme, radicalisering en georganiseerde misdaad. De EU en de VS houden regelmatig gezamenlijke bijeenkomsten op het gebied van justitie en binnenlandse zaken om de samenwerking inzake aangelegenheden van gemeenschappelijk belang te verdiepen, de mondiale veiligheid te bevorderen en elkaar op de hoogte te brengen van de vorderingen betreffende wetgeving inzake de bijbehorende dossiers. De Europese justitiële en rechtshandhavingsagentschappen en hun Amerikaanse tegenhangers werken nauw samen aan operationele en wetgevingsaangelegenheden. Rechtshandhavingsinstanties van de VS nemen actief deel aan verschillende Empact-acties en -netwerken, in het kader van een overeenkomst voor operationele samenwerking tussen de VS en Europol. Een krachtig voorbeeld van doeltreffende samenwerking is de operationele taskforce Greenlight/Trojan Shield, een van de tot dusver omvangrijkste en meest geavanceerde rechtshandhavingsoperaties gericht op de bestrijding van versleutelde criminele activiteiten. Het programma voor het traceren van terrorismefinanciering tussen de EU en de VS levert tal van concrete aanknopingspunten op voor onderzoek naar terroristen[111]. De samenwerking berust ook op een duidelijke monitoring van waarborgen en controles.

Dankzij regelmatige dialogen tussen de EU en de VS over cyberbeveiliging worden de samenwerking en coördinatie inzake cyberdiplomatie en cyberweerbaarheid, met inbegrip van de normalisatie van cyberbeveiliging, versterkt. De samenwerking is bovendien verdiept dankzij de Handels- en Technologieraad (TTC), met een gezamenlijke verklaring over cyberbeveiliging en stappen voor mogelijke samenwerking inzake onderzoek en ontwikkeling na 5G en 6G, inzake exportcontroles, de screening van investeringen en sancties tegen Rusland en Belarus. De TTC zal ook de samenwerking tussen de EU en de VS op het gebied van buitenlandse desinformatie en inmenging verder bevorderen.

Belangrijke uitdagingen op het gebied van beveiliging in **Afrika** zijn rechtstreeks van invloed op de Afrikanen zelf, maar bedreigen ook de veiligheid van de EU. Tal van projecten worden uitgevoerd om partnerlanden te helpen bij de opbouw van capaciteit om deze uitdagingen het hoofd te bieden, bijvoorbeeld via de financiering van de internationale academie voor terrorismebestrijding in West-Afrika of met het regionale initiatief ter verbetering van capaciteit voor de bestrijding van witwassen en de financiering van terrorisme in de regio van de Grote Hoorn.

[110] Besluit (EU) 2022/2271 van de Raad — Albanië; Besluit (EU) 2022/2272 van de Raad — Bosnië en Herzegovina; Besluit (EU) 2022/2273 van de Raad — Montenegro; Besluit (EU) 2022/2274 van de Raad — Servië.

[111] Zie de zesde gezamenlijke evaluatie van de uitvoering van de TFTP-overeenkomst, COM(2022) 585.

De landen van **Latijns-Amerika en het Caribisch gebied** (LAC) zijn essentiële partners voor de EU, en in mei 2022 werd een nieuw regionaal initiatief voor veiligheid en recht van Team Europa opgestart met als doel het opzetten van een partnerschap tussen de EU en de LAC inzake de versterking van de rechtsstaat en het opvoeren van de strijd tegen de georganiseerde misdaad.

De verordening tot vaststelling van een kader voor de **screening van buitenlandse directe investeringen** in de Unie trad in oktober 2020 in werking[112] en biedt een kader voor betere bescherming tegen buitenlandse directe investeringen die een risico vormen voor de veiligheid of openbare orde in meer dan een lidstaat. Tijdens het volledige eerste werkingsjaar van de verordening werden bij de Commissie meer dan 400 zaken aangemeld. Met de verordening inzake producten voor tweeërlei gebruik[113] die in september 2021 werd vastgesteld, werd het **controlesysteem voor de uitvoer van producten voor tweeërlei gebruik** aangescherpt en versterkt. Er werden nieuwe bepalingen ingevoerd die de EU toestaan om — in coördinatie met de lidstaten — autonome controles op de uitvoer van niet in de lijst opgenomen producten en technologieën vast te stellen.

In een geglobaliseerde wereld, waar zware criminaliteit en terrorisme steeds transnationaler worden, moeten de rechtshandhavings- en justitiële autoriteiten over alle middelen kunnen beschikken om in samenwerking met externe partners de veiligheid van hun burgers te garanderen. Daartoe moeten de justitiële autoriteiten van derde landen kunnen samenwerken en informatie kunnen uitwisselen met **Europol en Eurojust**. In juni 2022 werd tussen Europol en Nieuw-Zeeland een akkoord gesloten over de uitwisseling van persoonsgegevens bij de bestrijding van zware criminaliteit en terrorisme[114]. Dit zal worden gevolgd door onderhandelingen met een aantal andere landen, maar in de meeste gevallen worden er slechts langzaam vorderingen gemaakt. Wat Eurojust betreft, zijn de onderhandelingen met Armenië goed gevorderd aangezien er een akkoord is bereikt over de tekst, en zijn er onderhandelingen met Colombia, Algerije en Libanon van start gegaan.

In april 2022 hebben de **EU en de VN** tijdens de vierde Leidersdialoog over terrorismebestrijding concrete stappen gezet naar de versterking van hun bestaande partnerschap voor de bestrijding van hardnekkige maar zich ontwikkelende dreigingen voor de internationale vrede en veiligheid. Het strategische partnerschap werd verder versterkt door de lancering van de nieuwe "EU-UN Global Terrorism Threats Facility", een door de EU gefinancierd initiatief ter ondersteuning van staten die worden geconfronteerd met terrorisme en gewelddadig extremisme. De ondersteuning behelst onder meer bijstand, opleiding en begeleiding. Andere aangelegenheden van gemeenschappelijke zorg zijn onder meer opkomende dreigingen in verband met nieuwe technologieën en de manier waarop zij van invloed zijn op jongeren die een specifieke doelgroep zijn voor radicalisering die zich uit in geweld, en terrorisme op grond van vreemdelingenhaat, racisme en andere vormen van onverdraagzaamheid, of in naam van een godsdienst of overtuiging.

[112] Verordening (EU) 2019/452.

[113] Verordening (EU) 2021/821 (herschikking).

[114] De Europese Toezichthouder voor gegevensbescherming (EDPS) beschreef het akkoord in positieve bewoordingen als een model voor toekomstige akkoorden inzake de uitwisseling van persoonsgegevens voor rechtshandhavingsdoeleinden.

Ook de samenwerking tussen de **EU en de NAVO** werd geïntensiveerd, met tastbare resultaten op alle samenwerkingsgebieden[115]. De EU en de NAVO hebben hun werkzaamheden en samenwerking opgevoerd in het licht van de aanvalsoorlog van Rusland, met een eensgezinde beleidskoers en coördinatie om Oekraïne te helpen zichzelf te verdedigen en zijn bevolking te beschermen. Het strategische partnerschap tussen de EU en de NAVO is krachtiger en relevanter dan ooit op dit cruciale moment voor de Euro-Atlantische veiligheid. In januari 2022 werd een specifieke gestructureerde dialoog over weerbaarheid opgestart, die momenteel wordt verdiept om de bescherming van kritieke infrastructuur te ondersteunen. In dat verband zal een EU-NAVO-taskforce worden opgezet. Op het gebied van militaire mobiliteit zijn verdere verbeteringen doorgevoerd in verband met vervoers- en regelgevingsaspecten, met inbegrip van het vervoer van gevaarlijke goederen. Ook het tegengaan van hybride dreigingen blijft een belangrijk gebied van samenwerking met de NAVO. Uitwisselingen betreffen terrorismebestrijding, evenals strategische communicatie, buitenlandse desinformatie en inmenging en cyberkwesties. Oefeningen omvatten de EU Integrated Resolve in november 2022 in het kader van het PACE-concept (PACE staat voor parallelle en gecoördineerde oefeningen), met betrokkenheid van NAVO-medewerkers, om de interactie tussen de respectieve crisisresponsmechanismen te verbeteren.

Sinds september 2022 is de EU medevoorzitter van het **Global Counter Terrorism Forum**. Prioriteiten zijn onder meer de aanpak van de terroristische dreiging in Afrika en de integratie van gender en onderwijs in het terrorismebestrijdingsbeleid.

Onderhandelingen over een samenwerkingsakkoord tussen de Unie en **Interpol** zijn aan de gang en zullen naar verwachting op technisch niveau worden afgesloten in de loop van de eerste helft van 2023. Het hoofddoel is de verdere versterking van de informatie-uitwisseling tussen Interpol en EU-agentschappen en -organen om de lidstaten beter te ondersteunen en de veiligheid van de burgers, niet alleen in de EU maar overal ter wereld, te verbeteren.

Voorbeeld van belangrijke resultaten

Operatie Desert Light — Europees drugskartel opgerold in zes landen: in november 2022 werden in heel Europa en in de Verenigde Arabische Emiraten (VAE) gecoördineerde invallen uitgevoerd gericht op het commando- en controlecentrum en de logistieke infrastructuur voor drugshandel in Europa. Belangrijke doelwitten hadden een "superkartel" gevormd dat ongeveer een derde van de cocaïnehandel in Europa controleerde. In totaal werden 49 verdachten gearresteerd na onderzoeken in Spanje, Frankrijk, België, Nederland en de VAE met de steun van Europol. In de loop van de onderzoeken confisqueerden rechtshandhavingsinstanties dertig ton drugs.

7. CONCLUSIE

De voorbije tweeënhalf jaar heeft de Commissie in nauwe samenwerking met de Europese Dienst voor extern optreden succesvolle resultaten geboekt met betrekking tot nagenoeg alle maatregelen die in de strategie voor de veiligheidsunie worden uiteengezet. Het brede scala aan voorstellen moet worden goedgekeurd en vooral uitgevoerd. De besluiten en acties van het Europees Parlement, de Raad en de afzonderlijke lidstaten zullen van cruciaal belang zijn

[115] Zie het zevende voortgangsverslag inzake de uitvoering van de gemeenschappelijke reeks voorstellen die door de Raad van de EU en de Noord-Atlantische Raad op 6 december 2016 en 5 december 2017 werden bekrachtigd, 20 juni 2022.

om te waarborgen dat de EU erin slaagt een krachtig veiligheidsecosysteem voor haar burgers tot stand te brengen.

Tegelijkertijd zal de ons omringende veiligheidsomgeving blijven veranderen. Sinds de vaststelling van de strategie voor de veiligheidsunie werd de EU geconfronteerd met de COVID-19-pandemie en de gevolgen van de agressie van Rusland tegen Oekraïne. Onlinedreigingen zijn exponentieel toegenomen en snelle aanpassings- en voorzorgsmaatregelen zijn meer dan ooit nodig. De EU moet zich blijven toerusten om het hoofd te kunnen bieden aan alle zich ontwikkelende dreigingen die de veiligheid van haar burgers in gevaar brengen. Voortdurende waakzaamheid, vastberaden optreden en collectieve reacties zullen van cruciaal belang zijn voor het collectieve welslagen van de EU in de toekomst.