EUROPESE
COMMISSIE

Brussel, 24.7.2020
COM(2020) 605 final

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

betreffende de EU-strategie voor de veiligheidsunie

I. Inleiding

De politieke beleidslijnen van de Commissie hebben duidelijk gemaakt dat we alles op alles moeten zetten als het erom gaat onze burgers te beschermen. Veiligheid is niet alleen iets waar we persoonlijk baat bij hebben, maar beschermt ook de grondrechten en biedt de basis voor het vertrouwen in en de dynamiek van onze economie, onze samenleving en onze democratie. Het veiligheidsklimaat is voor de Europeanen vandaag de dag steeds veranderlijk, als gevolg van wisselende dreigingen en andere factoren, zoals klimaatverandering, demografische ontwikkelingen en politieke instabiliteit buiten onze grenzen. De globalisering, het vrije verkeer en de digitale transformatie blijven welvaart brengen, ons leven makkelijker maken en innovatie en groei stimuleren, maar gaan ook gepaard met risico's en kosten. Terrorisme, georganiseerde criminaliteit, drugshandel en mensenhandel vormen rechtstreekse bedreigingen voor de burgers en onze Europese manier van leven. Cyberaanvallen en cybercriminaliteit komen steeds vaker voor. Ook de bedreigingen voor de veiligheid worden complexer: zij nemen toe door het vermogen om grensoverschrijdend te werken en door interconnectiviteit, en maken gebruik van de vervaging van de grenzen tussen de fysieke en de digitale wereld. Zij exploiteren kwetsbare groepen en sociale en economische verschillen. Aanvallen kunnen elk moment plaatsvinden zonder per se veel sporen achter te laten, en zowel statelijke als niet-statelijke actoren kunnen gebruikmaken van allerlei hybride bedreigingen[1]. Wat buiten de EU gebeurt, kan kritieke gevolgen hebben voor de veiligheid binnen de EU.

De COVID-19-crisis heeft er ook toe geleid dat wij onze notie van veiligheidsbedreigingen en de bijbehorende beleidsmaatregelen hebben herzien. De crisis heeft de noodzaak om de veiligheid te waarborgen, zowel in de fysieke als in de digitale omgeving, des te urgenter gemaakt. Gebleken is dat open strategische autonomie voor onze toeleveringsketens in termen van kritische producten, diensten, infrastructuren en technologieën, van groot belang is. Door de crisis is het des te noodzakelijker alle sectoren en alle mensen te betrekken bij een gezamenlijke inspanning om ervoor te zorgen dat de EU in de eerste plaats beter is voorbereid en weerbaarder is en dat zij over betere instrumenten beschikt om waar nodig te reageren.

Burgers kunnen niet worden beschermd door optreden van de afzonderlijke lidstaten alleen. Het is meer dan ooit noodzakelijk om voort te bouwen op onze sterke punten en samen te werken, en de EU is meer dan ooit in de positie om een verschil te maken. Zij kan het goede voorbeeld geven door haar algemene stelsel voor crisisbeheersing te versterken en zowel binnen als buiten haar grenzen te werken aan mondiale stabiliteit. Hoewel de primaire verantwoordelijkheid voor de beveiliging bij de lidstaten ligt, zijn we de laatste jaren steeds meer tot het inzicht gekomen dat de veiligheid van één lidstaat de veiligheid van iedereen is. De EU kan een multidisciplinair, geïntegreerd antwoord bieden en de veiligheidsactoren in de lidstaten helpen met de instrumenten en de informatie die zij nodig hebben[2].

De EU kan er ook voor zorgen dat het veiligheidsbeleid verankerd blijft in onze gemeenschappelijke Europese waarden – inachtneming en handhaving van de rechtsstaat,

---

[1] De definities van wat een hybride bedreiging is, lopen uiteen. Met de term wordt gedoeld op een combinatie van dwingende en ontregelende activiteit en conventionele en onconventionele methoden (op diplomatiek, militair, economisch en technologisch vlak), die op een gecoördineerde manier kunnen worden gebruikt door zowel statelijke als niet-statelijke actoren om specifieke doelstellingen te bereiken, maar waarbij nog geen sprake is van formeel verklaarde oorlogsvoering (zie JOIN(2016) 18 final).

[2] Bijvoorbeeld via de diensten van het ruimtevaartprogramma van de EU, zoals Copernicus, dat aardobservatiegegevens biedt alsmede toepassingen voor grensbewaking, maritieme veiligheid, rechtshandhaving, bestrijding van piraterij, ontmoediging van drugssmokkel en beheer van noodsituaties.

gelijkheid[3] en grondrechten, transparantie, verantwoording en democratische controle – ter versterking van het vertrouwensfundament van het beleid. De EU kan een echte en doeltreffende veiligheidsunie tot stand brengen, waarin de rechten en vrijheden van personen goed worden beschermd. Veiligheid en eerbiediging van de grondrechten zijn doelstellingen die niet met elkaar strijdig zijn, maar onderling samenhangen en elkaar aanvullen. Onze waarden en onze grondrechten moeten aan de basis liggen van het veiligheidsbeleid. De beginselen van noodzakelijkheid, evenredigheid en wettigheid moeten worden gegarandeerd, en verantwoording en gerechtelijk verhaal moeten gewaarborgd zijn. Tegelijkertijd moet een doeltreffende respons mogelijk zijn wat betreft de bescherming van personen, met name de meest kwetsbaren onder hen.

Er zijn al aanzienlijke juridische, praktische en ondersteunende instrumenten opgezet, maar deze moeten worden versterkt en beter worden uitgevoerd. Er is al veel gedaan om de informatie-uitwisseling en de samenwerking op het gebied van inlichtingen met de lidstaten te verbeteren en de armslag van terroristen en criminelen te beperken. Maar er is nog steeds sprake van fragmentatie.

De werkzaamheden moeten zich ook uitstrekken tot buiten de grenzen van de EU. Bij het beschermen van de Unie en haar burgers is het niet langer alleen zaak om de veiligheid binnen de grenzen van de EU te waarborgen, maar ook om de externe dimensie van veiligheid aan te pakken. De EU-aanpak van de externe veiligheid in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid (GBVB) en het gemeenschappelijk veiligheids- en defensiebeleid (GVDB) blijft een essentieel onderdeel van de inspanningen van de EU om de veiligheid in de EU te vergroten. Samenwerking met derde landen en op mondiaal niveau om gemeenschappelijke uitdagingen aan te pakken is van cruciaal belang voor een doeltreffende en alomvattende reactie, en stabiliteit en veiligheid in de buurlanden van de EU zijn van cruciaal belang voor onze eigen veiligheid in de EU.

Deze nieuwe strategie bouwt voort op eerdere werkzaamheden van het Europees Parlement[4], de Raad[5] en de Commissie[6], en laat zien dat voor een echte en doeltreffende veiligheidsunie een sterke kern van instrumenten en beleidsmaatregelen in de praktijk de veiligheid moet waarborgen. Daarbij moet worden erkend dat veiligheid implicaties heeft voor alle geledingen van de samenleving en voor al het overheidsbeleid. De EU moet zorgen voor een veilige omgeving voor iedereen, ongeacht ras of etnische afstamming, godsdienst, levensovertuiging, geslacht, leeftijd of seksuele oriëntatie.

Deze strategie bestrijkt de periode 2020–2025 en is gericht op de opbouw van vermogens en capaciteiten om een toekomstbestendige veiligheidsomgeving te waarborgen. Zij gaat uit van een samenlevingsbrede aanpak van veiligheid, waarmee op gecoördineerde wijze een doeltreffende respons kan worden gegeven op snel veranderende dreigingssituaties. Om de digitale en fysieke risico's in het gehele ecosysteem van de veiligheidsunie op geïntegreerde wijze aan te pakken, worden strategische prioriteiten en de bijbehorende maatregelen worden

---

3 Een Unie van gelijkheid: strategie voor gendergelijkheid 2020–2025 (COM(2020) 152).

4 Bijvoorbeeld de werkzaamheden van de commissie-TERR van het Europees Parlement, die in november 2018 verslag heeft uitgebracht.

5 Van de conclusies van de Raad van juni 2015 over een "vernieuwde interneveiligheidsstrategie" tot de meer recente bevindingen van de Raad van december 2019.

6 Uitvoering van de Europese veiligheidsagenda ter bestrijding van terrorisme en ter voorbereiding van een echte en doeltreffende Veiligheidsunie (COM(2016) 230 final van 20.4.2016). Zie de recente beoordeling van de uitvoering van de wetgeving op het gebied van de interne veiligheid: Tenuitvoerlegging van de wetgeving inzake binnenlandse zaken op het gebied van interne veiligheid 2017–2020 (SWD(2020) 135).

vastgesteld, waarbij de nadruk wordt gelegd op terreinen waar de EU meerwaarde kan bieden. De bedoeling is een veiligheidsdividend tot stand te brengen waarmee iedereen in de EU wordt beschermd.

II. Een snel veranderend Europese landschap van veiligheidsbedreigingen

Voor de veiligheid, de welvaart en het welzijn van de burgers is het essentieel dat zij goed worden beschermd. Bedreigingen van de veiligheid hangen samen met de mate waarin het leven en de bestaansmiddelen van burgers kwetsbaar zijn. Hoe groter de kwetsbaarheid, des te groter is het risico dat die kwetsbaarheid kan worden geëxploiteerd. Zowel kwetsbaarheden als dreigingen zijn voortdurend in ontwikkeling, en de EU moet zich dus aanpassen.

We zijn in ons dagelijks leven afhankelijk van een grote verscheidenheid aan diensten, op gebieden als energie, vervoer, financiën en gezondheidszorg. Deze maken gebruik van zowel fysieke als digitale infrastructuur, wat de kwetsbaarheid en het risico van verstoring nog groter maakt. Tijdens de COVID-19-pandemie konden veel bedrijven en openbare diensten blijven draaien door middel van nieuwe technologieën om werken op afstand mogelijk te maken of de logistiek van de toeleveringsketens in stand te houden. Dit heeft echter ook de deur opengezet voor een enorme toename van kwaadaardige aanvallen, waarbij getracht wordt om voor criminele activiteiten misbruik te maken van de verstoring van de normale patronen waartoe de pandemie en de verschuiving naar digitaal thuiswerken hebben geleid[7]. Tekorten aan goederen hebben geleid tot nieuwe kansen voor de georganiseerde misdaad. Dit had fatale gevolgen kunnen hebben door de verstoring van essentiële gezondheidsdiensten, nu deze onder ongekende druk staan.

Nu digitale technologieën die ons leven ten goede komen, steeds vaker worden toegepast, is ook de **cyberbeveiliging** van technologieën een kwestie van strategisch belang geworden[8]. Huishoudens, banken, financiële diensten en ondernemingen (met name in het midden- en kleinbedrijf) worden zwaar getroffen door cyberaanvallen. De potentiële schade wordt nog verder versterkt door de onderlinge afhankelijkheid van fysieke en digitale systemen: elke fysieke impact zal gevolgen hebben voor de digitale systemen, terwijl cyberaanvallen op informatiesystemen en digitale infrastructuren essentiële diensten stil kunnen leggen[9]. De opkomst van het internet der dingen en het toegenomen gebruik van kunstmatige intelligentie zullen nieuwe voordelen maar ook allerlei nieuwe risico's opleveren.

Onze wereld steunt op digitale infrastructuren, technologieën en onlinesystemen die ons in staat stellen zaken te doen en van producten en diensten gebruik te maken. Bij dat alles zijn we afhankelijk van communicatie en interactie. De afhankelijkheid van onlinesystemen heeft

---

7 Europol: *Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU* (april 2020).

8 Aanbeveling van de Commissie inzake de cyberbeveiliging van 5G-netwerken (C(2019) 2335); Mededeling *Uitrol van beveiligde 5G in de EU – uitvoering van de EU-toolbox* (COM(2020) 50).

9 In maart 2020 werd het universitair ziekenhuis van Brno in Tsjechië getroffen door een cyberaanval, waardoor het patiënten moest doorverwijzen en operaties moest uitstellen (Europol: *Pandemic Profiteering. How criminals exploit the COVID-19 crisis*). Kunstmatige intelligentie kan worden misbruikt voor digitale, politieke en fysieke aanvallen en voor surveillance. Het verzamelen van gegevens in het kader van het internet der dingen kan worden gebruikt voor surveillance van personen (slimme horloges, virtuele assistenten enz.).

de deur wijd opengezet voor **cybercriminaliteit**[10]. Met "cybercrime-as-a-service" en de ondergrondse cybercrime-economie zijn cybercrimeproducten en -diensten gemakkelijk te krijgen. Criminelen passen zich snel aan en gebruiken nieuwe technologieën voor hun eigen doeleinden. Zo komen er bijvoorbeeld nagemaakte en vervalste geneesmiddelen in de legitieme toeleveringsketen van geneesmiddelen terecht[11]. De exponentiële toename van onlinemateriaal dat in verband staat met seksueel misbruik van kinderen[12] toont de maatschappelijke gevolgen van veranderende criminaliteitspatronen aan. Uit een recent onderzoek is gebleken dat de meeste mensen in de EU (55%) zich er zorgen over maken dat criminelen en fraudeurs toegang krijgen tot hun gegevens[13].

De **mondiale omgeving** versterkt deze dreigingen nog. Door het assertieve industriebeleid van derde landen, in combinatie met de aanhoudende, door de cyberomgeving gefaciliteerde diefstal van intellectuele eigendom, verandert het strategische model voor de bescherming en bevordering van Europese belangen. Dit wordt nog versterkt door de opkomst van toepassingen voor tweeërlei gebruik, waardoor een sterke civiele technologische sector ook een krachtige troef wordt voor defensie- en veiligheidsvermogens. Industriële spionage heeft aanzienlijke gevolgen voor de economie, de werkgelegenheid en de groei in de EU: cyberdiefstal van bedrijfsgeheimen kost de EU naar schatting 60 miljard EUR[14]. Dit vereist dat er zorgvuldig over wordt nagedacht in hoeverre afhankelijkheden en de toegenomen blootstelling aan cyberbedreigingen van invloed zijn op het vermogen van de EU om zowel particulieren als bedrijven bescherming te bieden.

De COVID-19-crisis heeft ook onderstreept hoe sociale verdeeldheid en onzekerheden leiden tot kwetsbaarheid op veiligheidsgebied. Dit versterkt het potentieel voor meer geavanceerde en **hybride aanvallen** van de kant van statelijke en niet-statelijke actoren, waarbij zwakke plekken worden benut door een combinatie van cyberaanvallen, beschadiging van kritieke infrastructuur[15], desinformatiecampagnes en radicalisering van het politieke narratief[16].

Tegelijkertijd blijven al lang bestaande bedreigingen zich verder ontwikkelen. Er was in 2019 een neerwaartse trend waar te nemen waar het ging om **terroristische aanslagen** in de EU. De dreiging die voor burgers in de EU uitgaat van jihadistische aanslagen van of geïnspireerd door IS en Al Qaida, en filialen daarvan, blijft echter groot[17]. Daarnaast neemt ook de

---

[10] Volgens sommige prognoses zullen de kosten van gegevenslekken tegen 2024 oplopen tot 5 biljoen USD per jaar, tegenover 3 biljoen USD in 2015 (Juniper Research, The Future of Cybercrime & Security).

[11] In een studie uit 2016 (Legiscript) wordt geschat dat wereldwijd slechts 4% van de internetapotheken op rechtmatige wijze te werk gaat, en dat consumenten in de EU belangrijke doelwitten zijn voor de 30 000–35 000 illegale internetapotheken die online actief zijn.

[12] EU-strategie voor doeltreffender bestrijding van seksueel misbruik van kinderen (COM(2020) 607).

[13] Bureau van de Europese Unie voor de grondrechten (2020): Your rights matter: Security concerns and experiences. Fundamental Rights Survey, Luxemburg, Bureau voor Publicaties van de Europese Unie.

[14] The scale and impact of industrial espionage and theft of trade secrets through cyber, 2018.

[15] Kritieke infrastructuren zijn essentieel voor vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de ontwrichting of vernietiging aanzienlijke gevolgen heeft (Richtlijn 2008/114/EG van de Raad).

[16] 97% van de EU-burgers is al eens nepnieuws tegengekomen, en 38% wordt er dagelijks mee geconfronteerd (zie JOIN(2020) 8 final).

[17] In totaal zijn in dertien lidstaten van de EU 119 gelukte, mislukte of verijdelde terroristische aanslagen gemeld, waarbij tien doden en 27 gewonden vielen (Europol: European Union Terrorism Situation and Trend Report, 2020).

dreiging van gewelddadig rechtsextremisme toe[18]. De aanvallen die zijn ingegeven door racisme moeten aanleiding geven tot ernstige bezorgdheid: gezien de dodelijke antisemitische terroristische aanslagen in Halle blijft een krachtiger respons noodzakelijk, overeenkomstig de verklaring van de Raad van 2018[19]. Een op de vijf mensen in de EU maakt zich grote zorgen dat er de komende twaalf maanden een terroristische aanslag zou kunnen worden gepleegd[20]. Verreweg de meeste van de recente terroristische aanslagen waren laagtechnologische aanslagen, waarbij alleen handelende daders het gemunt hadden op personen in openbare ruimten, terwijl terroristische propaganda op internet een nieuwe betekenis kreeg door de livestreaming van de aanslagen in Christchurch[21]. De dreiging die van geradicaliseerde personen uitgaat, is nog steeds hoog, en wordt mogelijk nog versterkt door terugkerende buitenlandse terroristische strijders en extremisten die uit de gevangenis zijn vrijgelaten[22].

De crisis heeft ook laten zien hoe bestaande dreigingen zich in nieuwe omstandigheden verder kunnen ontwikkelen. **Misdaadorganisaties** hebben gebruik gemaakt van goederentekorten om nieuwe illegale markten te creëren. De handel in illegale drugs is nog steeds de grootste criminele markt in de EU, met een verkoopwaarde van minimaal 30 miljard EUR per jaar in de EU[23]. Mensenhandel bestaat nog steeds: volgens ramingen wordt met alle vormen van uitbuiting jaarlijks bijna 30 miljard EUR winst gemaakt[24]. De internationale handel in vervalste geneesmiddelen heeft inmiddels een omvang van 38,9 miljard EUR bereikt[25]. Tegelijkertijd betekent de kleine kans op confiscatie dat criminelen hun criminele activiteiten kunnen uitbreiden en de legale economie verder kunnen infiltreren[26]. Het is voor criminelen en terroristen gemakkelijker geworden om aan vuurwapens te komen, via de onlinemarkt en door middel van nieuwe technologieën zoals 3D-printen[27]. Het gebruik van kunstmatige intelligentie, nieuwe technologieën en robotica zal het risico dat criminelen de voordelen van innovatie voor kwaadaardige doeleinden exploiteren, verder doen toenemen[28].

Deze bedreigingen vallen onder meerdere categorieën en treffen verschillende geledingen van de samenleving op verschillende manieren. Zij vormen alle een groot gevaar voor mensen en

---

[18] In 2019 zijn er in drie lidstaten zes rechtsextremistische terroristische aanslagen gemeld (waarvan er één is gelukt, één is mislukt en vier zijn verijdeld) tegenover slechts één in 2018. Bovendien zijn er doden gevallen bij incidenten die niet als terroristisch zijn aangemerkt (Europol, 2020).

[19] Zie ook de verklaring van de Raad betreffende de bestrijding van antisemitisme en de ontwikkeling van een gemeenschappelijke beveiligingsaanpak voor een betere bescherming van de Joodse gemeenschappen en instellingen in Europa.

[20] Bureau van de Europese Unie voor de grondrechten: Your rights matter: Security concerns and experiences, 2020.

[21] In de periode van juli 2015 tot eind 2019 trof Europol op 361 platformen terroristische inhoud aan (Europol, 2020).

[22] Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism, 2019.

[23] EMCDDA en Europol: EU Drugs Market Report 2019.

[24] Europol: The Trafficking in Human Beings – Financial Business Model (2015).

[25] Verslag van het Bureau voor intellectuele eigendom van de Europese Unie en de OESO: Trade in Counterfeit Pharmaceutical Products

[26] Verslag *Ontneming en confiscatie van vermogensbestanddelen: zorgen dat misdaad niet loont* (COM(2020) 217).

[27] In 2017 werden bij 41% van alle terroristische aanslagen vuurwapens gebruikt (Europol, 2018).

[28] In juli 2020 presenteerden de Franse en de Nederlandse rechtshandhavings- en justitiële autoriteiten, samen met Europol en Eurojust, het gezamenlijk onderzoek over de ontmanteling van EncroChat, een versleuteld telefoonnetwerk dat werd gebruikt door criminele netwerken die betrokken zijn bij gewelddadige aanslagen, corruptie, moordpogingen en grootschalige drugstransporten.

bedrijven en vereisen een alomvattende en coherente respons op EU-niveau. Wanneer kwetsbaarheden op veiligheidsgebied zelfs kunnen ontstaan door met internet verbonden kleine huishoudelijke apparaten, zoals een koelkast of koffiezetapparaat met internettoegang, kunnen we voor de bescherming van onze veiligheid niet langer alleen vertrouwen op traditionele overheidsactoren. Marktdeelnemers moeten meer verantwoordelijkheid nemen voor de cyberbeveiliging van producten en diensten die zij in de handel brengen, en ook mensen moeten ten minste over een basiskennis van cyberbeveiliging beschikken om zichzelf te kunnen beschermen.

III. Een gecoördineerde EU-respons voor de hele samenleving

De EU heeft al aangetoond hoe zij een reële meerwaarde kan bieden. Sinds 2015 heeft de veiligheidsunie nieuwe verbanden gelegd wat betreft de manier waarop het veiligheidsbeleid op EU-niveau wordt aangepakt. Er moet echter meer worden gedaan om daar de hele samenleving, met inbegrip van overheden op alle niveaus, bedrijven in alle sectoren en mensen in alle lidstaten bij te betrekken. De groeiende bewustwording van de risico's van afhankelijkheid[29] en de behoefte aan een sterke Europese industriële strategie op te bouwen[30], betekenen dat de EU een kritische massa van industrie, technologische productie en veerkracht van de toeleveringsketen nodig heeft. Een sterke positie betekent ook dat de grondrechten en waarden van de EU volledig moeten worden geëerbiedigd: dat is een eerste voorwaarde voor een legitiem, doeltreffend en duurzaam veiligheidsbeleid. Met deze strategie voor de veiligheidsunie worden concrete werkstromen vastgesteld voor de toekomst. De strategie is opgezet rond de volgende gemeenschappelijke doelstellingen:

- ***Opbouw van vermogens en capaciteiten met het oog op vroegtijdige opsporing en preventie van en respons op crises.*** Europa moet weerbaarder worden, zodat het toekomstige schokken kan voorkomen, zich ertegen kan beschermen en er beter tegen bestand is. We moeten vermogens en capaciteiten opbouwen om veiligheidscrises vroegtijdig te kunnen opsporen en er snel op te kunnen reageren. Dit vereist een geïntegreerde en gecoördineerde aanpak, zowel op mondiaal niveau als via sectorspecifieke initiatieven (zoals voor de financiële sector, energie, justitie, rechtshandhaving, gezondheidszorg, zeevaart en vervoer), waarbij we voortbouwen op bestaande instrumenten en initiatieven[31]. De Commissie zal tevens met voorstellen komen voor een breed crisismanagementsysteem binnen de EU, dat ook relevant kan zijn op veiligheidsgebied.
- ***Nadruk op resultaten.*** Een prestatiegerichte strategie moet gebaseerd zijn op een zorgvuldige dreigings- en risicobeoordeling, zodat we onze inspanningen zo gericht mogelijk kunnen inzetten. De juiste regels en de juiste instrumenten moeten worden

[29] De risico's van afhankelijkheid van het buitenland hebben betrekking op een toegenomen blootstelling aan potentiële dreigingen. Deze lopen uiteen van de exploitatie van kwetsbaarheden in IT-infrastructuren waardoor kritieke infrastructuur (zoals die voor energie, vervoer, banken, gezondheid) in gevaar komt of industriële besturingssystemen worden overgenomen, tot een verhoogde capaciteit voor datadiefstal of spionage.

[30] Mededeling van de Commissie *Een nieuwe industriestrategie voor Europa* (COM(2020) 102).

[31] Zoals de geïntegreerde regeling politieke crisisrespons (IPCR), het coördinatiecentrum voor respons in noodsituaties, de aanbeveling van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises (C(2017) 6100) en het operationele EU-protocol voor de bestrijding van hybride bedreigingen (EU Playbook) (SWD(2016) 227).

vastgesteld en toegepast. Betrouwbare strategische inlichtingen moeten als basis dienen voor het veiligheidsbeleid van de EU. Indien EU-wetgeving vereist is, moet deze correct worden opgevolgd, zodat de wetgeving volledig wordt toegepast. Zo wordt vermeden dat er fragmentatie ontstaat en dat er lacunes blijven bestaan die geëxploiteerd kunnen worden. Voor een effectieve uitvoering van deze strategie moet tevens voor passende financiering worden gezorgd in de programmeringsperiode 2021–2027, ook wat de betrokken EU-agentschappen betreft.

- ***Alle betrokkenen in de openbare en de particuliere sector moeten zich gezamenlijk inzetten.*** Het komt voor dat belangrijke spelers in de publieke en de particuliere sector huiverig zijn om voor de veiligheid relevante informatie te delen, uit angst om de nationale veiligheid in gevaar te brengen of om concurrentieoverwegingen[32]. Maar we kunnen het effectiefst optreden als we erop ingesteld zijn elkaar te steunen. In de eerste plaats vergt dit intensievere samenwerking tussen de lidstaten, met de medewerking van de rechtshandhavings-, justitie- en andere overheidsinstanties, en met de instellingen en agentschappen van de EU. Zo kunnen we het begrip en de uitwisseling versterken die nodig zijn voor gemeenschappelijke oplossingen. Samenwerking met de particuliere sector is ook essentieel, temeer daar een belangrijk deel van de digitale en niet-digitale infrastructuur die cruciaal is voor de doeltreffende bestrijding van criminaliteit en terrorisme, in handen is van het bedrijfsleven. Mensen kunnen zelf ook een bijdrage leveren, bijvoorbeeld door de vaardigheden en de kennis te verwerven die nodig zijn om cybercriminaliteit en desinformatie te bestrijden. Tot slot moet deze gezamenlijke inspanning zich ook uitstrekken tot buiten onze grenzen en moeten we met gelijkgestemde partners nauwere banden aanknopen.

IV. Iedereen in de EU beschermen: Strategische prioriteiten voor de veiligheidsunie

De EU verkeert in een unieke positie om deze nieuwe mondiale bedreigingen en uitdagingen het hoofd te bieden. Uit bovenstaande dreigingsanalyse blijkt dat op EU-niveau, met volledige eerbiediging van de grondrechten, vier strategische prioriteiten moeten worden gesteld: i) een toekomstbestendige veiligheidsomgeving, ii) aanpak van veranderende dreigingen, iii) bescherming van Europeanen tegen terrorisme en georganiseerde misdaad, iv) een krachtig Europees veiligheidsecosysteem.

1. Een toekomstbestendige veiligheidsomgeving

Bescherming en weerbaarheid van kritieke infrastructuur

Mensen vertrouwen in hun dagelijks leven op belangrijke infrastructuur om te reizen, om te werken, om gebruik te maken van essentiële openbare diensten zoals ziekenhuizen, vervoer en energievoorziening, of om hun democratische rechten uit te oefenen. Als die infrastructuren onvoldoende worden beschermd en hun weerbaarheid tekortschiet, kunnen door aanvallen in de afzonderlijke lidstaten en mogelijk in de hele EU enorme storingen worden veroorzaakt, zowel fysieke als digitale.

[32] Gezamenlijke mededeling *Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU* (JOIN (2017) 450).

Het bestaande EU-kader voor bescherming en weerbaarheid van kritieke infrastructuren[33] heeft geen gelijke tred gehouden met de zich ontwikkelende risico's. Door de toenemende onderlinge afhankelijkheid kunnen verstoringen in de ene sector een onmiddellijk effect hebben op activiteiten in andere sectoren: een aanval op de elektriciteitsproductie kan de telecommunicatie stilleggen en ziekenhuizen, banken of luchthavens uitschakelen, terwijl een aanval op digitale infrastructuur zou kunnen leiden tot storingen in netwerken voor energie of financiën. Naarmate onze economie en onze maatschappij steeds meer online gaan, worden risico's zoals deze steeds meer een acuut gevaar. Het wetgevingskader moet voor deze toegenomen onderlinge verwevenheid en onderlinge afhankelijkheid zijn toegerust met robuuste maatregelen (van zowel cyber- als fysieke aard) voor de bescherming en de veerkracht van kritieke infrastructuur. Essentiële diensten, waaronder die welke gebaseerd zijn op ruimte-infrastructuren, moeten adequaat worden beschermd tegen bestaande en verwachte dreigingen, maar moeten ook veerkrachtig zijn. Dit impliceert het vermogen van een systeem om zich voor te bereiden en te anticiperen op ongunstige voorvallen, deze te absorberen, zich ervan te herstellen en zich er met meer succes aan aan te passen.

Tegelijkertijd hebben de lidstaten gebruikgemaakt van hun beoordelingsmarge door de bestaande wetgeving op verschillende manieren ten uitvoer te leggen. De daaruit voortvloeiende fragmentatie kan de interne markt ondermijnen en grensoverschrijdende coördinatie bemoeilijken, vooral in grensregio's. Exploitanten die in verschillende lidstaten essentiële diensten leveren, moeten aan verschillende meldingsregelingen voldoen. De Commissie onderzoekt of **nieuwe kaders voor zowel fysieke als digitale infrastructuren** kunnen zorgen voor meer consistentie en een samenhangender aanpak om het betrouwbare aanbod van essentiële diensten te waarborgen. Dit kader moet vergezeld gaan van **sectorspecifieke initiatieven** om de specifieke risico's van kritieke infrastructuren, zoals op het gebied van vervoer, ruimte, energie, financiën en gezondheid, aan te pakken[34]. Aangezien de financiële sector sterk afhankelijk is van IT-diensten en zeer gevoelig is voor cyberaanvallen, zal als eerste stap een initiatief worden genomen voor de digitale operationele veerkracht van de financiële sectoren. Vanwege de bijzondere gevoeligheden en de bijzondere impact van het energiesysteem zal met een specifiek initiatief worden bijgedragen tot een sterkere weerbaarheid van kritieke energie-infrastructuur tegen fysieke, cyber- en hybride bedreigingen, waarbij wordt gezorgd voor een gelijk grensoverschrijdend speelveld voor alle energie-exploitanten.

De voor de veiligheid relevante effecten van buitenlandse directe investeringen die gevolgen kunnen hebben voor kritieke infrastructuren of kritieke technologieën, zullen ook worden onderworpen aan de beoordelingen die de EU-lidstaten en de Commissie verrichten binnen het nieuwe Europese kader voor de screening van buitenlandse directe investeringen[35].

---

[33] Richtlijn (EU) 2016/1148 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PB L 194 van 19.7.2016), Richtlijn 2008/114/EG van de Raad inzake de identificatie van Europese kritieke infrastructuren, de aanmerking van infrastructuren als Europese kritieke infrastructuren en de beoordeling van de noodzaak de bescherming van dergelijke infrastructuren te verbeteren.

[34] Aangezien de gezondheidssector onder druk is komen te staan, met name tijdens de COVID-19-crisis, zal de Commissie ook initiatieven overwegen om het EU-kader voor gezondheidsbeveiliging en de verantwoordelijke EU-agentschappen te versterken, zodat zij kunnen reageren op ernstige grensoverschrijdende bedreigingen van de gezondheid.

[35] Wanneer Verordening (EU) 2019/452 van het Europees Parlement en de Raad van 19 maart 2019 tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Unie op 11 oktober 2020 volledig in werking treedt, zal de EU beschikken over een nieuw samenwerkingsmechanisme inzake

De EU kan ook nieuwe instrumenten ontwikkelen om de veerkracht van kritieke infrastructuren te ondersteunen. Het wereldwijde internet heeft tot nu toe blijk gegeven van een grote veerkracht, met name wat betreft het vermogen om grotere verkeersvolumes te ondersteunen. We moeten echter voorbereid zijn op mogelijke toekomstige crises die de veiligheid, stabiliteit en veerkracht van het internet kunnen aantasten. Om ervoor te zorgen dat het internet blijft functioneren, moeten robuuste maatregelen worden getroffen tegen cyberincidenten en kwaadwillige onlineactiviteiten, en moet de afhankelijkheid van zich buiten Europa bevindende infrastructuren en diensten worden beperkt. Dit vereist een combinatie van wetgeving, waarbij de bestaande regels worden herzien om een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de EU te waarborgen, meer investeringen in onderzoek en innovatie, en onderzoek naar de inzet of versterking van essentiële infrastructuren en middelen voor het internet, met name het domeinnaamsysteem[36].

Een essentieel element voor de bescherming van essentiële digitale activa op nationaal en EU-niveau is het aanbieden van een kanaal voor veilige communicatie ten behoeve van kritieke infrastructuren. De Commissie werkt samen met de lidstaten aan een gecertificeerde, beveiligde end-to-end-kwantuminfrastructuur, op terrestrische en ruimtebasis, in combinatie met het beveiligde satellietcommunicatiesysteem voor de overheid, zoals vastgelegd in de verordening inzake het ruimtevaartprogramma[37].

Cyberbeveiliging

Het aantal cyberaanvallen blijft stijgen[38]. Deze aanvallen worden ook steeds geavanceerder, ze zijn afkomstig uit allerlei verschillende bronnen binnen en buiten de EU en zijn gericht op gebieden met een maximale kwetsbaarheid. Er zijn vaak statelijke of door een staat gesteunde actoren bij betrokken, die zich richten op de belangrijkste digitale infrastructuren zoals grote aanbieders van clouddiensten[39]. Cyberrisico's zijn ook een belangrijke bedreiging voor het financiële stelsel gebleken. Het Internationaal Monetair Fonds heeft het jaarlijkse verlies als gevolg van cyberaanvallen geraamd op 9% van de netto-inkomsten van alle banken wereldwijd, dat wil zeggen ongeveer 100 miljard USD[40]. De overstap naar verbonden apparaten levert grote voordelen op voor de gebruikers, maar nu er minder gegevens in datacentra worden opgeslagen en verwerkt en juist meer dicht bij de gebruiker (edgecomputing)[41], zal cyberbeveiliging zich niet langer voornamelijk kunnen richten op de bescherming van centrale punten[42].

---

directe investeringen van buiten de EU die gevolgen kunnen hebben voor de veiligheid of de openbare orde. Krachtens de verordening zullen de lidstaten en de Commissie potentiële risico's in verband met dergelijke buitenlandse directe investeringen beoordelen en, in voorkomend geval, wanneer dat voor meer dan één lidstaat relevant is, passende middelen voorstellen om deze risico's te beperken.

36 Een domeinnaamsysteem (DNS) is een hiërarchisch en gedecentraliseerd naamgevingsysteem voor computers, diensten en andere middelen die met het internet of met een particulier netwerk zijn verbonden. Het DNS vertaalt domeinnamen naar de IP-adressen die vereist zijn voor het lokaliseren en identificeren van computerdiensten en -apparatuur.

37 Voorstel voor een verordening tot vaststelling van het ruimtevaartprogramma van de Unie en het Agentschap van de Europese Unie voor het ruimtevaartprogramma (COM(2018) 447).

38 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

39 Distributed Denial of Service (DDoS)-aanvallen vormen een permanente dreiging: grote aanbieders moesten massale DDoS-aanvallen afslaan, zoals een aanval op Amazon Web Services in februari 2020.

40 https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

41 "Edgecomputing" is een gedistribueerde, open IT-architectuur met een gedecentraliseerde verwerkingscapaciteit, waarmee mobiele technologie en technologie voor het internet der dingen mogelijk

In 2017 heeft de EU een aanpak van cyberbeveiliging voorgesteld waarbij weerbaarheid, een snelle respons en doeltreffende afschrikking centraal staan[43]. De EU moet nu ervoor zorgen dat haar capaciteiten op het gebied van cyberbeveiliging gelijke tred houden met de realiteit, zodat zowel weerbaarheid als een snelle respons kan worden gerealiseerd. Dit vergt een daadwerkelijk samenlevingsbrede aanpak, waarbij de instellingen, organen en instanties van de EU, de lidstaten, de industrie, de academische wereld en particulieren de nodige prioriteit geven aan cyberbeveiliging[44]. Deze horizontale aanpak moet dan weer worden aangevuld met sectorspecifieke cyberbeveiligingsbenaderingen voor gebieden als energie, financiële diensten, vervoer en gezondheidszorg. In de volgende fase van de werkzaamheden van de EU moeten alle krachten worden gebundeld in een herziene Europese strategie voor cyberbeveiliging.

Met het verkennen van nieuwe, versterkte vormen van samenwerking tussen inlichtingendiensten, moeten EU INTCEN en andere organisaties op het gebied van beveiliging een bijdrage leveren aan de inspanningen om cyberbeveiliging te verbeteren en terrorisme, extremisme, radicalisme en hybride bedreigingen te bestrijden.

Gezien de lopende uitrol van de **5G-infrastructuur** in de EU en de potentiële afhankelijkheid van veel kritieke diensten van 5G-netwerken, zouden de gevolgen van systemische en wijdverbreide verstoringen bijzonder ernstig zijn. Het proces dat op gang is gebracht door de aanbeveling van de Commissie van 2019 over de cyberbeveiliging van 5G-netwerken[45] heeft nu geleid tot specifieke maatregelen van de lidstaten als onderdeel van een 5G-toolbox[46].

Een van de belangrijkste behoeften op de lange termijn is het ontwikkelen van een cultuur van **cyberbeveiliging door ontwerp**, waarbij beveiliging vanaf de eerste fase in producten en diensten wordt ingebouwd. Een belangrijke bijdrage hieraan is het nieuwe kader voor de certificering van cyberbeveiliging op grond van de cyberbeveiligingsverordening[47]. Dit kader is al in gebruik en twee certificeringsregelingen zijn al in voorbereiding. De prioriteiten voor nog een aantal regelingen zullen later dit jaar worden vastgesteld. De samenwerking tussen het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa), de gegevensbeschermingsautoriteiten en het Europees Comité voor gegevensbescherming[48] is op dit gebied van cruciaal belang.

De Commissie heeft reeds vastgesteld dat er behoefte is aan een **gezamenlijke cybereenheid** die als platform voor gestructureerde en gecoördineerde samenwerking moet dienen. Een mechanisme voor wederzijdse bijstand op EU-niveau in tijden van crisis zou daarvan deel

---

wordt gemaakt. Bij edgecomputing worden de gegevens verwerkt door het apparaat zelf of door een lokale computer of server, in plaats van te worden doorgeleid naar een datacentrum.

42 Mededeling *Een Europese datastrategie* (COM(2020) 66 final).

43 Gezamenlijke mededeling *Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU* (JOIN(2017) 450).

44 Het verslag *Cybersecurity, our digital anchor* van het Gemeenschappelijk Centrum voor onderzoek biedt multidimensionale inzichten in de toename van cyberbeveiliging gedurende de afgelopen 40 jaar.

45 Aanbeveling van de Commissie over de cyberbeveiliging van 5G-netwerken (COM(2019) 534, C(2019) 2335). De aanbeveling voorziet in een toetsing ervan in het laatste kwartaal van 2020.

46 Zie het verslag van de NIS-samenwerkingsgroep over de uitvoering van de toolbox van 24 juli 2020.

47 Verordening (EU) 2019/881 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging) en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie (de cyberbeveiligingsverordening).

48 Mededeling *Gegevensbescherming als pijler van zeggenschap van de burger en de EU-aanpak van de digitale transformatie — twee jaar toepassing van de algemene verordening gegevensbescherming* (COM(2020) 264).

kunnen uitmaken. Voortbouwend op de uitvoering van de aanbeveling met een blauwdruk[49] zou de gezamenlijke cybereenheid vertrouwen kunnen opbouwen tussen de verschillende actoren in het Europese cyberbeveiligingsecosysteem en lidstaten daarmee een belangrijke dienst kunnen aanbieden. De Commissie zal besprekingen starten met relevante belanghebbenden (te beginnen met de lidstaten) en tegen eind 2020 een duidelijk proces, mijlpalen en tijdschema vaststellen.

Belangrijk is ook dat er gemeenschappelijke regels gelden inzake informatiebeveiliging en cyberbeveiliging voor alle instellingen, organen en instanties van de EU. Het doel moet zijn bindende en strenge gemeenschappelijke normen vast te stellen voor de veilige uitwisseling van informatie en voor de beveiliging van digitale infrastructuren en systemen bij alle instellingen, organen en instanties van de EU. Dit nieuwe kader moet de basis vormen voor krachtige en efficiënte operationele samenwerking op het gebied van cyberbeveiliging tussen de instellingen, organen en instanties van de EU, met als middelpunt het computercrisisteam (CERT-EU) voor de instellingen, organen en instanties van de EU.

Gezien het mondiale karakter ervan is het opbouwen en onderhouden van robuuste **internationale partnerschappen** van fundamenteel belang voor de verdere preventie en bestrijding van en respons op cyberaanvallen. Het kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten ("instrumentarium voor cyberdiplomatie")[50] omvat maatregelen in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid, waaronder beperkende maatregelen (sancties), die kunnen worden ingezet tegen activiteiten die schadelijk zijn voor de politieke, veiligheids- en economische belangen van de EU. De EU moet daarnaast haar werkzaamheden in het kader van de ontwikkelings- en samenwerkingsfondsen intensiveren om te voorzien in capaciteitsopbouw voor het ondersteunen van de partnerlanden bij het versterken van hun digitale ecosystemen, het vaststellen van nationale wetgevingshervormingen en het naleven van internationale normen. Dit versterkt de weerbaarheid van de gemeenschap in het algemeen en haar vermogen om een doeltreffende respons te geven op cyberdreigingen. In dit verband moeten specifieke werkzaamheden plaatsvinden ter bevordering van de EU-normen en de relevante wetgeving ter versterking van de cyberbeveiliging van de partnerlanden in de nabuurschap[51].

Openbare ruimten beschermen

De recente terroristische aanslagen waren gericht op **openbare ruimten**, waaronder gebedshuizen en vervoersknooppunten. Daarbij werd gebruik gemaakt van de open en toegankelijke aard van die doelwitten. De opkomst van terrorisme dat voortvloeit uit politiek of ideologisch gemotiveerd extremisme heeft deze dreiging des te acuter gemaakt. Daardoor is een krachtiger fysieke bescherming van dergelijke ruimten nodig, alsmede adequate opsporingssystemen, zonder dat dit ten koste mag gaan van de vrijheden van de burgers[52]. De Commissie zal de publiek-private samenwerking voor de bescherming van openbare ruimten bevorderen door middel van financiering, uitwisseling van ervaringen en goede praktijken,

[49] Aanbeveling (EU) 2017/1584 van de Commissie inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.

[50] https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/nl/pdf

[51] Zie de richtsnoeren voor externe cybercapaciteitsopbouw van de EU, aangenomen in de conclusies van de Raad van 26 juni 2018.

[52] Systemen voor biometrische identificatie op afstand verdienen specifieke aandacht. De eerste standpunten van de Commissie worden uiteengezet in het Witboek van 19 februari 2020 over kunstmatige intelligentie (COM(2020) 65).

specifieke richtsnoeren[53] en aanbevelingen[54]. Ook voorlichting, prestatievereisten, testen van detectieapparatuur en grondiger antecedentenonderzoek, om dreigingen van binnenuit te bestrijden, zullen deel uitmaken van de aanpak. Een belangrijk aspect om in het oog te houden is dat minderheden en kwetsbare personen, onder wie personen die het doelwit zijn op grond van hun godsdienst of geslacht, onevenredig zwaar kunnen worden getroffen. Daarvoor is dan ook bijzondere aandacht nodig. Regionale en lokale overheden spelen een belangrijke rol bij het verbeteren van de beveiliging van openbare ruimten. De Commissie draagt ook bij tot het bevorderen van innovatie van steden op het gebied van de beveiliging van openbare ruimten[55]. De start in november 2018 van een nieuw partnerschap voor "veiligheid in openbare ruimten" in het kader van de Stedenagenda[56] getuigt van het vaste voornemen van de lidstaten, de Commissie en de steden om bedreigingen voor de veiligheid in de stedelijke ruimte beter aan te pakken.

De markt voor **drones** blijft nog steeds groeien, met veel waardevolle en legitieme toepassingen. Drones kunnen echter ook worden misbruikt door criminelen en terroristen, waarbij de openbare ruimten in het bijzonder gevaar lopen. Tot de doelwitten behoren individuen, bijeenkomsten, kritieke infrastructuur, rechtshandhavingsinstanties, grenzen en openbare ruimten. Kennis over het gebruik van drones bij conflicten kan ook weer in Europa terechtkomen, hetzij rechtstreeks (via teruggekeerde buitenlandse terroristische strijders), hetzij online. De regels die het Europees Agentschap voor de veiligheid van de luchtvaart heeft ontwikkeld, zijn een belangrijke eerste stap op gebieden zoals de registratie van dronebestuurders en de verplichting dat drones op afstand identificeerbaar zijn. Nu drones steeds gemakkelijker verkrijgbaar en steeds betaalbaarder worden en steeds meer taken aankunnen, zijn extra maatregelen nodig. Daarbij kan het gaan om het delen van informatie, om richtsnoeren en goede praktijken voor het gebruik ervan door iedereen, inclusief door de rechtshandhavingsinstanties, en om meer testen van maatregelen tegen drones[57]. Daarnaast moeten de privacy- en gegevensbeschermingseffecten van het gebruik van drones in openbare ruimten nader worden geanalyseerd en aangepakt.

Belangrijkste maatregelen
• Wetgeving inzake de bescherming en weerbaarheid van kritieke infrastructuur • Herziening van de richtlijn netwerk- en informatiesystemen • Initiatief inzake de operationele veerkracht van het financiële stelsel • Bescherming en cyberbeveiliging van kritieke energie-infrastructuur en een netcode voor

[53] Bijvoorbeeld de richtsnoeren voor de selectie van geschikte oplossingen voor veiligheidsbarrières ter bescherming van de openbare ruimte (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf)

[54] Richtsnoeren inzake goede praktijken worden gegeven in SWD(2019) 140, waarin ook een hoofdstuk over publiek-private samenwerking is opgenomen. Bij de financiering in het kader van het ISF – Politie is er speciale aandacht voor het verbeteren van de publiek-private samenwerking.

[55] Drie steden (Piraeus in Griekenland, Tampere in Finland en Turijn in Italië) gaan nieuwe oplossingen testen in het kader van de stedelijke innovatieve acties die worden medegefinancierd door het Europees Fonds voor Regionale Ontwikkeling (EFRO).

[56] De Stedenagenda voor de EU volgt een nieuwe multilevel-werkmethode voor de bevordering van de samenwerking tussen de lidstaten, de steden, de Commissie en andere belanghebbenden om de groei, leefbaarheid en innovatie in de steden van Europa te stimuleren en sociale uitdagingen te identificeren en aan te pakken.

[57] Onlangs is een meerjarig testprogramma opgestart om de lidstaten te ondersteunen bij de ontwikkeling van gemeenschappelijke methoden en een testplatform op dit gebied.

cyberbeveiliging voor grensoverschrijdende elektriciteitsstromen
- Europese strategie inzake cyberbeveiliging
- Volgende stappen naar de oprichting van een gezamenlijke cybereenheid
- Gemeenschappelijke regels inzake informatiebeveiliging en cyberbeveiliging voor instellingen, organen en instanties van de EU
- Intensievere samenwerking voor de bescherming van openbare ruimten, waaronder gebedshuizen
- Uitwisseling van beste praktijken voor de aanpak van misbruik van drones

2. Aanpak van veranderende dreigingen

Cybercriminaliteit

Technologie biedt nieuwe kansen voor de samenleving, en geeft de rechterlijke macht en rechtshandhaving nieuwe instrumenten in handen. Maar technologie opent tegelijkertijd deuren voor criminelen. Malware, diefstal van persoonlijke of zakelijke gegevens door hacken, en het blokkeren van digitale activiteiten die financiële of reputatieschade veroorzaken, zijn allemaal in opmars. Een weerbare omgeving door krachtige cyberbeveiliging is de eerste verdedigingslinie. De rechtshandhavingsinstanties moeten bij digitaal onderzoek duidelijke regels kunnen volgen om misdrijven te onderzoeken en te vervolgen en slachtoffers de nodige bescherming te bieden. De werkzaamheden op dit gebied moeten voortbouwen op de gezamenlijke cybercrime-taskforce van Europol en het crisisresponsprotocol van de rechtshandhavingsinstanties, dat is opgezet om de respons op grootschalige cyberaanvallen te coördineren. Doeltreffende mechanismen voor publiek-private partnerschappen en samenwerking zijn eveneens essentieel.

Tegelijkertijd moet de bestrijding van cybercriminaliteit in de hele EU een strategische communicatieprioriteit worden, om de Europeanen attent te maken op de risico's die zij lopen en de preventieve maatregelen die zij kunnen nemen. Dit moet onderdeel zijn van een proactieve aanpak. Essentieel is ook dat het huidige rechtskader volledig wordt uitgevoerd[58]: de Commissie is bereid zo nodig inbreukprocedures in te leiden en dit kader voortdurend te toetsen om ervoor te zorgen dat het aan het beoogde doel blijft beantwoorden. De Commissie zal tevens (samen met Europol en het Agentschap van de Europese Unie voor cyberbeveiliging) de haalbaarheid onderzoeken van een EU-systeem voor snelle waarschuwing bij cybercriminaliteit, dat bij een golf van cybercriminaliteit informatievoorziening en een snelle respons kan waarborgen.

Cybercriminaliteit is een mondiale uitdaging die alleen met doeltreffende internationale samenwerking kan worden aangepakt. De EU steunt het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa, dat een doeltreffend en beproefd kader biedt dat alle landen in staat stelt te bepalen welke systemen en communicatiekanalen zij nodig hebben om doeltreffend met elkaar te kunnen samenwerken.

Bijna de helft van de EU-burgers maakt zich zorgen over misbruik van gegevens[59] en **identiteitsdiefstal**[60]. Frauduleus gebruik van een identiteit voor financieel gewin is één aspect

[58] Richtlijn 2013/40/EU over aanvallen op informatiesystemen.
[59] 46% (Eurobarometer over de houding van de Europeanen tegenover cyberbeveiliging, januari 2020).

daarvan, maar identiteitsdiefstal kan ook een ernstige persoonlijke en psychologische impact hebben, doordat valse berichten die door de identiteitsdief zijn gepost, jarenlang online kunnen blijven staan. De Commissie zal mogelijke praktische maatregelen onderzoeken om slachtoffers te beschermen tegen alle vormen van identiteitsdiefstal, rekening houdend met het komende Europese initiatief inzake digitale identiteit[61].

Voor het aanpakken van cybercrime moeten we naar de toekomst kijken. Dat we in de samenleving nieuwe technologische ontwikkelingen gebruiken om de economie en de samenleving te versterken, betekent dat ook criminelen kunnen trachten een en ander voor slechte doeleinden te gebruiken. Criminelen kunnen bijvoorbeeld van kunstmatige intelligentie gebruikmaken om wachtwoorden te achterhalen, om het maken van malware te vereenvoudigen, of om beelden en geluid te gebruiken die vervolgens voor identiteitsdiefstal of -fraude kunnen worden toegepast.

Moderne rechtshandhaving

Politie en justitie moeten zich aanpassen aan de nieuwe technologie. Technologische ontwikkelingen en nieuwe bedreigingen vereisen dat rechtshandhavingsinstanties nieuwe instrumenten kunnen gebruiken, nieuwe vaardigheden verwerven en alternatieve onderzoekstechnieken ontwikkelen. Ter aanvulling van de wetgevingsmaatregelen om de grensoverschrijdende toegang tot elektronisch bewijsmateriaal voor strafrechtelijke onderzoeken te verbeteren, kan de EU de rechtshandhavingsinstanties helpen de nodige capaciteit te ontwikkelen om de voor het onderzoeken van misdrijven benodigde gegevens te identificeren, veilig te stellen en te lezen en deze gegevens in rechtszaken als bewijsmateriaal te gebruiken. De Commissie zal onderzoeken welke maatregelen kunnen worden genomen om de **rechtshandhavingscapaciteit in digitale onderzoeken te versterken**, door vast te stellen hoe onderzoek en ontwikkeling optimaal kunnen worden benut om nieuwe instrumenten voor rechtshandhaving te creëren, en hoe door opleiding de benodigde vaardigheden kunnen worden verkregen ten behoeve van politie en justitie. Dit houdt ook in dat strikte wetenschappelijke evaluaties en testmethoden worden toegepast via het Gemeenschappelijk Centrum voor onderzoek van de Commissie.

Door gemeenschappelijke benaderingen kan er ook voor worden gezorgd dat **kunstmatige intelligentie**, **ruimtevaartcapaciteiten**, **big data** en **high performance computing worden geïntegreerd** in het beveiligingsbeleid op een manier die nuttig is voor zowel de criminaliteitsbestrijding als de bescherming van de grondrechten. Kunstmatige intelligentie kan een krachtig instrument zijn voor het bestrijden van criminaliteit, doordat KI grote hoeveelheden informatie kan analyseren en patronen en anomalieën kan ontdekken, en zo een enorme onderzoekscapaciteit creëert[62]. KI kan ook concrete instrumenten opleveren, die bijvoorbeeld bijdragen aan het identificeren van terroristische online-inhoud, het opsporen van verdachte transacties bij de verkoop van gevaarlijke producten en het bieden van bijstand aan burgers in noodsituaties. Om dit potentieel te verwezenlijken, moeten voor onderzoek en innovatie en voor de gebruikers van kunstmatige intelligentie de juiste governance en technische infrastructuur beschikbaar worden gesteld. Daarbij moeten de particuliere sector en

---

60 De overgrote meerderheid van de respondenten van de Eurobarometer van 2018 over de houding van de Europeanen tegenover internetbeveiliging (95%) zag identiteitsdiefstal als een ernstig misdrijf, en zeven op de tien respondenten vinden het een zeer ernstig misdrijf. De in januari 2020 gepubliceerde Eurobarometer bevestigde de bezorgdheid over cybercriminaliteit, onlinefraude en identiteitsdiefstal: twee derde van de respondenten was bezorgd over bankfraude (67%) of identiteitsdiefstal (66%).

61 Mededeling van 19 februari 2020 *De digitale toekomst van Europa vormgeven* (COM(2020) 67).

62 Bijvoorbeeld bij financiële misdrijven.

de academische wereld actief worden betrokken. In dit verband moeten de strengste normen voor de naleving van de grondrechten worden gewaarborgd, evenals een doeltreffende bescherming van de burgers. Met name moeten besluiten die gevolgen hebben voor personen, door mensen worden getoetst en voldoen aan de toepasselijke EU-wetgeving[63].

Zo'n 85% van de onderzoeken naar ernstige misdrijven vereist elektronische informatie en elektronisch bewijsmateriaal, terwijl 65% van het totale aantal verzoeken in dat kader naar aanbieders in een ander rechtsgebied gaat[64]. Het feit dat traditionele fysieke sporen nu online moeten worden gezocht, heeft de kloof tussen de capaciteiten van de rechtshandhaving en die van de criminelen verder vergroot. Het is essentieel om duidelijke regels op te stellen voor grensoverschrijdende toegang tot elektronisch bewijsmateriaal voor strafrechtelijke onderzoeken. Daarom zouden het Europees Parlement en de Raad snel hun goedkeuring moeten verlenen aan de voorstellen inzake elektronisch bewijsmateriaal, zodat rechtshandhavers over een efficiënt instrument kunnen beschikken. Grensoverschrijdende toegang tot elektronisch bewijsmateriaal, waarover multilaterale en bilaterale onderhandelingen zullen moeten worden gevoerd, is eveneens essentieel voor de vaststelling van onderling verenigbare regels op internationaal niveau[65].

De **toegang tot digitaal bewijsmateriaal** is ook afhankelijk van de beschikbaarheid van informatie. Als gegevens te snel worden gewist, kan belangrijk bewijsmateriaal verdwijnen en daarmee de mogelijkheid om verdachten en criminele netwerken (en slachtoffers) te identificeren en te lokaliseren. Maar regelingen inzake gegevensbewaring roepen ook vragen op over de bescherming van de privacy. Afhankelijk van de uitkomst van een aantal zaken die bij het Europese Hof van Justitie aanhangig zijn gemaakt, zal de Commissie de te volgen koers op het gebied van gegevensbewaring beoordelen.

De toegang tot internet-domeinnaaminformatie (de zogeheten WHOIS-gegevens)[66] is belangrijk voor strafrechtelijke onderzoeken, cyberbeveiliging en consumentenbescherming. De toegang tot deze informatie wordt echter moeilijker, in afwachting van de goedkeuring van een nieuw WHOIS-beleid door de Internet Corporation for Assigned Names and Numbers (ICANN). De Commissie zal met de ICANN en de multistakeholdergemeenschap blijven samenwerken om ervoor te zorgen dat partijen die rechtmatig om toegang verzoeken, waaronder rechtshandhavingsinstanties, op efficiënte wijze toegang kunnen krijgen tot WHOIS-gegevens, in overeenstemming met de internationale en EU-regelgeving inzake gegevensbescherming. Hiertoe moeten mogelijke oplossingen worden beoordeeld, zoals de vraag of er wetgeving nodig is ter verduidelijking van de regels voor de toegang tot dergelijke informatie.

Rechtshandhavingsinstanties en gerechtelijke autoriteiten moeten ook worden toegerust om de nodige gegevens en bewijsmateriaal te verkrijgen zodra de **5G-architectuur voor mobiele**

---

[63] Dit houdt in dat moet worden voldaan aan de geldende wetgeving, met inbegrip van de algemene verordening gegevensbescherming (Verordening (EU) 2016/679) en de richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680, die de verwerking van persoonsgegevens regelt in verband met het opsporen, voorkomen, onderzoeken en vervolgen van strafbare feiten of de tenuitvoerlegging van straffen).

[64] Werkdocument van de diensten van de Commissie SWD(2018) 118 final.

[65] Met name het tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa en een overeenkomst tussen de EU en de Verenigde Staten inzake grensoverschrijdende toegang tot elektronisch bewijsmateriaal.

[66] WHOIS-gegevens zijn opgeslagen in databases die wereldwijd worden bijgehouden door 2 500 entiteiten die als register en registrator fungeren.

telecommunicatie volledig is uitgerold in de EU. Daarbij moet het vertrouwelijke karakter van de communicatie in acht worden genomen. Voor het ontwikkelen van internationale normen, het vaststellen van beste praktijken, processen en technische interoperabiliteit op belangrijke technologische gebieden zoals KI, het internet der dingen of blockchaintechnologie, zal de Commissie een versterkte, gecoördineerde aanpak ondersteunen.

Vandaag de dag wordt bij een aanzienlijk deel van de onderzoeken naar alle vormen van criminaliteit en terrorisme gebruikgemaakt van **versleutelde informatie**. Versleuteling is essentieel voor de digitale wereld, namelijk voor het beveiligen van digitale systemen en transacties en het beschermen van een aantal grondrechten, waaronder vrijheid van meningsuiting, privacy en gegevensbescherming. Indien versleuteling echter voor criminele doeleinden wordt gebruikt, kan zij de identiteit van criminelen verhullen en de inhoud van hun communicatie verbergen. De Commissie zal voor deze uitdagingen evenwichtige technische, operationele en juridische oplossingen onderzoeken en ondersteunen. Zij zal een aanpak bevorderen die de effectiviteit van de versleuteling voor de bescherming van de privacy en de beveiliging van de communicatie waarborgt, en tegelijkertijd een doeltreffend antwoord biedt op criminaliteit en terrorisme.

Bestrijding van terroristische online-inhoud

Om de onlineomgeving en de fysieke omgeving even veilig te maken, moet de **bestrijding van illegale online-inhoud** worden voortgezet. Bij steeds meer van de belangrijkste bedreigingen voor burgers, zoals terrorisme, extremisme en seksueel misbruik van kinderen, wordt gebruikgemaakt van de digitale omgeving. Daarom is concrete actie nodig, alsmede een kader om de eerbiediging van de grondrechten te waarborgen. Een essentiële eerste stap is dat de onderhandelingen over de voorgestelde wetgeving inzake terroristische online-inhoud[67] snel worden afgerond en dat wordt voorzien in de uitvoering daarvan. Intensievere vrijwillige samenwerking tussen de rechtshandhavingsinstanties en de particuliere sector in het **EU-internetforum** is ook cruciaal voor de bestrijding van het misbruik van het internet door terroristen, gewelddadige extremisten en criminelen. De EU-eenheid voor de melding van internetuitingen bij Europol zal een cruciale rol blijven spelen bij het toezicht op de activiteiten van terroristische onlinegroepen en op de maatregelen die door onlineplatformen worden getroffen[68], alsook bij de verdere ontwikkeling van het **EU-crisisprotocol**[69]. Daarnaast zal de Commissie blijven samenwerken met internationale partners; zo zal zij deelnemen aan het **Global Internet Forum to Counter Terrorism** om deze uitdagingen op mondiaal niveau aan te pakken. In het kader van het programma voor de versterking van het maatschappelijk middenveld zal verder worden gewerkt aan de ontwikkeling van alternatieve verhalen en een tegengeluid[70].

Om de verspreiding van illegale haatzaaiende uitlatingen op internet te voorkomen en te bestrijden, heeft de Commissie in 2016 de gedragscode voor de bestrijding van illegale haatzaaiende uitlatingen op internet ingevoerd, waarbij onlineplatformen vrijwillig toezegden om haatzaaiende uitlatingen te verwijderen. Uit de meest recente evaluatie blijkt dat de bedrijven 90% van de gemelde inhoud binnen 24 uur beoordelen en van de inhoud die als

[67] Voorstel voor een verordening ter voorkoming van de verspreiding van terroristische online-inhoud (COM(2018) 640 van 12 september 2018).

[68] Europol, november 2019.

[69] A Europe that protects – EU Crisis Protocol: responding to terrorist content online (oktober 2019).

[70] Dit hangt samen met het werk in het kader van het programma voor voorlichting over radicalisering (zie onder IV.3).

illegale haatzaaiende uitlating wordt beschouwd, 71% verwijderen. De platforms moeten echter transparanter handelen en meer feedback geven aan de gebruikers. Zij moeten zorgen voor een consistente beoordeling van de gemelde inhoud[71].

Het EU-internetforum zal ook de uitwisseling van gegevens over bestaande en in ontwikkeling zijnde technologie vergemakkelijken om de problemen in verband met online seksueel misbruik van kinderen aan te pakken. De aanpak van seksueel misbruik van kinderen online staat centraal in een nieuwe strategie om de **strijd tegen seksueel misbruik van kinderen op te voeren**[72], met als doel het gebruik van de op EU-niveau beschikbare instrumenten voor de bestrijding van deze misdrijven te maximaliseren. Ondernemingen moeten hun activiteiten om onlinemateriaal in verband met seksueel misbruik van kinderen op te sporen en te verwijderen, kunnen voortzetten. De door dit materiaal veroorzaakte schade vereist een kader met duidelijke en permanente verplichtingen om het probleem aan te pakken. In de strategie zal ook worden aangekondigd dat de Commissie sectorspecifieke wetgeving zal opstellen om seksueel misbruik van kinderen online doeltreffender te bestrijden, met volledige eerbiediging van de grondrechten.

Meer in het algemeen zullen in de komende wet inzake digitale diensten ook de regels inzake aansprakelijkheid en veiligheid voor digitale diensten worden verduidelijkt en aangescherpt en zullen belemmeringen voor maatregelen om illegale inhoud, goederen of diensten te bestrijden, worden weggenomen.

Daarnaast zal de Commissie blijven samenwerken met internationale partners en met het **Global Internet Forum to Counter Terrorism**, onder meer via het onafhankelijke adviescomité, om te bespreken hoe deze uitdagingen op mondiaal niveau kunnen worden aangepakt met behoud van de waarden en grondrechten van de EU. Ook nieuwe onderwerpen zoals algoritmes of onlinekansspelen zouden aan bod moeten komen[73].

Hybride dreigingen

De schaal en diversiteit van hybride dreigingen is vandaag de dag ongekend. Dit is ook tijdens de COVID-19-crisis gebleken: diverse statelijke en niet-statelijke actoren hebben getracht gebruik te maken van de pandemie, met name door de informatieomgeving te manipuleren en kerninfrastructuren op de proef te stellen. Hierdoor kan de sociale cohesie worden verzwakt en kan het vertrouwen in de EU-instellingen en de overheid in de lidstaten worden ondermijnd.

De EU-aanpak van hybride dreigingen is uiteengezet in het gezamenlijk kader van 2016[74] en de gezamenlijke mededeling van 2018 over het opbouwen van weerbaarheid tegen hybride bedreigingen[75]. De actie op EU-niveau wordt ondersteund met een omvangrijk instrumentarium dat betrekking heeft op de nexus interne-externe veiligheid en stoelt op een samenlevingsbrede aanpak en nauwe samenwerking met strategische partners, met name de NAVO en de G7. Tegelijk met deze strategie wordt een verslag over de uitvoering van de

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] EU-strategie voor doeltreffender bestrijding van seksueel misbruik van kinderen (COM(2020) 607).

[73] Terroristen maken voor uitwisselingen steeds vaker gebruik van de berichtensystemen van gokplatforms en jonge terroristen spelen met videospellen gewelddadige aanvallen na.

[74] Gezamenlijk kader ter bestrijding van hybride bedreigingen – een reactie van de Europese Unie (JOIN(2016) 18).

[75] Het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen (JOIN(2018) 16).

EU-aanpak van hybride bedreigingen gepubliceerd[76]. Op basis van de tegelijk met deze strategie gepresenteerde inventarisatie[77] zullen de diensten van de Commissie en de Europese Dienst voor extern optreden een **onlineplatform met toegangsbeperking** opzetten als referentie voor de lidstaten betreffende instrumenten en maatregelen op EU-niveau tegen hybride bedreigingen.

Hoewel de verantwoordelijkheid voor de bestrijding van hybride bedreigingen in de eerste plaats bij de lidstaten berust – vanwege de intrinsieke verbanden met het nationale veiligheids- en defensiebeleid – zijn er kwetsbaarheden waar alle lidstaten mee kampen en reiken sommige bedreigingen tot over de grenzen, bijvoorbeeld wanneer zij gericht zijn op grensoverschrijdende netwerken of infrastructuren. De Commissie en de hoge vertegenwoordiger zullen een EU-aanpak voor hybride bedreigingen vaststellen die de externe en interne dimensie naadloos samenbrengt en zowel de nationale als de EU-brede overwegingen in aanmerking neemt. Zo moet het volledige spectrum van de maatregelen worden bestreken: van vroegtijdige opsporing, analyse, bewustmaking, opbouw van weerbaarheid en preventie tot crisisrespons en beheersing van de gevolgen.

Omdat hybride bedreigingen constant evolueren, zal naast de versterkte uitvoering bijzondere aandacht uitgaan naar de **integratie van overwegingen inzake hybride dreigingen in de beleidsvorming**, om de dynamische ontwikkelingen bij te houden en ervoor te zorgen dat geen enkel potentieel relevant initiatief over het hoofd wordt gezien. De effecten van nieuwe initiatieven zullen ook worden beoordeeld uit het oogpunt van hybride bedreigingen. Dat geldt ook voor initiatieven op gebieden die tot nu toe buiten het kader tegen hybride bedreigingen vielen, zoals onderwijs, technologie en wetenschappelijk onderzoek. Deze aanpak kan baat hebben bij het werk dat is verricht met betrekking tot de conceptualisering van hybride bedreigingen, waardoor een volledig beeld wordt gegeven van de verschillende instrumenten die door tegenstanders kunnen worden ingezet[78]. Er moet op worden toegezien dat het besluitvormingsproces wordt geschraagd door regelmatige, alomvattende, op inlichtingen gebaseerde rapportage over de ontwikkeling van hybride bedreigingen. In hoge mate zal dit afhankelijk zijn van het inlichtingenwerk van de lidstaten en van de verdere versterking van de samenwerking op inlichtingengebied met de bevoegde diensten van de lidstaten via EU INTCEN.

Wat de ontwikkeling van het **situationeel bewustzijn** betreft, zullen de diensten van de Commissie en de Europese Dienst voor extern optreden de mogelijkheden onderzoeken om de informatiestromen uit verschillende bronnen (waaronder de lidstaten en EU-agentschappen zoals Enisa, Europol en Frontex) te stroomlijnen. De EU-Fusiecel voor analyse van hybride dreigingen blijft het contactpunt van de EU voor de beoordeling van hybride dreigingen. **Weerbaarheid opbouwen** is essentieel voor het voorkomen van hybride dreigingen en de bescherming ertegen. Daarom is het van cruciaal belang om de vooruitgang op dit gebied systematisch te volgen en objectief te meten. Allereerst moeten voor instellingen en instanties van de lidstaten en de EU per sector de uitgangsposities worden vastgesteld wat de

[76] Verslag over de uitvoering van het gezamenlijk kader ter bestrijding van hybride bedreigingen van 2016 en de gezamenlijke mededeling over het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen van 2018 (SWD(2020) 153).

[77] Inventarisatie van de maatregelen in verband met de versterking van de weerbaarheid en de bestrijding van hybride bedreigingen (SWD(2020) 152).

[78] *The Landscape of Hybrid Threats: A Conceptual Model* (JRC117280), gezamenlijk ontwikkeld door het Gemeenschappelijk Centrum voor onderzoek en het Kenniscentrum voor de bestrijding van hybride dreigingen.

weerbaarheid tegen hybride dreigingen betreft. Om de **paraatheid voor een crisisrespons op hybride dreigingen** op te voeren, moet tot slot het bestaande protocol, dat in het "EU Playbook"[79] van 2016 is opgenomen, worden herzien. Ten grondslag daaraan ligt een bredere toetsing en versterking van het EU-crisisbestrijdingssysteem, die momenteel wordt overwogen[80]. Daarmee wordt beoogd het effect van het optreden van de EU te maximaliseren, door alle sectorale responsen snel op elkaar af te stemmen en te zorgen voor een naadloze samenwerking met onze partners, in de eerste plaats de NAVO.

Belangrijkste maatregelen
• Zorgen dat de wetgeving inzake cybercriminaliteit wordt uitgevoerd en aan zijn doel beantwoordt • Een strategie voor doeltreffendere bestrijding van seksueel misbruik van kinderen • Voorstellen voor het opsporen en verwijderen van materiaal in verband met seksueel misbruik van kinderen • Een EU-aanpak van de bestrijding van hybride bedreigingen • Herziening van het operationeel EU-protocol voor de bestrijding van hybride bedreigingen (EU Playbook) • Beoordeling van maatregelen om de rechtshandhavingscapaciteit in digitale onderzoeken te versterken

3. Bescherming van Europeanen tegen terrorisme en georganiseerde misdaad

Terrorisme en radicalisering

De dreiging van terrorisme is in de EU nog steeds sterk. Hoewel de aanslagen in aantal zijn afgenomen, kunnen deze nog steeds een verwoestend effect hebben. Radicalisering kan ook leiden tot een sterkere polarisatie en aantasting van de sociale cohesie. De lidstaten behouden de primaire verantwoordelijkheid voor de bestrijding van terrorisme en radicalisering. De grens- en sectoroverschrijdende dimensies van de dreiging worden echter steeds sterker en vereisen verdere stappen in de samenwerking en coördinatie van de EU. Doeltreffende uitvoering van de EU-wetgeving inzake terrorismebestrijding, met inbegrip van beperkende maatregelen[81], is een prioriteit. Het is nog steeds de bedoeling om het mandaat van het Europees Openbaar Ministerie uit te breiden tot de vervolging van grensoverschrijdende terroristische misdrijven.

De bestrijding van terrorisme begint met het aanpakken van de onderliggende oorzaken. Polarisatie in de samenleving, echte of vermeende discriminatie en andere psychologische en sociologische factoren kunnen mensen kwetsbaarder maken voor een radicaal discours. De aanpak van **radicalisering** gaat in dit verband hand in hand met de bevordering van sociale

[79] Operationeel EU-protocol voor de bestrijding van hybride bedreigingen (EU Playbook) (SWD(2016) 227).

[80] De leden van de Europese Raad hebben na hun videoconferentie op 26 maart 2020 een verklaring aangenomen over de maatregelen die de EU heeft getroffen naar aanleiding van de COVID-19-uitbraak en de Commissie verzocht voorstellen te doen om een ambitieuzer en breder systeem voor crisisbeheersing in de EU tot stand te brengen.

[81] Ter bestrijding van het terrorisme heeft de Raad beperkende maatregelen tegen IS en Al Qaida vastgesteld, alsmede specifieke beperkende maatregelen tegen bepaalde personen en entiteiten. De EU-sanctiekaart (https://www.sanctionsmap.eu/#/main) geeft een overzicht van alle beperkende maatregelen.

cohesie op lokaal, nationaal en Europees niveau. De afgelopen tien jaar zijn tal van ingrijpende initiatieven en beleidsmaatregelen ontwikkeld, met name via het netwerk voor voorlichting over radicalisering en het initiatief "EU-steden tegen radicalisering"[82]. We moeten nu maatregelen overwegen om het beleid, de initiatieven en de fondsen van de EU te stroomlijnen om radicalisering tegen te gaan. Met dergelijke maatregelen kunnen we de ontwikkeling van capaciteiten en vaardigheden ondersteunen, de samenwerking verbeteren, de kennisbasis versterken en bijdragen tot de evaluatie van de vorderingen, met de medewerking van alle belanghebbenden, onder wie eerstelijnswerkers, beleidsmakers en de academische wereld[83]. Zachte beleidsgebieden, zoals onderwijs, cultuur, jeugd en sport, zouden radicalisering kunnen helpen voorkomen door risicojongeren kansen te bieden en voor grotere cohesie in de EU te zorgen[84]. Prioritaire gebieden zijn onder meer het werk op het gebied van vroegtijdige opsporing en risicobeheersing, de opbouw van veerkracht, stimuleren van deradicalisering, alsmede rehabilitatie en re-integratie in de samenleving.

Terroristen hebben pogingen gedaan om **chemische, biologische, radiologische en nucleaire** (CBRN)[85] materialen aan te kopen en als wapen in te zetten, en de kennis en het vermogen te ontwikkelen om deze te gebruiken[86]. Het potentieel van CBRN-aanslagen wordt in terroristische propaganda sterk benadrukt. Gezien de potentiële schade is daar bijzondere aandacht voor nodig. Op basis van de aanpak die wordt gehanteerd om de toegang tot precursoren voor explosieven te reguleren, zal de Commissie onderzoek doen naar het beperken van de toegang tot bepaalde gevaarlijke chemische stoffen die kunnen worden gebruikt om aanslagen te plegen. De ontwikkeling van de capaciteit van de EU inzake civiele bescherming (rescEU) op CBRN-gebied is eveneens essentieel. Samenwerking met derde landen is ook van belang om een gemeenschappelijke cultuur van CBRN-veiligheid en -beveiliging te bevorderen, die ten volle gebruikmaakt van de CBRN-kenniscentra van de EU. Deze samenwerking omvat nationale beoordelingen van lacunes en risico's, steun voor nationale en regionale CBRN-actieplannen, uitwisselingen van goede praktijken en activiteiten inzake CBRN-capaciteitsopbouw.

De EU heeft de meest geavanceerde wetgeving ter wereld ontwikkeld om de toegang tot **precursoren voor explosieven**[87] te beperken en verdachte, op het vervaardigen van geïmproviseerde explosieven gerichte transacties op te sporen. Maar de dreiging die uitgaat van zelfgemaakte explosieven, die gebruikt zijn bij diverse aanslagen in de EU[88], is nog steeds groot. Allereerst moet worden toegezien op de uitvoering van de voorschriften en moet worden voorkomen dat de online-omgeving de mogelijkheid biedt om controles te omzeilen.

---

[82] Het proefproject "EU-steden tegen radicalisering" heeft een tweeledige doelstelling: uitwisseling van expertise tussen steden in de EU bevorderen en feedback verzamelen over de beste manier om lokale gemeenschappen op EU-niveau te ondersteunen.

[83] Bijvoorbeeld financiering in het kader van het Europees veiligheidsfonds en het burgerschapsprogramma.

[84] EU-acties zoals de virtuele uitwisselingen in het kader van Erasmus+ en e-twinning.

[85] De afgelopen twee jaar zijn er bijvoorbeeld verschillende gevallen geweest in Europa (Frankrijk, Duitsland, Italië) en elders (Tunesië, Indonesië) waarbij biologische agentia werden gebruikt (meestal plantaardige toxinen).

[86] De Raad heeft beperkende maatregelen vastgesteld tegen de proliferatie en het gebruik van chemische wapens.

[87] Chemische stoffen die kunnen worden misbruikt voor de vervaardiging van zelfgemaakte explosieven. Deze worden gereguleerd door Verordening (EU) 2019/1148 over het op de markt brengen en het gebruik van precursoren voor explosieven.

[88] Dergelijke verwoestende aanslagen zijn onder andere gepleegd in Oslo (2011), Parijs (2015), Brussel (2016) en Manchester (2017). Bij een aanslag met een zelfgemaakt explosief in Lyon (2019) raakten 13 mensen gewond.

Ook de effectieve vervolging van personen die terroristische misdrijven hebben gepleegd, onder wie **buitenlandse terroristische strijders** die zich momenteel in Syrië en Irak bevinden, is een belangrijk onderdeel van het terrorismebestrijdingsbeleid. Hoewel deze zaken in de eerste plaats door de lidstaten worden behandeld, kunnen de lidstaten door EU-coördinatie en -steun worden geholpen bij de aanpak van gemeenschappelijke uitdagingen. De maatregelen die momenteel worden genomen om de wetgeving inzake grensbeveiliging[89] volledig uit te voeren en ten volle gebruik te maken van alle relevante EU-databanken voor het uitwisselen van informatie over bekende verdachten, zijn een belangrijke onderdeel daarvan. Naast de identificatie van personen met een hoog risico is een integratie- en rehabilitatiebeleid nodig. Samenwerking tussen beroepsgroepen, onder meer met gevangenis- en reclasseringspersoneel, versterkt de juridische kennis van de wijze waarop mensen radicaliseren tot gewelddadig extremisme, evenals de aanpak van de justitiële sector met betrekking tot strafoplegging en alternatieven voor detentie.

Het probleem van buitenlandse terroristische strijders is een goed voorbeeld van het verband tussen interne en **externe veiligheid**. Samenwerking op het gebied van terrorismebestrijding en het voorkomen en bestrijden van radicalisering en gewelddadig extremisme is van cruciaal belang voor de veiligheid binnen de EU[90]. Er moeten verdere stappen worden gezet om partnerschappen voor terrorismebestrijding en samenwerking met buurlanden en andere landen te ontwikkelen, waarbij gebruik moet worden gemaakt van de expertise van het netwerk van terrorismebestrijdings-/beveiligingsdeskundigen in de EU. Het gezamenlijke actieplan inzake terrorismebestrijding voor de Westelijke Balkan is een goed voorbeeld van dergelijke gerichte samenwerking. Met name moet ernaar worden gestreefd het vermogen van de partnerlanden om buitenlandse terroristische strijders te identificeren en te lokaliseren, te ondersteunen. De EU zal ook de multilaterale samenwerking blijven bevorderen, in overleg met de leidende mondiale actoren op dit gebied, zoals de Verenigde Naties, de NAVO, de Raad van Europa, Interpol en de OVSE. Zij zal ook samenwerken met het mondiaal forum voor terrorismebestrijding en de wereldwijde coalitie tegen IS, en met relevante actoren uit het maatschappelijk middenveld. De instrumenten van het externe beleid van de Unie, waaronder ontwikkeling en samenwerking, spelen ook een belangrijke rol bij het samen met derde landen voorkomen van terrorisme en piraterij. Internationale samenwerking is ook van essentieel belang voor het afsnijden van alle bronnen van **terrorismefinanciering**, bijvoorbeeld via de Financial Action Task Force.

Georganiseerde misdaad

Georganiseerde misdaad leidt tot enorme economische kosten en het verlies van levens. Het economische verlies als gevolg van georganiseerde misdaad en corruptie is wel geschat op 218 tot 282 miljard EUR per jaar[91]. Er werden in 2017 in Europa meer dan 5 000 georganiseerde criminele groepen onderzocht: een stijging van 50% ten opzichte van 2013[92]. De georganiseerde misdaad opereert in toenemende mate grensoverschrijdend, onder meer vanuit de onmiddellijke buurlanden van de EU; de bestrijding ervan vereist derhalve

[89] Met inbegrip van het nieuwe mandaat van het Europees Grens- en kustwachtagentschap (Frontex).

[90] In de conclusies van de Raad van 16 juni 2020 wordt gewezen op de noodzaak EU-burgers te beschermen tegen alle vormen van terrorisme en gewelddadig extremisme, ongeacht de oorsprong ervan, en het externe optreden van de EU ter bestrijding van terrorisme en het optreden van de EU op een aantal prioritaire geografische en thematische gebieden te versterken.

[91] In termen van het bruto binnenlands product (bbp); verslag van Europol: *Does crime still pay? – Criminal asset recovery in the EU*, 2016.

[92] Europol, Serious and Organised Threat Assessment (SOCTA), 2013 en 2017.

intensievere operationele samenwerking en informatie-uitwisseling met partners in de buurlanden.

Er ontstaan nieuwe uitdagingen, nu de criminaliteit online gaat: de COVID-19-pandemie leidde tot een enorme toename van onlinezwendel met betrekking tot kwetsbare groepen, terwijl gezondheids- en sanitaire producten het doelwit werden van diefstallen en inbraken[93]. De EU moet haar activiteiten ter bestrijding van georganiseerde misdaad opvoeren, ook op internationaal niveau, en meer instrumenten inzetten om het bedrijfsmodel van de georganiseerde misdaad te vernietigen. Bestrijding van georganiseerde misdaad vereist ook nauwe samenwerking met lokale en regionale overheden en met het maatschappelijk middenveld, die belangrijke partners zijn op het gebied van criminaliteitspreventie en bij het verlenen van bijstand en ondersteuning aan slachtoffers. De noodzaak van samenwerking is bijzonder groot bij overheden in grensregio's. Deze werkzaamheden zullen worden ondergebracht in een **agenda voor de bestrijding van georganiseerde misdaad**.

Van de georganiseerde criminele groepen die in de EU actief zijn, houdt meer dan een derde zich bezig met de illegale handel in drugs en de productie en distributie ervan. Drugsverslaving leidde in 2019 tot meer dan achtduizend sterfgevallen door overdosis in de EU. **Drugshandel** is voor het merendeel grensoverschrijdend van aard, en de winsten ervan komen voor een groot deel in de legale economie terecht[94]. Met een nieuwe Europese drugsagenda[95] worden de inspanningen van de EU en de lidstaten om de vraag naar en het aanbod van drugs terug te dringen, versterkt. Er zullen gezamenlijke maatregelen worden vastgesteld om dit gemeenschappelijke probleem aan te pakken en de dialoog en de samenwerking tussen de EU en de externe partners over drugskwesties zullen worden versterkt. Na een evaluatie van het Europees Waarnemingscentrum voor drugs en drugsverslaving zal de Commissie beoordelen of het mandaat van het Waarnemingscentrum moet worden aangepast om aan de nieuwe uitdagingen het hoofd te kunnen bieden.

Georganiseerde criminele groepen en terroristen zijn ook actief betrokken bij de handel in **illegale vuurwapens**. Tussen 2009 en 2018 vonden in Europa 23 grote schietpartijen plaats, waarbij meer dan 340 mensen om het leven kwamen[96]. Vuurwapens worden vaak via de buurlanden naar de EU gesmokkeld[97]. Dat betekent dat de coördinatie en de samenwerking binnen de EU en met de internationale partners, met name Interpol, moeten worden versterkt om de verzameling van informatie en de verslaglegging over de inbeslagname van vuurwapens te harmoniseren. Het is ook essentieel de traceerbaarheid van wapens, onder meer op internet, te verbeteren en te zorgen voor informatie-uitwisseling tussen vergunningverlenende instanties en rechtshandhavingsinstanties. De Commissie werkt aan een nieuw **EU-actieplan tegen de illegale handel in vuurwapens**[98] en zal ook nagaan of de

[93] Europol 2020.
[94] EMCDDA en Europol: EU Drug Markets Report 2019 (november 2019).
[95] EU-drugsagenda en actieplan 2021–2025 (COM(2020) 606).
[96] Vlaams Vredesinstituut, Armed to kill (oktober 2019).
[97] Sinds 2002 financiert de EU de strijd tegen de verspreiding van en de handel in handvuurwapens en lichte wapens in de regio; zij heeft met name het Zuidoost-Europese vuurwapendeskundigennetwerk (SEEFEN) gefinancierd. Sinds 2019 worden de partners van de Westelijke Balkan volledig betrokken bij de prioriteit inzake vuurwapens van het Europees multidisciplinair platform tegen criminaliteitsdreiging (Empact).
[98] COM(2020) 608.

regels inzake uitvoervergunningen en invoer- en doorvoermaatregelen voor vuurwapens nog aan hun doel beantwoorden[99].

Criminele organisaties behandelen migranten en mensen die internationale bescherming nodig hebben als handelswaar. De binnenkomst van irreguliere migranten in de EU wordt voor 90% gefaciliteerd door criminele netwerken[100]. Migrantensmokkel is ook vaak verweven met andere vormen van georganiseerde criminaliteit, met name mensenhandel[101]. Naast de enorme prijs van mensenhandel uit menselijk oogpunt, schat Europol dat de jaarlijkse winst voor alle vormen van uitbuiting door mensenhandel wereldwijd 29,4 miljard EUR bedraagt. Mensenhandel is een transnationaal delict dat wordt gevoed door de illegale vraag van binnen en buiten de EU en invloed heeft op alle EU-lidstaten. Gezien de slechte staat van dienst op het gebied van de identificatie, de vervolging en de veroordeling van deze delicten is een nieuwe aanpak vereist om de actie op te voeren. Een nieuwe **alomvattende aanpak van mensenhandel** zal verschillende beleidsmaatregelen bijeenbrengen. Daarnaast zal de Commissie een **nieuw EU-actieplan tegen migrantensmokkel** voor de periode 2021–2025 presenteren. Beide onderdelen daarvan leggen het accent op het bestrijden van criminele netwerken, het stimuleren van samenwerking en het ondersteunen van de werkzaamheden op het gebied van rechtshandhaving.

Misdaadorganisaties – en terroristen – zoeken ook kansen op andere gebieden, met name gebieden die hoge winsten opleveren tegen een laag risico, zoals **milieucriminaliteit**. Illegale jacht op en handel in wilde dieren, illegale mijnbouw, illegale houtkap en illegale verwijdering en vervoer van afval zijn op drie na de meest winstgevende criminele activiteiten ter wereld[102]. Er is ook sprake van criminele exploitatie van regelingen voor de handel in emissierechten en systemen voor energiecertificaten, en van misbruik van de financiering voor ecologische veerkracht en duurzame ontwikkeling. Naast het bevorderen van de maatregelen die de EU, de lidstaten en de internationale gemeenschap treffen om de inspanningen ter bestrijding van milieucriminaliteit[103] op te voeren, beoordeelt de Commissie of de richtlijn milieucriminaliteit[104] nog steeds geschikt is voor het beoogde doel. De **illegale handel in cultuurgoederen** is ook een van de meest lucratieve criminele activiteiten geworden, en dient steeds vaker als bron van financiering voor terroristen en misdaadorganisaties. Er moeten stappen worden ondernomen om de online- en offlinetraceerbaarheid van cultuurgoederen in de interne markt te verbeteren en om beter samen te werken met derde landen waar cultuurgoederen worden geplunderd. Ook moet actieve ondersteuning worden geboden aan rechtshandhavingsinstanties en academische gemeenschappen.

Economische en financiële delicten zijn zeer complex, maar benadelen elk jaar miljoenen burgers en duizenden bedrijven in de EU. Het bestrijden van fraude is essentieel en vereist actie op EU-niveau. Samen met Eurojust, het Europees Openbaar Ministerie en het Europees Bureau voor fraudebestrijding, steunt Europol de lidstaten en de EU bij de bescherming van de economische en financiële markten en de bescherming van het geld van de Europese belastingbetaler. Het Europees Openbaar Ministerie zal eind 2020 volledig operationeel

[99] Verordening (EU) nr. 258/2012 tot uitvoering van artikel 10 van het Protocol van de Verenigde Naties tegen de illegale vervaardiging van en handel in vuurwapens.
[100] Bron: Europol.
[101] Europol: EMSC, vierde jaarverslag.
[102] UNEP-INTERPOL Rapid Response Assessment: *The Rise of Environmental Crime*, juni 2016.
[103] De Europese Green Deal (COM(2019) 640 final).
[104] Richtlijn 2008/99/EG inzake de bescherming van het milieu door middel van het strafrecht.

worden. Het zal strafbare feiten die de EU-begroting schaden, zoals fraude, corruptie en witwassen, onderzoeken, vervolgen en voor de rechter brengen. Ook grensoverschrijdende btw-fraude, die de belastingbetaler tenminste 50 miljard EUR per jaar kost, zal door het EOM worden aangepakt.

De Commissie zal ook steun verlenen aan de ontwikkeling van expertise en van een wetgevingskader inzake nieuwe risico's, zoals cryptoactiva en nieuwe betalingssystemen. In het bijzonder zal de Commissie kijken naar de respons op de opkomst van cryptovaluta zoals bitcoin en het effect van deze nieuwe technologieën op de wijze waarop financiële activa in omloop worden gebracht, gewisseld, gedeeld en uitgegeven.

Voor illegaal geld zou in de Europese Unie een nultolerantiebeleid moeten gelden. In de loop van dertig jaar heeft de EU een solide regelgevingskader ontwikkeld voor het voorkomen en bestrijden van **witwassen** en terrorismefinanciering, waarbij de bescherming van persoonsgegevens volledig in acht wordt genomen. Er is echter een groeiende consensus dat het huidige kader aanzienlijk beter moet worden uitgevoerd. Er zijn grote verschillen in de manier waarop het wordt toegepast en de ernstige tekortkomingen bij de handhaving van de regels moeten worden verholpen. Zoals in het actieplan van mei 2020[105] is uiteengezet, wordt er momenteel gewerkt aan de beoordeling van de mogelijkheden om het EU-kader voor de bestrijding van witwassen en terrorismefinanciering te versterken. Zo zou onderzoek kunnen worden gedaan naar de koppeling van nationale centrale registers van bankrekeningen, waardoor de toegang tot financiële informatie voor financiële-inlichtingeneenheden en de bevoegde autoriteiten aanzienlijk zou kunnen worden versneld.

De **winsten van misdaadorganisaties** in de EU worden geschat op 110 miljard EUR per jaar. De huidige respons omvat ook geharmoniseerde wetgeving inzake confiscatie en ontneming van vermogensbestanddelen[106], die als doel heeft de bevriezing en confiscatie van criminele vermogensbestanddelen in de EU te verbeteren en het wederzijdse vertrouwen en doeltreffende grensoverschrijdende samenwerking tussen de lidstaten te bevorderen. Van de winsten wordt echter slechts zo'n 1% geconfisqueerd[107], waardoor misdaadorganisaties kunnen investeren in expansie van hun criminele activiteiten en in de legale economie kunnen infiltreren; met name kleine en middelgrote ondernemingen, die moeilijk aan krediet kunnen komen, zijn een belangrijk doelwit voor witwassers. De Commissie zal de uitvoering van de wetgeving[108] analyseren en de eventuele noodzaak beoordelen van verdere gemeenschappelijke regels, met inbegrip van confiscatie zonder veroordeling. De bureaus voor de ontneming van vermogensbestanddelen[109], die een belangrijke taak hebben in het proces voor de ontneming van vermogensbestanddelen, kunnen ook worden uitgerust met betere instrumenten om activa in de EU sneller te identificeren en te traceren, zodat de confiscatiepercentages hoger kunnen worden.

---

[105] Actieplan voor de preventie van witwassen en financieren van terrorisme (C(2020) 2800).

[106] Volgens de EU-wetgeving moeten in alle lidstaten bureaus voor de ontneming van vermogensbestanddelen gevestigd zijn.

[107] Verslag *Ontneming en confiscatie van vermogensbestanddelen: zorgen dat misdaad niet loont* (COM(2020) 217).

[108] Richtlijn 2014/42/EU betreffende de bevriezing en confiscatie van hulpmiddelen en opbrengsten van misdrijven in de Europese Unie.

[109] Besluit 2007/845/JBZ van de Raad betreffende de samenwerking tussen de nationale bureaus voor de ontneming van vermogensbestanddelen op het gebied van de opsporing en de identificatie van opbrengsten van misdrijven of andere vermogensbestanddelen die hun oorsprong vinden in misdrijven.

Er is een sterk verband tussen georganiseerde misdaad en **corruptie**. Naar schatting kost alleen al corruptie de EU-economie 120 miljard EUR per jaar[110]. Voorkoming en bestrijding van corruptie blijven onderworpen aan regelmatige monitoring in het kader van het rechtsstaatmechanisme en het Europees semester. Het Europees semester heeft een beoordeling verricht van uitdagingen in de strijd tegen corruptie, zoals openbare aanbestedingen, het openbaar bestuur, het ondernemingsklimaat en de gezondheidszorg. Het nieuwe jaarlijkse verslag van de Commissie over de rechtsstaat behandelt ook de strijd tegen corruptie. Zo wordt een preventieve dialoog met de nationale autoriteiten en belanghebbenden op EU- en nationaal niveau mogelijk gemaakt. Maatschappelijke organisaties kunnen ook een belangrijke rol spelen door het optreden van de overheid ter voorkoming en bestrijding van georganiseerde misdaad en corruptie te stimuleren. Het zou nuttig zijn de desbetreffende groepen samen te brengen in een gemeenschappelijk forum. Vanwege hun grensoverschrijdende aard zijn ook samenwerking met en bijstand aan naburige EU-regio's bij de aanpak van georganiseerde criminaliteit en corruptie essentieel.

Belangrijkste maatregelen

- Agenda inzake terrorismebestrijding voor de EU, met hernieuwde maatregelen tegen radicalisering in de EU
- Nieuwe samenwerking tegen terrorisme met belangrijke derde landen en internationale organisaties
- Agenda voor de bestrijding van georganiseerde misdaad, waaronder mensenhandel
- EU-agenda en -actieplan inzake drugs voor 2021–2025
- Evaluatie van het Europees Waarnemingscentrum voor drugs en drugsverslaving
- EU-actieplan 2020–2025 inzake illegale vuurwapenhandel
- Herziening van de wetgeving inzake bevriezing en confiscatie en inzake de bureaus voor de ontneming van vermogensbestanddelen
- Beoordeling van de richtlijn milieucriminaliteit
- EU-actieplan tegen migrantensmokkel 2021–2025

4. Een krachtig Europees veiligheidsecosysteem

Alle geledingen van de samenleving zouden gezamenlijk moeten streven naar een echte en doeltreffende veiligheidsunie. Bij de opbouw van de paraatheid en de weerbaarheid van allen en met name van de meest kwetsbaren, slachtoffers en getuigen, moeten overheden, rechtshandhavingsinstanties, de particuliere sector, het onderwijs en de burgers zelf worden ingeschakeld, toegerust en met elkaar in contact gebracht worden.

Alle beleidsmaatregelen hebben een veiligheidsdimensie nodig en de EU kan een bijdrage leveren op alle niveaus. Bij de mensen thuis is huiselijk geweld een van de ernstigste veiligheidsrisico's. Eén op de vier vrouwen in de EU heeft te maken gehad met partnergeweld[111]. De toetreding van de EU tot het Verdrag van Istanbul inzake het voorkomen en bestrijden van geweld tegen vrouwen en huiselijk geweld heeft nog steeds een hoge

[110] De totale economische kosten van corruptie zijn lastig in te schatten, hoewel daar wel een poging toe is ondernomen door organen zoals de Internationale Kamer van Koophandel, Transparency International, het Global Compact van de VN en het World Economic Forum, waaruit is gebleken dat er bij 5% van het mondiale bbp sprake is van corruptie.

[111] Een Unie van gelijkheid: strategie voor gendergelijkheid 2020–2025 (COM(2020) 152).

prioriteit. Indien de onderhandelingen geblokkeerd blijven, zal de Commissie andere maatregelen nemen om dezelfde doelstellingen te bereiken als het verdrag, en tevens voorstellen om geweld tegen vrouwen toe te voegen aan de lijst van in het Verdrag genoemde vormen van criminaliteit.

Samenwerking en informatie-uitwisseling

Een van de meest cruciale bijdragen die de EU kan leveren aan de bescherming van de burgers, is degenen die voor onze veiligheid moeten zorgen, helpen om goed samen te werken. Samenwerking en informatie-uitwisseling zijn de krachtigste instrumenten om criminaliteit en terrorisme te bestrijden en gerechtigheid na te streven. Met het oog op efficiëntie moet doelgericht en tijdig te werk worden gegaan. Met het oog op vertrouwen moeten gemeenschappelijke waarborgen en controles worden toegepast.

Er zijn een aantal EU-instrumenten en sectorspecifieke strategieën[112] opgezet om de **operationele samenwerking op het gebied van rechtshandhaving** tussen de lidstaten verder te ontwikkelen. Een van de belangrijkste EU-instrumenten ter ondersteuning van de samenwerking op het gebied van rechtshandhaving tussen de lidstaten is het Schengeninformatiesysteem, dat wordt gebruikt om gegevens over gezochte en vermiste personen en voorwerpen in realtime uit te wisselen. De resultaten hebben geleid tot de arrestatie van criminelen, de inbeslagname van drugs en de redding van potentiële slachtoffers[113]. De samenwerking kan echter nog worden verbeterd door de beschikbare instrumenten te stroomlijnen en te moderniseren. Het rechtskader van de EU dat de operationele samenwerking op het gebied van rechtshandhaving regelt, is al dertig jaar oud. Het is een complex web van bilaterale overeenkomsten tussen de lidstaten, waarvan er vele inmiddels achterhaald zijn of nauwelijks worden toegepast. Deze situatie leidt tot het gevaar van versnippering. In kleinere of niet aan zee grenzende landen moeten rechtshandhavingsfunctionarissen die over de grenzen heen actief zijn, operationele acties uitvoeren volgens, in sommige gevallen, wel zeven verschillende regelgevingen: het resultaat is dat sommige operaties, zoals achtervolging van verdachten over de binnengrenzen, gewoonweg achterwege blijven. Ook de operationele samenwerking op het gebied van nieuwe technologieën, zoals drones, valt niet onder het huidige EU-kader.

De operationele effectiviteit kan worden ondersteund met specifieke samenwerking op het gebied van rechtshandhaving, die ook kan bijdragen tot belangrijke steun voor andere beleidsdoelstellingen, zoals het verstrekken van beveiligingsinput voor de nu vereiste beoordeling van buitenlandse directe investeringen. De Commissie zal nagaan hoe dit kan worden ondersteund met een code voor politiële samenwerking. De rechtshandhavingsinstanties van de lidstaten maken steeds meer gebruik van ondersteuning en expertise op EU-niveau. EU INTCEN speelt een sleutelrol door het bevorderen van de uitwisseling van strategische inlichtingen tussen de inlichtingen- en veiligheidsdiensten van de lidstaten die aan de EU-instellingen inlichtingengestuurd situationeel bewustzijn bieden[114]. Ook **Europol** kan een sleutelrol spelen door de samenwerking met derde landen ter bestrijding van criminaliteit en terrorisme uit te breiden in goede samenhang met andere externe beleidsmaatregelen en instrumenten van de EU. Europol kent momenteel echter een

[112] Zoals het actieplan van de EU-strategie voor maritieme veiligheid, dat belangrijke resultaten heeft opgeleverd met de samenwerking tussen de betrokken EU-agentschappen op het gebied van kustwachttaken.

[113] De strijd van de EU tegen de georganiseerde misdaad in 2019 (Raad, 2020).

[114] EU INTCEN fungeert als enige toegangspoort voor de inlichtingen- en veiligheidsdiensten van de lidstaten met het oog op het verstrekken van inlichtingengestuurd situationeel bewustzijn aan de EU.

aantal ernstige beperkingen (met name wat betreft de rechtstreekse uitwisseling van persoonsgegevens met particuliere entiteiten) waardoor het de lidstaten niet doeltreffend kan ondersteunen bij de bestrijding van terrorisme en criminaliteit. Het mandaat van Europol wordt thans geëvalueerd om na te gaan hoe het zodanig kan worden verbeterd dat het agentschap zijn taken volledig kan uitvoeren. In dit verband moeten de bevoegde autoriteiten op EU-niveau (zoals OLAF, Europol, Eurojust en het Europees Openbaar Ministerie) ook nauwer samenwerken en de uitwisseling van informatie verbeteren.

Een andere belangrijke schakel is de verdere ontwikkeling van **Eurojust** om de synergie tussen samenwerking op het gebied van rechtshandhaving en justitiële samenwerking te maximaliseren. De EU zou ook baat hebben bij een grotere strategische coherentie: **Empact**[115], de EU-beleidscyclus voor zware en internationale georganiseerde criminaliteit, biedt de autoriteiten een op strafrechtelijke inlichtingen gebaseerde methodologie voor de gezamenlijke aanpak van de belangrijkste criminaliteitsdreigingen voor de EU. Empact heeft de afgelopen tien jaar tot belangrijke operationele resultaten[116] geleid. Op basis van de ervaring van de betrokkenen moet het bestaande mechanisme worden gestroomlijnd en vereenvoudigd om de meest urgente en evoluerende criminele dreigingen beter aan te pakken in het kader van een nieuwe beleidscyclus voor 2022–2025.

Voor de dagelijkse werkzaamheden in verband met de vervolging van misdrijven is het essentieel om tijdig over alle relevante **informatie** te kunnen beschikken. Ondanks de ontwikkeling van nieuwe databanken op EU-niveau inzake veiligheid en grensbeheer is nog steeds veel informatie alleen in nationale databanken opgenomen of wordt deze uitgewisseld buiten de EU-databanken om. Dit leidt tot een aanzienlijke extra werklast, vertraging en een verhoogd risico dat belangrijke informatie niet wordt benut. Betere, snellere en vereenvoudigde processen, waarbij alle onderdelen van de veiligheidssector worden betrokken, zouden betere resultaten opleveren. Alleen met de juiste instrumenten kan de uitwisseling van informatie tot het gewenste doel leiden, namelijk doeltreffende vervolging van strafbare feiten, met de nodige waarborgen dat bij de uitwisseling van gegevens de wetgeving inzake gegevensbescherming en de grondrechten worden nageleefd. In het licht van de ontwikkelingen op het gebied van technologie, forensische wetenschap en gegevensbescherming en de gewijzigde operationele behoeften, zou de EU kunnen overwegen of er met het oog op strafrechtelijk onderzoek behoefte is aan modernisering van instrumenten als de **Prümbesluiten van 2008** voor geautomatiseerde uitwisseling van DNA-, vingerafdruk- en kentekengegevens, door de geautomatiseerde uitwisseling mogelijk te maken van nog andere soorten gegevens die reeds beschikbaar zijn in strafrechtelijke of andere databanken van de lidstaten. Ook zal de Commissie nagaan of het mogelijk is politiegegevens uit te wisselen om te achterhalen of er in andere lidstaten politiegegevens over een persoon voorhanden zijn en om de toegang tot deze gegevens, zodra deze zijn geïdentificeerd, te vergemakkelijken, met alle nodige waarborgen.

Dankzij **informatie over reizigers** zijn de grenscontroles verbeterd, is irreguliere migratie verminderd en is bijgedragen aan de identificatie van personen die veiligheidsrisico's met zich meebrengen. API-gegevens zijn biografische gegevens van alle passagiers, die de luchtvaartmaatschappijen bij het inchecken verzamelen en voorafgaand aan de vlucht aan de grenscontroleautoriteiten op de plaats van bestemming verstrekken. De herziening van het

[115] Empact staat voor European Multidisciplinary Platform Against Criminal Threats (Europees multidisciplinair platform tegen criminaliteitsdreiging).

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

rechtskader[117] zou een doeltreffender gebruik van de informatie mogelijk maken, waarbij de naleving van de wetgeving inzake gegevensbescherming wordt gewaarborgd en de doorstroming van de passagiers wordt vergemakkelijkt. Persoonsgegevens van passagiers (PNR) zijn gegevens die de passagiers bij het boeken van een vlucht verstrekken. De uitvoering van de PNR-richtlijn[118] is essentieel, en de Commissie zal deze blijven ondersteunen en handhaven. Bovendien zal de Commissie, bij wijze van tussentijdse maatregel, de huidige aanpak van de **doorgifte van PNR-gegevens aan derde landen** evalueren.

Justitiële samenwerking is een noodzakelijke aanvulling op de inspanningen van de politie ter bestrijding van grensoverschrijdende criminaliteit. De justitiële samenwerking is de afgelopen twintig jaar ingrijpend veranderd. Organen zoals het **Europees Openbaar Ministerie** en **Eurojust** moeten kunnen beschikken over de middelen om optimaal te functioneren of moeten worden versterkt. De samenwerking tussen justitiële beroepsbeoefenaars zou ook kunnen worden verbeterd door verdere maatregelen te nemen voor de wederzijdse erkenning van rechterlijke beslissingen, justitiële opleiding en informatie-uitwisseling. Het doel moet zijn het wederzijds vertrouwen tussen rechters en openbare aanklagers te vergroten, omdat dit essentieel is voor een soepel functioneren van grensoverschrijdende procedures. Door het gebruik van **digitale technologieën** kan ook de efficiëntie van onze rechtsstelsels worden verbeterd. Er wordt gewerkt aan het opzetten van een nieuw systeem voor digitale uitwisseling, dat gebruikt zal worden voor de verzending van Europese onderzoeksbevelen, verzoeken om wederzijdse rechtshulp en de daarmee samenhangende communicatie tussen de lidstaten, met ondersteuning door Eurojust. De Commissie zal in samenwerking met de lidstaten de uitrol van de noodzakelijke IT-systemen op nationaal niveau versnellen.

Internationale samenwerking is ook cruciaal voor doeltreffende rechtshandhaving en justitiële samenwerking. Bilaterale overeenkomsten met belangrijke partners spelen een grote rol bij het verkrijgen van informatie en bewijsmateriaal dat van buiten de EU afkomstig is. **Interpol**, een van de grootste intergouvernementele criminele politieorganisaties, speelt een belangrijke rol. De Commissie zal nagaan hoe de samenwerking met Interpol kan worden versterkt, bijvoorbeeld door middel van mogelijke toegang tot de databanken van Interpol en verbetering van de operationele en strategische samenwerking. De rechtshandhavingsinstanties in de EU doen ook een beroep op belangrijke partnerlanden om criminelen en terroristen op te sporen en te onderzoeken. De **veiligheidspartnerschappen tussen de EU en derde landen** zouden kunnen worden versterkt om beter te kunnen samenwerken bij de bestrijding van gemeenschappelijke dreigingen zoals terrorisme, georganiseerde misdaad, cybercriminaliteit, seksueel misbruik van kinderen en mensenhandel. Bij zo'n aanpak zou worden uitgegaan van gemeenschappelijke veiligheidsbelangen en permanente samenwerkings- en veiligheidsdialogen.

Net als de uitwisseling van informatie kan ook de uitwisseling van expertise bijzonder waardevol zijn voor het versterken van de paraatheid van de rechtshandhavingsinstanties ten aanzien van **niet-traditionele bedreigingen**. De Commissie zal niet alleen de uitwisseling van beste praktijken aanmoedigen, maar ook de mogelijkheid onderzoeken om een **coördinatiemechanisme op EU-niveau voor de politiediensten** op te zetten, bedoeld voor

[117] Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders om passagiersgegevens door te geven.

[118] Richtlijn (EU) 2016/681 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

situaties van overmacht, zoals pandemieën. De pandemie heeft ook aangetoond dat digitaal buurtpolitiewerk, vergezeld van juridische kaders om onlinepolitiewerk te vergemakkelijken, van fundamenteel belang zal zijn voor de bestrijding van criminaliteit en terrorisme. Partnerschappen tussen politie en gemeenschappen, zowel offline als online, kunnen criminaliteit voorkomen en de gevolgen van georganiseerde misdaad, radicalisering en terroristische activiteiten beperken. Een goede verbinding tussen het politiewerk op lokaal, regionaal, nationaal en EU-niveau is een belangrijke succesfactor voor de EU-veiligheidsunie in haar geheel.

De bijdrage van sterke buitengrenzen

Een modern en efficiënt beheer van de buitengrenzen heeft een dubbel voordeel: het behoudt de integriteit van Schengen en het waarborgt de veiligheid van onze burgers. Als alle relevante actoren ten volle worden betrokken bij de beveiliging aan de grens, kan dat een reële impact hebben op de preventie van grensoverschrijdende criminaliteit en terrorisme. De gezamenlijke operationele activiteiten van de onlangs versterkte Europese grens- en kustwacht[119] dragen bij tot het voorkomen en opsporen van grensoverschrijdende criminaliteit aan de **buitengrenzen** en buiten de EU. De activiteiten van de douane bij het opsporen van veiligheids- en beveiligingsrisico's ten aanzien van alle goederen voordat zij in de EU aankomen, en bij het controleren van goederen op het moment dat zij aankomen, zijn van cruciaal belang voor de bestrijding van grensoverschrijdende criminaliteit en terrorisme. In het komende actieplan inzake de douane-unie zullen maatregelen worden aangekondigd ter versterking van risicobeheersing en interne veiligheid, onder meer door te beoordelen of het haalbaar is een koppeling aan te brengen tussen de informatiesystemen die betrokken zijn bij de analyse van veiligheidsrisico's.

Het kader voor de **interoperabiliteit van de EU-informatiesystemen** op het gebied van justitie en binnenlandse zaken is in mei 2019 goedgekeurd. Deze nieuwe architectuur is bedoeld om de efficiëntie en doeltreffendheid van de nieuwe of opgewaardeerde informatiesystemen[120] te verbeteren. Daardoor komt sneller en systematischer informatie beschikbaar voor rechtshandhavers, grenswachters en migratiefunctionarissen. Dat draagt bij tot correcte identificatie en tot het bestrijden van identiteitsfraude. Om dit te verwezenlijken moet de tenuitvoerlegging van de interoperabiliteit een prioriteit zijn, zowel op politiek als op technisch niveau. Nauwe samenwerking tussen EU-agentschappen en alle lidstaten is cruciaal om de doelstelling van volledige interoperabiliteit tegen 2023 te verwezenlijken.

Fraude met reisdocumenten wordt beschouwd als een van de meest voorkomende strafbare feiten. De fraude vergemakkelijkt het illegale verkeer van criminelen en terroristen en speelt een sleutelrol bij mensenhandel en drugshandel[121]. De Commissie zal nagaan hoe de bestaande werkzaamheden inzake de beveiligingsnormen voor EU-verblijfs- en reisdocumenten kunnen worden uitgebreid, onder meer door middel van digitalisering. Vanaf augustus 2021 zullen de lidstaten beginnen met de afgifte van identiteitskaarten en

[119] Deze bestaat uit het Europees Grens- en kustwachtagentschap (Frontex) en de grenswacht- en kustwachtautoriteiten van de lidstaten.

[120] Het inreis-uitreissysteem (EES), het Europees systeem voor reisinformatie en -autorisatie (Etias), het uitgebreide Europees Strafregister Informatiesysteem (ECRIS-TCN), het Schengeninformatiesysteem, het Visuminformatiesysteem en het nog te upgraden Eurodac.

[121] Het verband tussen documentenfraude en mensenhandel wordt beschreven in het tweede verslag over de vorderingen die zijn gemaakt op het gebied van de bestrijding van mensenhandel (COM(2018) 777), het begeleidende document SWD(2018) 473 en het situatieverslag van Europol over mensenhandel in de EU van 2016.

verblijfsdocumenten die aan geharmoniseerde beveiligingsnormen voldoen en een chip bevatten met biometrische kenmerken, die door alle grensautoriteiten van de EU kan worden geverifieerd. De Commissie zal toezien op de uitvoering van deze nieuwe regels, alsmede op de geleidelijke vervanging van de documenten die momenteel in omloop zijn.

Onderzoek en innovatie op veiligheidsgebied versterken

Cyberbeveiliging en bestrijding van de georganiseerde misdaad, computercriminaliteit en terrorisme zijn allemaal sterk afhankelijk van de ontwikkeling van instrumenten waarmee in de toekomst veiligere nieuwe technologie voor een krachtigere beveiliging kan worden gefaciliteerd, de uitdagingen waarvoor die technologie ons stelt, kunnen worden aangepakt en de werkzaamheden op het gebied van rechtshandhaving kunnen worden ondersteund. Daarvoor is op zijn beurt het werk van particuliere partners en industrieën noodzakelijk.

Innovatie moet worden gezien als een strategisch instrument om actuele dreigingen tegen te gaan en te anticiperen op toekomstige risico's en kansen. Innovatieve technologieën kunnen nieuwe instrumenten aanreiken om de rechtshandhavingsinstanties en andere veiligheidsactoren bij te staan. Kunstmatige intelligentie en analyse van big data kunnen krachtige computersystemen benutten om betere opsporing en snelle uitvoerige analyse van de gegevens mogelijk te maken[122]. Een essentiële voorwaarde voor de ontwikkeling van betrouwbare technologieën is dat de bevoegde autoriteiten over datasets van hoge kwaliteit beschikken voor het opleiden, testen en valideren van algoritmen[123]. Meer in het algemeen is het risico van technologische afhankelijkheid momenteel sterk: de EU is bijvoorbeeld een netto-importeur van cyberbeveiligingsproducten en -diensten, met alle gevolgen van dien voor de economie en voor kritieke infrastructuren. Om de technologie te beheersen en de continuïteit van de voorziening ook te garanderen in geval van ongunstige gebeurtenissen en crises, moet Europa aanwezig zijn en over capaciteit beschikken binnen de kritieke onderdelen van de relevante waardeketens.

Onderzoek, innovatie en technologische ontwikkeling in de EU bieden de mogelijkheid om de veiligheidsdimensie in aanmerking te nemen bij de ontwikkeling van deze technologieën en de toepassing ervan. De volgende generatie van EU-financieringsvoorstellen kan daarvoor een belangrijke stimulans vormen[124]. Bij de initiatieven op het gebied van Europese dataruimten en cloudinfrastructuren is met de beveiliging vanaf het begin rekening gehouden. Het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra[125] hebben tot doel een doeltreffende en efficiënte structuur op te zetten om de capaciteiten en resultaten op het gebied van cyberbeveiliging te bundelen en te delen. Het ruimtevaartprogramma van de EU verleent diensten ter ondersteuning van de veiligheid van de EU, haar lidstaten en individuele personen[126].

---

[122] Hierbij moet gebruik worden gemaakt van de strategie van de Commissie inzake kunstmatige intelligentie.

[123] Een Europese datastrategie (COM(2020) 66 final).

[124] De voorstellen van de Commissie voor Horizon Europa, het Fonds voor interne veiligheid, het Fonds voor geïntegreerd grensbeheer, het EUInvest-programma, het Europees Fonds voor regionale ontwikkeling en het programma Digitaal Europa zullen de ontwikkeling en inzet van innovatieve beveiligingstechnologieën en -oplossingen in de veiligheidswaardeketen ondersteunen.

[125] Voorstel van 12 september 2018 voor een verordening tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra (COM(2018) 630).

[126] Zo levert Copernicus diensten die het toezicht op de buitengrenzen van de EU en de maritieme bewaking mogelijk maken, wat bijdraagt aan de bestrijding van piraterij en smokkel en aan de ondersteuning van

Met meer dan 600 projecten en een totale waarde van bijna 3 miljard EUR sinds 2007, is het door de EU gefinancierde beveiligingsonderzoek een belangrijk instrument om technologie en kennis ter ondersteuning van beveiligingsoplossingen te stimuleren. In het kader van de evaluatie van het mandaat van Europol zal de Commissie zich buigen over de oprichting van een **Europese innovatiehub voor interne veiligheid**[127] die tot doel zou hebben gemeenschappelijke oplossingen te vinden voor gemeenschappelijke uitdagingen en kansen op het gebied van beveiliging, die de lidstaten wellicht niet elk voor zich kunnen benutten. Samenwerking is van fundamenteel belang om de investeringen optimaal te concentreren en innovatieve technologieën te ontwikkelen die zowel zekerheid als economisch voordeel opleveren.

Vaardigheden en bewustmaking

De bewustwording van beveiligingskwesties en het verwerven van de vaardigheden om het hoofd te bieden aan potentiële bedreigingen zijn van essentieel belang om een veerkrachtigere samenleving tot stand te brengen, met beter voorbereide ondernemingen, overheidsdiensten en personen. Problemen op het gebied van IT-infrastructuur en e-systemen hebben aangetoond dat onze menselijke capaciteit voor paraatheid en respons op het gebied van cyberbeveiliging moet worden verbeterd. De pandemie heeft ook laten zien hoe belangrijk digitalisering is op alle gebieden van de economie en de samenleving van de EU.

Basiskennis van de veiligheidsdreigingen en de manier waarop deze moeten worden bestreden, kan al een reële impact hebben op de veerkracht van de samenleving. Bewustheid van de risico's van cybercriminaliteit en van de noodzaak om zichzelf daartegen te beschermen, moeten samengaan met de activiteiten van dienstverleners voor de bescherming tegen cyberaanvallen. Voorlichting over de gevaren en risico's van drugshandel kan het voor criminelen moeilijker maken om te slagen. De EU kan de verspreiding van beste praktijken stimuleren, bijvoorbeeld via het netwerk van centra voor veiliger internet[128], en ervoor zorgen dat deze doelstellingen in haar eigen programma's worden opgenomen.

Het toekomstige actieplan voor digitaal onderwijs moet gerichte maatregelen omvatten om ervoor te zorgen dat de hele bevolking IT-vaardigheden aanleert. De onlangs aangenomen agenda voor vaardigheden[129] ondersteunt het aanleren van vaardigheden gedurende het hele leven. De agenda omvat specifieke maatregelen om het aantal afgestudeerden in de exacte wetenschappen, de technologie, de techniek, de kunsten en de wiskunde te verhogen, omdat zij nodig zijn op speerpuntgebieden zoals cyberbeveiliging. De aanvullende maatregelen die worden gefinancierd via het programma Digitaal Europa, zullen professionals in staat stellen gelijke tred te houden met de ontwikkelingen in het veiligheidsdreigingslandschap en zullen tegelijkertijd de tekorten op dit gebied op de arbeidsmarkt van de EU opvangen. Hierdoor zullen personen in staat worden gesteld de nodige vaardigheden te verwerven om het hoofd te bieden aan veiligheidsdreigingen en slagen bedrijven erin om de specialisten te vinden die zij op dit gebied nodig hebben. De nieuwe Europese onderzoeksruimte en de Europese

kritieke infrastructuren. Wanneer het eenmaal volledig operationeel is, zal het een belangrijke factor zijn voor civiele en militaire missies en operaties.

127 Deze zou ook werken met Frontex, Cepol, eu-LISA en het Gemeenschappelijk Centrum voor Onderzoek.

128 Zie www.betterinternetforkids.eu: het centrale portaal en de nationale centra voor veiliger internet worden momenteel gefinancierd in het kader van CEF/Telecom, en toekomstige financiering is voorgesteld in het kader van het programma Digitaal Europa.

129 Europese vaardighedenagenda voor duurzaam concurrentievermogen, sociale rechtvaardigheid en veerkracht (COM(2020) 274 final).

onderwijsruimte zullen ook loopbanen in wetenschap, technologie, techniek, kunsten en wiskunde bevorderen.

Ook de toegang van **slachtoffers** tot hun rechten is belangrijk; zij moeten de bijstand en ondersteuning krijgen die zij gezien hun specifieke omstandigheden nodig hebben. Bijzondere inspanningen zijn vereist als het gaat om minderheden en de meest kwetsbare slachtoffers, zoals kinderen en vrouwen die het slachtoffer zijn van mensenhandel met het oog op seksuele uitbuiting of blootstaan aan huiselijk geweld[130].

Een bijzondere rol is weggelegd voor verbeterde **vaardigheden op het gebied van rechtshandhaving**. De huidige en nieuwe technologische bedreigingen vereisen meer investeringen in het bijscholen van rechtshandhavingspersoneel in de vroegste fase en gedurende hun gehele loopbaan. Cepol kan de lidstaten als essentiële partner bijstaan bij deze taak. Opleiding op het gebied van rechtshandhaving met betrekking tot racisme en vreemdelingenhaat, en inzake de rechten van de burgers in het algemeen, moet een essentieel onderdeel zijn van een EU-veiligheidscultuur. De nationale justitiële stelsels en beoefenaars van juridische beroepen moeten ook toegerust zijn om zich aan te passen aan en te reageren op ongekende uitdagingen. Opleiding is essentieel om overheden in staat te stellen de instrumenten in een operationele praktijksituatie te gebruiken. Bovendien moet alles in het werk worden gesteld om gendermainstreaming en de participatie van vrouwen in de rechtshandhaving te versterken.

Belangrijkste maatregelen

- Versterking van het mandaat van Europol
- Onderzoek naar een EU-code voor politiële samenwerking en politiecoördinatie in crisistijden
- Versterking van Eurojust om gerechtelijke en rechtshandhavingsinstanties te verbinden
- Herziening van de richtlijn betreffende vooraf te verstrekken passagiersgegevens
- Mededeling over de externe dimensie van de persoonsgegevens van passagiers
- Versterking van de samenwerking tussen de EU en Interpol
- Een kader voor onderhandelingen met belangrijke derde landen over uitwisseling van informatie
- Betere beveiligingsnormen voor reisdocumenten
- Onderzoek naar een Europese innovatiehub voor interne veiligheid

V. Conclusies

In deze steeds turbulentere wereld wordt de Europese Unie nog steeds alom gezien als een van de veiligste en best beveiligde plaatsen. Dat kan echter niet als vanzelfsprekend worden beschouwd.

Met de nieuwe strategie voor de veiligheidsunie wordt de basis gelegd voor een veiligheidsecosysteem dat de hele Europese samenleving bestrijkt. De strategie is gebaseerd op de wetenschap dat veiligheid een gedeelde verantwoordelijkheid is. Veiligheid is een kwestie die iedereen aangaat. Alle overheidsorganen, bedrijven, sociale organisaties,

[130] Zie de strategie voor gendergelijkheid (COM(2020) 152), de EU-strategie inzake de rechten van slachtoffers (COM(2020) 258) en de Europese Strategie voor een beter internet voor kinderen (COM(2012) 196).

instellingen en burgers moeten hun eigen verantwoordelijkheid nemen om onze samenleving veiliger te maken.

Veiligheidskwesties moeten nu vanuit een veel breder perspectief worden bekeken dan in het verleden. Onterecht onderscheid tussen de fysieke en de digitale wereld moet worden tegengegaan. De EU-strategie voor de veiligheidsunie bestrijkt het volledige scala van veiligheidsbehoeften en richt zich met name op de gebieden die de komende jaren het meest kritiek zijn voor de veiligheid van de EU. Er wordt ook erkend dat bedreigingen voor de veiligheid zich niets aantrekken van geografische grenzen en dat de interne en externe veiligheid onderling steeds meer verweven zijn[131]. In dat verband is het belangrijk dat de EU met internationale partners samenwerkt om alle EU-burgers te beschermen en blijft zorgen voor nauwe coördinatie met het externe optreden van de EU bij het uitvoeren van deze strategie.

Onze veiligheid is nauw verbonden met onze fundamentele waarden. Alle in het kader van deze strategie voorgestelde acties en initiatieven zullen geheel in overeenstemming zijn met de grondrechten en onze Europese waarden. Deze vormen de basis van onze Europese manier van leven en moeten centraal blijven staan bij al ons werk.

Tot slot blijft de Commissie zich er ten volle van bewust dat de waarde van alle beleid en alle maatregelen afhankelijk is van de uitvoering ervan. Daarom moeten we blijven hameren op een correcte uitvoering en handhaving van de bestaande en toekomstige wetgeving. Dit zal worden gemonitord aan de hand van periodieke verslagen over de veiligheidsunie en de Commissie zal het Europees Parlement, de Raad en belanghebbenden volledig op de hoogte houden van en blijven betrekken bij alle relevante acties. Daarnaast staat de Commissie paraat om samen met de instellingen gezamenlijke discussies aan te gaan en te organiseren over de strategie van de veiligheidsunie, zodat we samen de geboekte vooruitgang kunnen inventariseren en samen de uitdagingen van de toekomst kunnen aangaan.

De Commissie verzoekt het Europees Parlement en de Raad deze strategie voor de veiligheidsunie te bekrachtigen als basis voor samenwerking en gezamenlijke actie inzake veiligheid in de komende vijf jaar.

[131] Zie de integrale EU-strategie.