EUROPESE
COMMISSIE

Brussel, 30.10.2019
COM(2019) 552 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT, DE EUROPESE RAAD EN DE RAAD

Twintigste voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie

I. INLEIDING

Dit is het twintigste voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie. In dit verslag komen ontwikkelingen aan de orde met betrekking tot twee belangrijke pijlers: de bestrijding van terrorisme, georganiseerde criminaliteit en de middelen ter ondersteuning daarvan, en de verbetering van onze weerbaarheid en veerkracht tegenover die dreigingen.

Voor de Commissie-Juncker was veiligheid van meet af aan een topprioriteit. Voortbouwend op de Europese veiligheidsagenda van april 2015[1] en de mededeling van april 2016 ter voorbereiding van een echte en doeltreffende veiligheidsunie[2], heeft de EU met een gecoördineerde aanpak gereageerd op een reeks terroristische aanslagen en andere toenemende veiligheidsproblemen en daarbij aanzienlijke vooruitgang geboekt met het verbeteren van onze collectieve veiligheid.[3]. Het is steeds duidelijker geworden dat de huidige veiligheidsproblemen — of het nu gaat om terrorisme, georganiseerde misdaad, cyberaanvallen, desinformatie of andere, zich voortdurend ontwikkelende cyberdreigingen — bedreigingen vormen voor alle lidstaten. Alleen door samen te werken, kunnen we het niveau van collectieve veiligheid bereiken dat burgers terecht verlangen en verwachten. Dit gezamenlijke besef is de basis geweest voor de vorderingen die zijn gemaakt in het kader van de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Gezien de behoeften van de nationale autoriteiten die zich inzetten voor de veiligheid van de burgers, was de steun op EU-niveau gericht op wetgevings- en operationele maatregelen waarbij gemeenschappelijk optreden gevolgen kan hebben voor de veiligheid van de lidstaten. Deze werkzaamheden zijn uitgevoerd in nauwe samenwerking met het Europees Parlement en de Raad, en met volledige transparantie voor het brede publiek. Volledige eerbiediging van de grondrechten stond centraal bij deze werkzaamheden, aangezien de veiligheid van de Unie alleen kan worden gewaarborgd wanneer burgers erop kunnen vertrouwen dat hun grondrechten ten volle worden geëerbiedigd.

De EU heeft gewerkt aan **terrorismebestrijding** door de armslag van terroristen te beperken, met nieuwe regels die het hun moeilijker maken toegang te krijgen tot explosieven, vuurwapens en financiering, en hun bewegingsvrijheid beperken. De EU heeft de **informatie-uitwisseling** geïntensiveerd om de verantwoordelijken in de frontlinie, politiefunctionarissen en grenswachten efficiënte toegang te bieden tot accurate en volledige gegevens, en daarbij optimaal gebruik te maken van bestaande informatie en lacunes en blinde vlekken te verhelpen. Krachtige bescherming van de buitengrenzen is een vereiste voor een veilige ruimte van vrij verkeer zonder controles aan de binnengrenzen. In maart 2019 hebben het Europees Parlement en de Raad een akkoord bereikt over een versterkte en volledig uitgeruste **Europese grens- en kustwacht** en de nieuwe verordening zal naar verwachting begin december 2019 in werking treden. De EU heeft personen die in lokale gemeenschappen werken, een platform en financiering geboden om beste praktijken uit te wisselen inzake **het bestrijden van radicalisering en het voorkomen van gewelddadig extremisme**, en nieuwe regels voorgesteld om terroristische online-inhoud op doeltreffende wijze te verwijderen. Met actieplannen ter ondersteuning van de bescherming van openbare ruimten en ter verbetering van de paraatheid bij veiligheidsrisico's op chemisch, biologisch, radiologisch en nucleair

[1] COM(2015) 185 final van 28.4.2015.
[2] COM(2016) 230 final van 20.4.2016.
[3] Vorige voortgangsverslagen over de totstandbrenging van de Veiligheidsunie: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

gebied, heeft de EU-steun **steden beter bestand gemaakt** tegen aanvallen. De EU heeft zich gebogen over **cyberbeveiliging en cyberdreigingen** door een nieuwe EU-cyberbeveiligingsstrategie op te zetten en de desbetreffende wetgeving aan te nemen, en door **desinformatie** aan te pakken om onze verkiezingen beter te beschermen. Er wordt nog steeds gewerkt aan het versterken van de beveiliging van onze **digitale kritieke infrastructuur**, onder meer door beter samen te werken op het gebied van de **cyberbeveiliging van 5G-netwerken** in heel Europa.

Er moet nog meer worden gedaan. De live gestreamde aanval op een synagoge en moord op twee burgers in Halle, Duitsland op 9 oktober 2019, was een schokkende herinnering aan de dreiging die uitgaat van gewelddadig rechts-extremisme en antisemitisme. Daardoor werd nogmaals gewezen op het misbruik van het internet voor terroristische propaganda en bijgevolg op de **noodzaak van EU-brede regels voor de verwijdering van terroristische online-inhoud**. Op de Raad Justitie en Binnenlandse Zaken van 7-8 oktober 2019 werd gedebatteerd over gewelddadig rechts-extremisme en terrorisme en daarbij werd benadrukt dat verdere besprekingen nodig waren, onder meer over het tegengaan van de verspreiding van illegale rechts-extremistische content online en offline. Tegelijkertijd blijkt uit de moord op drie politieagenten en een ander personeelslid in het Parijse politiehoofdkwartier op 3 oktober 2019 dat de dreiging van jihadistisch geïnspireerd terrorisme nog steeds reëel is en dat de lopende inspanningen om de lidstaten te ondersteunen bij het aanpakken van deze dreiging, moeten worden voortgezet. De ontsnapping van opgesloten leden van IS in het kader van de recente gebeurtenissen in Noord-Syrië kan ernstige gevolgen hebben voor de veiligheid in Europa. Het is belangrijk dat de lidstaten ten volle gebruikmaken van bestaande informatiesystemen om buitenlandse terroristische strijders op te sporen en te identificeren wanneer zij de buitengrenzen overschrijden. Er wordt ook gewerkt aan het gebruik van slagveldinformatie om buitenlandse terroristische strijders te vervolgen.

In dit verslag wordt een overzicht gegeven van de vooruitgang die recentelijk is geboekt bij de totstandbrenging van een echte en doeltreffende Veiligheidsunie, waarbij de nadruk wordt gelegd op gebieden waar verdere actie nodig is. Het voorziet in een update over de uitvoering van overeengekomen maatregelen inzake **cyberbeveiliging van 5G-netwerken**, met name over het op 9 oktober 2019 gepubliceerde **EU-risicobeoordelingsverslag**, en over de **bestrijding van desinformatie**.

Dit verslag heeft met name betrekking op de **externe dimensie** van de samenwerking in de Veiligheidsunie: de ondertekening van twee bilaterale terrorismebestrijdingsregelingen met Albanië en Noord-Macedonië, en de vooruitgang die is geboekt in de samenwerking met partners uit derde landen op het gebied van de uitwisseling van **persoonsgegevens van passagiers**. Daarnaast heeft de Commissie tegelijk met dit verslag een verzoek ingediend om machtiging voor de start van onderhandelingen over een overeenkomst tussen de EU en **Nieuw-Zeeland** over de uitwisseling van persoonsgegevens met Europol ter bestrijding van zware criminaliteit en terrorisme.

II. UITVOERING VAN WETGEVINGSPRIORITEITEN

1. Radicalisering via internet en in gemeenschappen voorkomen

Het **voorkomen van radicalisering** vormt de basis van de respons van de Unie op de dreigingen die uitgaan van terrorisme. In dit verband is het internet in de 21e eeuw het belangrijkste strijdperk voor het optreden van terroristen. Dat geradicaliseerde personen op die manier kunnen communiceren en inhoud kunnen delen, maakt de ontwikkeling mogelijk

van wereldwijde, groeiende netwerken van zowel jihadisten als gewelddadige rechts-extremisten. Daarom zet de Commissie haar tweeledige aanpak tegen radicalisering via internet voort, waarbij de voorgestelde regels voor het verwijderen van illegale terroristische online-inhoud het vrijwillige partnerschap met onlineplatforms moeten versterken.

Essentieel hiervoor is het **wetgevingsvoorstel om de verspreiding van terroristische online-inhoud te voorkomen**. Dit bevat duidelijke regels en waarborgen die internetplatforms verplichten om binnen één uur na ontvangst van een gemotiveerd verzoek van de bevoegde autoriteiten terroristische inhoud te verwijderen, en proactieve maatregelen te nemen die in verhouding staan tot de mate van blootstelling aan terroristische inhoud[4]. Er zijn interinstitutionele onderhandelingen aan de gang tussen het Europees Parlement en de Raad, en op 17 oktober 2019 vond een eerste trialoogvergadering plaats. Gezien de dreiging die uitgaat van terroristische online-inhoud, roept de Commissie de medewetgevers op om vóór eind 2019 overeenstemming te bereiken over de voorgestelde wetgeving.

De voorgestelde wetgeving vormt een aanvulling op het vrijwillige partnerschap met de internetindustrie en andere belanghebbenden in het kader van het **EU-Internetforum**. Sinds de oprichting ervan in 2015 fungeert het als katalysator voor het proactieve optreden van internetbedrijven om terroristische online-inhoud te identificeren en te verwijderen, en de weg te effenen voor het door het bedrijfsleven geleide initiatief van een gedeelde databank van hashcodes[5] en de oprichting van het wereldwijde internetforum ter bestrijding van terrorisme. De EU-eenheid voor de melding van internetuitingen, die deel uitmaakt van Europol, de rechtshandhavingsinstantie van de EU, heeft een belangrijke rol gespeeld bij het versterken van de samenwerking met internetbedrijven en heeft bijgedragen aan de algemene doelstellingen van het EU-internetforum. Op de meest recente ministeriële bijeenkomst van het EU-internetforum op 7 oktober 2019 hebben de EU-lidstaten en hoge vertegenwoordigers van internetbedrijven toegezegd om samen te werken in het kader van het zogeheten **EU-crisisprotocol**. Het EU-crisisprotocol bepaalt drempels voor nauwere samenwerking en stelt nieuwe manieren vast om beter te reageren op een crisis. Het gaat om een onderdeel van de inspanningen op internationaal niveau om de "Christchurch Call for Action"[6] ten uitvoer te leggen, die als doel heeft te zorgen voor een gecoördineerde en snelle reactie om de verspreiding van virale terroristische of gewelddadige extremistische inhoud online tegen te gaan.

Naast deze maatregelen tegen radicalisering via internet blijft de Commissie steun verlenen aan inspanningen op nationaal en lokaal niveau om **radicalisering op het terrein te voorkomen en tegen te gaan**. Voortbouwend op de uitgebreide ervaring en deskundigheid die is verzameld in het kader van het netwerk voor voorlichting over radicalisering, biedt de EU gerichte steun aan lokale actoren, waaronder steden[7], en biedt zij mogelijkheden voor uitwisseling tussen mensen uit de praktijk, onderzoekers en beleidsmakers. Zo heeft het

---

4 COM(2018) 640 final van 12.9.2018.

5 Een door een consortium van ondernemingen opgezet instrument om de samenwerking te vergemakkelijken, teneinde de verspreiding van terroristische inhoud op verschillende platforms te voorkomen.

6 Als reactie op de aanslagen in Christchurch hadden de Franse president Emmanuel Macron en de Nieuw-Zeelandse premier Jacinda Ardern leiders en online-platforms uitgenodigd om op 15 mei 2019 in Parijs de "Christchurch Call to Action" te lanceren. Voorzitter Juncker steunde de oproep en kondigde de ontwikkeling van een EU-crisisprotocol aan.

7 Voor de samenwerking met steden op het gebied van beveiliging, zie ook punt V.2 over paraatheid en bescherming, en met name over de bescherming van openbare ruimten.

netwerk specifieke richtsnoeren uitgebracht en workshops georganiseerd voor de ondersteuning van bevoegde instanties die omgaan met kinderen die uit conflictzones komen[8]. Om de continuïteit van de activiteiten in het kader van het netwerk voor voorlichting over radicalisering te waarborgen, heeft de Commissie de procedure opgestart voor een nieuw raamcontract met een geraamde waarde van 61 miljoen EUR over een periode van vier jaar, te beginnen in 2020[9].

Om de dreiging die uitgaat van terroristische online-inhoud tegen te gaan, verzoekt de Commissie het Europees Parlement en de Raad:

- de onderhandelingen over het wetgevingsvoorstel ter voorkoming van de verspreiding van terroristische online-inhoud vóór het einde van het jaar af te ronden.

2. Krachtigere en slimmere informatiesystemen voor veiligheid en grens- en migratiebeheer

De EU heeft de uitwisseling van informatie geïntensiveerd, waardoor identiteitsfraude beter kan worden aangepakt[10], grenscontroles worden verscherpt[11], rechtshandhavingsdatabanken voor heel Europa worden gemoderniseerd[12], informatielacunes worden opgevuld[13] en Europol, het rechtshandhavingsagentschap van de EU, wordt versterkt[14]. Centraal in dit

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

9 Het raamcontract is opgesplitst in twee percelen: 29 miljoen EUR ter ondersteuning van de activiteiten van het netwerk voor voorlichting over radicalisering voor de komende vier jaar en 32 miljoen EUR ter versterking van de capaciteiten van de lidstaten, nationale, regionale en lokale autoriteiten en prioritaire derde landen om radicalisering doeltreffend aan te pakken, met name door netwerkmogelijkheden en gerichte en op behoeften gebaseerde diensten te bieden en onderzoek en analyse aan te brengen.

10 Verordening (EU) 2019/1157 van 20 juni 2019 betreffende de versterking van de beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten afgegeven aan burgers van de Unie en hun familieleden die hun recht van vrij verkeer uitoefenen.

11 Invoering van systematische controles aan de buitengrenzen van alle burgers met gebruikmaking van het Schengeninformatiesysteem. Alle Schengenstaten, alsook Roemenië, Bulgarije, Kroatië en Cyprus, passen de in april 2017 ingevoerde regels inzake systematische controles aan de hand van relevante databanken aan de buitengrenzen toe. Op grond van die regels zijn aan land- of zeegrenzen tijdelijke afwijkingen mogelijk, zij het uitsluitend ten aanzien van EU-burgers, om rekening te houden met onevenredige gevolgen voor de verkeersstroom. Thans hebben zes lidstaten/met Schengen geassocieerde landen (Kroatië, Finland, Hongarije, Letland, Noorwegen en Slovenië) kennisgegeven van dergelijke afwijkingen. Wat de luchtgrenzen betreft, is de mogelijkheid om van de regels inzake systematische controles af te wijken, in april 2019 vervallen.

12 Het versterkte Schengeninformatiesysteem (Verordening (EU) 2018/1860 van 28.11.2018, Verordening (EU) 2018/1861 van 28.11.2018, Verordening (EU) 2018/1862 van 28.11.2018) en het Europees Strafregisterinformatiesysteem zijn uitgebreid tot onderdanen van derde landen (Verordening (EU) 2019/816 van 17.4.2019). De versterking van het Schengeninformatiesysteem omvat onder meer de algemene verplichting om signaleringen in verband met terrorisme in het systeem in te voeren.

13 Het EU-inreis/uitreissysteem (Verordening (EU) 2017/2226 van 30.11.2017) en het Europees systeem voor reisinformatie en -autorisatie (Verordening (EU) 2018/1240 van 12.9.2018 en Verordening (EU) 2018/1241 van 12.9.2018).

14 De laatste jaren is de rol van Europol aanzienlijk versterkt, zowel wat de reikwijdte als wat de diepgang betreft. Het Agentschap is in 2016 versterkt door de goedkeuring van de Europolverordening (Verordening (EU) 2016/794 van 11.5.2016). De lidstaten hebben de hoeveelheid informatie die met en via Europol wordt gedeeld, aanzienlijk verhoogd. De oprichting van het Centrum voor terrorismebestrijding (ECTC) van Europol heeft de analytische capaciteiten van Europol in terrorismezaken versterkt. Het budget van

verband staat de **interoperabiliteit van de EU-informatiesystemen**[15], die erop neerkomt dat de bestaande informatie optimaal kan worden benut en blinde vlekken worden verholpen. Door te voorzien in de behoeften van degenen die in de frontlinie opereren, zal de interoperabiliteit leiden tot snellere, meer systematische toegang tot informatie voor rechtshandhavingsambtenaren, grenswachters en migratiefunctionarissen, waardoor wordt bijgedragen aan de verbetering van de interne veiligheid en het grensbeheer.

Interoperabiliteit en alle innovatie die ermee gepaard gaat, zullen echter alleen een verschil maken voor veiligheid, grensbeheer en migratiebeheer op het terrein als elke lidstaat de betrokken wetgeving volledig ten uitvoer legt. Daarom is de **tenuitvoerlegging** van interoperabiliteit een topprioriteit in de Veiligheidsunie, zowel op politiek als op technisch niveau. De Commissie en eu-LISA, het Europees Agentschap voor het operationeel beheer van grootschalige IT-systemen op het gebied van vrijheid, veiligheid en recht, ondersteunen de lidstaten met deskundigheid en de uitwisseling van beste praktijken, door gebruik te maken van een netwerk van nationale coördinatoren en de ontwikkeling van een scorebord om doeltreffende monitoring- en coördinatieregelingen mogelijk te maken. Nauwe samenwerking tussen EU-agentschappen, lidstaten en met Schengen geassocieerde landen zal van cruciaal belang zijn om de ambitieuze doelstelling te halen, namelijk volledige interoperabiliteit van de EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer tegen 2020.

Intussen moeten het Europees Parlement en de Raad in dit verband **de wetgevingswerkzaamheden nog afronden**. Een snel akkoord over alle in behandeling zijnde wetgevingsvoorstellen is van essentieel belang voor een volledige en tijdige uitrol van de interoperabiliteit. Ten eerste moeten er, in het kader van de technische uitvoering van het **Europees systeem voor reisinformatie en -autorisatie**, technische wijzigingen worden aangebracht in de betrokken verordeningen[16], teneinde het systeem volledig te kunnen opzetten. De Commissie verzoekt het Europees Parlement de werkzaamheden met betrekking tot deze technische wijzigingen te bespoedigen, zodat zo snel mogelijk met de interinstitutionele onderhandelingen kan worden begonnen. Ten tweede zijn de interinstitutionele onderhandelingen over het voorstel van mei 2018 om het bestaande **Visuminformatiesysteem** te versterken en te verbeteren nog aan de gang[17]. Voortbouwend op de eerste trialoogvergadering, die plaatsvond op 22 oktober 2019, roept de Commissie beide medewetgevers op de onderhandelingen snel af te ronden. Ten derde is er nog geen akkoord over het voorstel van de Commissie van mei 2016 om het toepassingsgebied van **Eurodac**[18] uit te breiden door niet alleen de vingerafdrukken en relevante gegevens van asielzoekers en personen die zijn aangehouden in verband met het illegale grensoverschrijding op te slaan, maar ook die van illegaal verblijvende onderdanen van derde landen. De voorgestelde wijzigingen strekken er ook toe dat de vingerafdrukken en relevante gegevens van personen die de EU op irreguliere wijze binnenkomen, langer kunnen worden bewaard. De Commissie roept de medewetgevers op het voorstel vast te stellen.

Om krachtigere EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer tot stand te brengen, roept de Commissie het Europees Parlement en de Raad op om:

Europol is de afgelopen jaren voortdurend gegroeid, van 82 miljoen EUR in 2014 tot 138 miljoen EUR in 2019. De onderhandelingen over de begroting voor 2020 zijn aan de gang.

15 Verordening (EU) 2019/817 van 20.5.2019 en Verordening (EU) 2019/818 van 20.5.2019.

16 Verordening (EU) 2018/1240 van 12.9.2018 en Verordening (EU) 2018/1241 van 12.9.2018.

17 COM (2018) 302 final van 16.5.2018.

18 COM (2016) 272 final van 4.5.2016.

- snel tot een akkoord te komen over de voorgestelde technische wijzigingen die nodig zijn voor de invoering van het **Europees systeem voor reisinformatie en -autorisatie**.
- de onderhandelingen over het voorstel ter versterking van het bestaande **Visuminformatiesysteem** snel te voeren en af te ronden.
- het wetgevingsvoorstel betreffende **Eurodac** vast te stellen *(prioriteit van de gezamenlijke verklaring)*.

3. De armslag van terroristen beperken

De EU heeft krachtige maatregelen genomen om de armslag van terroristen te beperken, met nieuwe regels die het voor terroristen en andere criminelen moeilijker maken om toegang te krijgen tot explosieven[19], vuurwapens en financiering[20], en om hun bewegingsvrijheid te beperken[21].

Om de justitiële reactie op terrorisme te versterken, heeft het EU-agentschap voor justitiële samenwerking in strafzaken (Eurojust) op 1 september 2019 een **Europees justitieel register voor terrorismebestrijding** opgericht. In het register zal justitiële informatie worden samengebracht om verbanden tot stand te brengen in procedures tegen personen die van terroristische misdrijven worden verdacht, en zo de coördinatie tussen openbare aanklagers te versterken wat betreft onderzoek in het kader van terrorismebestrijding met mogelijke grensoverschrijdende gevolgen.

Er zijn echter verdere inspanningen nodig om onderzoeken in grensoverschrijdende zaken te ondersteunen en te vergemakkelijken, met name wat betreft de **toegang tot elektronisch bewijsmateriaal** voor rechtshandhaving. Wat de wetgevingsvoorstellen van april 2018 ter verbetering van de grensoverschrijdende toegang tot elektronisch bewijsmateriaal in het kader van strafrechtelijke onderzoeken[22] betreft, moet het Europees Parlement zijn onderhandelingspositie nog vaststellen voordat de medewetgevers onderhandelingen kunnen beginnen. De Commissie dringt er bij het Europees Parlement op aan om vooruitgang te boeken met dit wetgevingsvoorstel, zodat de medewetgevers het snel kunnen goedkeuren. Op basis van haar voorstel voor interne EU-regels voert de Commissie ook **internationale onderhandelingen** om de grensoverschrijdende toegang tot elektronisch bewijsmateriaal te verbeteren. Op 25 september 2019 hebben de Commissie en de autoriteiten van de Verenigde Staten de eerste formele onderhandelingsronde over een **overeenkomst tussen de EU en de VS over grensoverschrijdende toegang tot elektronisch bewijsmateriaal** gehouden. Een volgende ronde is op 6 november 2019 gepland. In het kader van de lopende onderhandelingen over een **tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa**, heeft de Commissie in juli, september en oktober 2019 namens de Unie deelgenomen aan drie onderhandelingssessies. Hoewel er bij deze onderhandelingen goede vooruitgang is geboekt, moet nog een aantal belangrijke onderwerpen van aanzienlijk belang voor de Unie worden behandeld, zoals waarborgen

[19] Verordening (EU) 2019/1148 van 20.6.2019 over het op de markt brengen en het gebruik van precursoren voor explosieven. De verordening is in werking getreden op 31 juli 2019 en wordt 18 maanden daarna van toepassing.

[20] Richtlijn (EU) 2019/1153 van 11 juli 2019 tot vaststelling van regels ter vergemakkelijking van het gebruik van financiële en andere informatie voor het voorkomen, opsporen, onderzoeken of vervolgen van bepaalde strafbare feiten.

[21] Invoering van systematische controle van alle burgers aan de buitengrenzen, met gebruikmaking van het Schengeninformatiesysteem.

[22] COM(2018) 225 final van 17.4.2018 en COM(2018) 226 final van 17.4.2018.

inzake gegevensbescherming. De onderhandelingen over een tweede aanvullend protocol zullen in november 2019 en in de loop van 2020 worden voortgezet. Het is belangrijk achter beide onderhandelingen vaart te zetten teneinde de internationale samenwerking op het gebied van het delen van elektronisch bewijsmateriaal te bevorderen op een wijze die verenigbaar is met het EU-recht en de daaruit voortvloeiende verplichtingen van de lidstaten en die tevens rekening houdt met toekomstige ontwikkelingen in het EU-recht.

In het licht van de aanhoudende bezorgdheid over het witwassen van geld heeft het Europees Parlement op 19 september 2019 een resolutie aangenomen **over de stand van zaken ten aanzien van de tenuitvoerlegging van de antiwitwaswetgeving van de Unie**[23], waarmee het heeft gereageerd op het pakket van vier verslagen over de bestrijding van het witwassen van geld dat de Commissie op 24 juli 2019 heeft goedgekeurd[24]. Daarin heeft het Europees Parlement de lidstaten opgeroepen ervoor te zorgen dat de antiwitwasrichtlijnen zo snel mogelijk naar behoren in hun nationale wetgeving worden omgezet. Het heeft de Commissie ook verzocht te beoordelen of een antiwitwasverordening geen passender rechtsinstrument zou zijn dan een richtlijn en na te gaan of er behoefte is aan een coördinatie- en ondersteuningsmechanisme voor financiële inlichtingeneenheden.

Om de toegang van rechtshandhavingsinstanties tot elektronisch bewijsmateriaal te verbeteren, roept de Commissie het Europees Parlement en de Raad op om:

- snel overeenstemming te bereiken over de wetgevingsvoorstellen inzake **elektronisch bewijsmateriaal** *(prioriteit van de gezamenlijke verklaring)*.

4. Cyberbeveiliging verbeteren

Het verbeteren van de cyberbeveiliging blijft een belangrijk aspect van de werkzaamheden om een echte en doeltreffende Veiligheidsunie tot stand te brengen. Dankzij de uitvoering van de EU-cyberbeveiligingsstrategie van 2017[25] heeft de Unie haar weerbaarheid versterkt door aanvallen op de Unie moeilijker te maken en zich daarvan sneller te herstellen, en heeft zij gezorgd voor krachtiger afschrikking door de pakkans en de kans op bestraffing van aanvallers te vergroten, onder meer door middel van een kader voor een gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten. De Unie ondersteunt ook de lidstaten op het gebied van cyberdefensie, door het EU-beleidskader voor cyberdefensie uit te voeren[26].

Door de inwerkingtreding van de cyberbeveiligingsverordening[27] in juni 2019 heeft het **EU-kader voor cyberbeveiligingscertificering** vorm gekregen. Certificering speelt een essentiële rol bij het vergroten van het vertrouwen in en de veiligheid van producten en diensten die van

23 https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_NL.html

24 Verslag over de beoordeling van risico's op het gebied van witwassen en terrorismefinanciering die van invloed zijn op de interne markt en verband houden met grensoverschrijdende activiteiten (COM(2019) 370 van 24.7.2019), verslag over de onderlinge koppeling van nationale gecentraliseerde automatische mechanismen (centrale registers of centrale elektronische systemen voor gegevensontsluiting) van de lidstaten voor bankrekeningen (COM(2019) 372 final van 24.7.2019), verslag over de beoordeling van recente vermeende gevallen van het witwassen van geld waarbij EU-kredietinstellingen betrokken zijn (COM(2019) 373 final van 24.7.2019), verslag waarin het kader voor de samenwerking tussen de financiële-inlichtingeneenheden wordt beoordeeld (COM(2019) 371 final van 24.7.2019).

25 JOIN(2017) 450 final van 13.9.2017.

26 EU-beleidskader voor cyberdefensie (update 2018), zoals aangenomen door de Raad op 19 november 2018 (14413/18).

27 Verordening (EU) 2019/881 van 17.4.2019.

cruciaal belang zijn voor de digitale eengemaakte markt. Het certificeringskader zal zorgen voor EU-brede certificatieregelingen in de vorm van een uitgebreide reeks regels, technische vereisten, normen en procedures. Er zijn twee deskundigengroepen bij betrokken, namelijk de Europese Groep voor cyberbeveiligingscertificering, die de autoriteiten van de lidstaten vertegenwoordigt, en de Groep van belanghebbenden bij cyberbeveiligingscertificering, die de sector vertegenwoordigt. Laatstgenoemde groep verenigt zowel de vraag- als de aanbodzijde van producten en diensten op het gebied van informatie- en communicatietechnologie, met inbegrip van kleine en middelgrote ondernemingen, digitaledienstverleners, Europese en internationale normalisatie-instellingen, nationale accreditatie-instanties, toezichthoudende autoriteiten voor gegevensbescherming en conformiteitsbeoordelingsinstanties.

Intussen moeten het Europees Parlement en de Raad nog overeenstemming bereiken over het wetgevingsinitiatief[28] inzake het **Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra**. Het voorstel beoogt de capaciteit van de Unie op het gebied van cyberbeveiliging te versterken door het Europese technologische en industriële cyberbeveiligingsecosysteem te stimuleren en de bijbehorende middelen te coördineren en te bundelen. De Commissie roept beide medewetgevers op om de interinstitutionele onderhandelingen over dit prioritaire initiatief ter verbetering van de cyberbeveiliging te hervatten en snel af te ronden.

De werkzaamheden voor een betere cyberbeveiliging omvatten ondersteuning van zowel het nationale als het regionale niveau[29].

Naast de cyberbedreigingen die gericht zijn op systemen en gegevens, blijft de EU aandacht besteden aan de complexe en veelzijdige uitdagingen die gepaard gaan met **hybride dreigingen**. In de Raad is een horizontale werkgroep inzake de bestrijding van hybride bedreigingen opgericht om de weerbaarheid van de EU en haar lidstaten tegen hybride bedreigingen te verbeteren en om maatregelen ter versterking van de weerbaarheid van samenlevingen tegen crises te ondersteunen. De Commissie en de Europese Dienst voor extern optreden ondersteunen deze inspanningen in het raam van het gezamenlijk kader voor de bestrijding van hybride bedreigingen van 2016[30] en de gezamenlijke mededeling van 2018[31] over het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen. Bovendien werkt het Gemeenschappelijk Centrum voor Onderzoek aan een kader voor een "conceptueel model" voor de karakterisering van hybride dreigingen, met als doel de lidstaten en hun bevoegde autoriteiten te helpen bij het bepalen van het soort hybride aanval waaraan zij kunnen worden blootgesteld. In het model wordt gekeken naar de manier waarop een (statelijke of niet-statelijke) actor op verschillende gebieden (economisch, militair, sociaal, politiek) gebruik maakt van een reeks instrumenten (van desinformatie tot spionage en fysieke activiteiten) om een doelwit te treffen en zo bepaalde doelstellingen te verwezenlijken.

---

28 COM(2018) 630 final van 12.9.2018.

29 Zo ondersteunt de Commissie een interregionaal partnerschap voor innovatie op het gebied van cyberbeveiliging waarbij Bretagne, Castilla y León, Noordrijn-Westfalen, Midden-Finland en Estland zijn betrokken, met het oog op de ontwikkeling van een Europese cyberbeveiligingswaardeketen met specifieke aandacht voor commercialisering en schaalvergroting.

30 JOIN(2016) 18 final van 6.4.2016.

31 JOIN(2018) 16 final van 13.6.2018.

Om de cyberbeveiliging te versterken, roept de Commissie het Europees Parlement en de Raad op om:

- snel overeenstemming te bereiken over het wetgevingsvoorstel inzake het **Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra**.

III. VERBETERING VAN DE BEVEILIGING VAN DIGITALE INFRASTRUCTUUR

Netwerken van de vijfde generatie (5G) zullen zich ontwikkelen tot de ruggengraat van onze steeds meer gedigitaliseerde economieën en samenlevingen. Miljarden verbonden objecten en systemen zullen ervan gebruikmaken, onder meer in kritieke sectoren zoals energie, vervoer, het bankwezen en de gezondheidszorg, maar ook industriële besturingssystemen die gevoelige informatie verwerken en ondersteunende veiligheidssystemen. Het is daarom van essentieel belang dat de cyberbeveiliging en schokbestendigheid van 5G-netwerken wordt gewaarborgd.

In het kader van een gecoördineerde aanpak hebben de lidstaten op 9 oktober 2019, met steun van de Commissie en het Europees Agentschap voor cyberbeveiliging, een verslag gepubliceerd over de gecoördineerde EU-risicobeoordeling inzake cyberbeveiliging in netwerken van de vijfde generatie (5G)[32]. Deze belangrijke stap maakt deel uit van de uitvoering van de in maart 2019 aangenomen aanbeveling van de Commissie om een hoog niveau van cyberbeveiliging van 5G-netwerken in de hele EU te waarborgen[33]. Het verslag is gebaseerd op de resultaten van de nationale risicobeoordelingen inzake cyberbeveiliging die alle lidstaten hebben uitgevoerd. In het verslag worden de belangrijkste dreigingen en dreigingsactoren, de meest kwetsbare activa, de belangrijkste zwakke punten (waaronder technische en andere kwetsbaarheden) en een aantal strategische risico's in kaart gebracht. Deze beoordeling vormt de basis voor het vaststellen van risicobeperkende maatregelen die op nationaal en Europees niveau kunnen worden toegepast.

In het verslag komt een aantal belangrijke **uitdagingen op het gebied van cyberbeveiliging** aan bod die in 5G-netwerken mogelijk belangrijker worden. Deze uitdagingen op het gebied van beveiliging houden voornamelijk verband met belangrijke *innovaties* op het gebied van 5G-technologie, met name het belang van software en het grote aantal diensten en toepassingen die op grond van 5G mogelijk zijn geworden, alsmede de rol van *leveranciers* bij de aanleg en exploitatie van 5G-netwerken en de mate van afhankelijkheid van individuele leveranciers. Dit betekent dat de producten, diensten en activiteiten van leveranciers steeds meer deel gaan uitmaken van het "aanvalsoppervlak" van 5G-netwerken. Bovendien zal het risicoprofiel van individuele leveranciers bijzonder belangrijk worden. Daartoe behoort de mate waarin de leverancier vatbaar is voor inmenging door een niet-EU-land.

Overeenkomstig het in de aanbeveling van de Commissie van maart 2019 beschreven proces moeten de lidstaten uiterlijk op 31 december 2019 overeenstemming bereiken over de **risicobeperkende maatregelen** die nodig zijn in het licht van de geconstateerde

[32] De gecoördineerde EU-risicobeoordeling inzake cyberbeveiliging in 5G-netwerken werd uitgevoerd door de Groep voor samenwerking op het gebied van de beveiliging van netwerk- en informatiesystemen, die is opgericht in het kader van de richtlijn betreffende de beveiliging van netwerk- en informatiesystemen (Richtlijn (EU) 2016/1148 van 6.7.2016), met steun van de Commissie en het Europees Agentschap voor cyberbeveiliging: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019)2355 final van 26.3.2019.

cyberbeveiligingsrisico's op nationaal en EU-niveau. De Commissie en de Europese Dienst voor extern optreden zullen ook blijven samenwerken met gelijkgezinde partners op het gebied van cyberbeveiliging en de schokbestendigheid van 5G-netwerken. In dat verband onderhoudt de Commissie contact met de NAVO over de gecoördineerde EU-risicobeoordeling inzake cyberbeveiliging in 5G-netwerken.

IV. BESTRIJDING VAN DESINFORMATIE EN BESCHERMING VAN VERKIEZINGEN TEGEN ANDERE CYBERDREIGINGEN

De EU heeft een **kader voor gecoördineerde actie tegen desinformatie** opgezet, dat volledig in overeenstemming is met de Europese waarden en grondrechten[34]. Uit hoofde van het actieplan tegen desinformatie[35]worden de mogelijkheden tot desinformatie verder beperkt, mede om de integriteit van de Europese verkiezingen te waarborgen.

Centraal daarbij staat de samenwerking met de sector via de op zelfregulering gebaseerde **praktijkcode tegen desinformatie** voor onlineplatforms en de reclamesector, die in oktober 2018 van toepassing is geworden[36]. De Commissie heeft de doeltreffendheid van de code na het eerste operationele jaar beoordeeld, op basis van de jaarlijkse zelfbeoordelingsverslagen die door de onlineplatforms en de andere ondertekenaars van de code werden ingediend en op 29 oktober 2019 samen met een verklaring van de Commissie werden gepubliceerd[37]. Algemeen gesteld blijkt uit de verslagen dat de ondertekenaars zich serieus hebben ingespannen om hun verbintenissen na te komen.

De maatregelen die de ondertekenaars van het platform ondernemen, variëren qua snelheid en reikwijdte ten aanzien van de vijf pijlers van de code. Over het algemeen is de meeste vooruitgang geboekt met betrekking tot de toezeggingen die verband houden met de Europese verkiezingen van 2019. Daarbij gaat het om het verstoren van reclame en financiële prikkels die aanzetten tot desinformatie (pijler 1), het waarborgen van de transparantie van politieke en thematische reclame (pijler 2) en de integriteit van diensten te beschermen tegen niet-authentieke accounts en gedragingen (pijler 3). Daarentegen is de vooruitgang minder ver gevorderd of zelfs uitgebleven met betrekking tot de toezegging consumenten grotere beslissingsmacht te geven (pijler 4) en de toezegging de onderzoeksgemeenschap sterker te doen staan, onder meer door voor onderzoeksdoeleinden relevante toegang tot datasets te bieden die aan de privacyregels voldoet (pijler 5). Verschillen zijn er voorts wat betreft de reikwijdte van de maatregelen die de respectieve platforms hebben ondernomen om hun toezeggingen gestand te doen. Ook passen niet alle lidstaten hun individuele beleidsmaatregelen op dezelfde wijze toe. De Commissie blijft met de ondertekenaars van de praktijkcode en andere belanghebbenden samenwerken om desinformatie krachtiger aan te pakken.

Uit hoofde van het actieplan tegen desinformatie hebben de Commissie en de hoge vertegenwoordiger in samenwerking met de lidstaten een **systeem voor snelle waarschuwingen** opgezet om desinformatiecampagnes tegen te gaan. Dankzij dit systeem

---

34 Zie het actieplan tegen desinformatie (JOIN(2018) 36 final van 5.12.2018).

35 JOIN(2019) 12 final van 14.6.2019.

36 Door de code te onderschrijven, hebben de onlineplatforms Google, Facebook, Twitter en Microsoft toegezegd manipulatief gebruik van hun diensten door malafide actoren te voorkomen, te zorgen voor transparantie en openbaarmaking van politieke reclame en andere maatregelen te nemen ter bevordering van de transparantie, verantwoordingsplicht en betrouwbaarheid van het online-ecosysteem. Beroepsorganisaties van de reclamebranche hebben zich er ook toe verbonden om samen met de platforms te werken aan het verbeteren van de controle op de plaatsing van advertenties en het ontwikkelen van tools voor merkveiligheid die beogen de plaatsing van advertenties op websites die desinformatie verspreiden, te beperken.

37 https://ec.europa.eu/commission/presscorner/detail/nl/statement_19_6166. Naast Google, Facebook, Twitter en Microsoft is de code onder meer ondertekend door Mozilla, zeven Europese of nationale verenigingen die de reclamesector vertegenwoordigen en EDiMA, een Europese vereniging van platforms en andere technologische bedrijven die actief zijn in de onlinesector.

konden EU-instellingen en de lidstaten voorafgaand aan de verkiezingen voor het Europees Parlement in 2019 informatie en analyses delen en hun optreden coördineren. Dit werk is na de verkiezingen nog geïntensiveerd. Zo wordt er op werkniveau dagelijks informatie uitgewisseld en zijn er drie vergaderingen van de contactpunten voor het systeem voor snelle waarschuwingen georganiseerd door verschillende lidstaten.

Een andere praktische stap om desinformatie te identificeren is het werk van het **strategischecommunicatieteam** ("StratComms"), en met name de East Stratcom Taskforce daarvan. Deze geeft uitvoering aan het "EUvsDisinfo"-project, dat pro-Kremlin-desinformatie monitort, analyseert en beantwoordt[38]. Sinds begin 2019 kon dit werk met het eerste specifieke budget van 3 miljoen EUR worden geïntensiveerd en uitgebreid, zodat pro-Kremlin-desinformatie via internet, radio- en tv-uitzendingen en sociale media nu in 19 talen, waaronder Engels, Servisch en Arabisch, kan worden onderworpen aan monitoring en analyse. Het aantal aan het licht gebrachte desinformatieactiviteiten is meer dan verdubbeld. Tot dusver gaat het in 2019 om ongeveer 2 000 gevallen, tegenover 765 in dezelfde periode in 2018. De East Stratcom Taskforce speelde een cruciale rol bij het monitoren en aan het licht brengen van de pro-Kremlin-desinformatie rond de verkiezingen van het Europees Parlement in 2019. Het onderzoek werd gekoppeld aan een campagne die de aandacht vestigde op pogingen tot inmenging in verkiezingsprocessen over de hele wereld. Dit initiatief, waarbij nauw met het Europees Parlement en de Commissie werd samengewerkt en meer dan 300 journalisten betrokken waren, leidde tot 20 media-interviews.

De Commissie heeft ook actie ondernomen om de **verspreiding van desinformatie en mythen over de instellingen en het beleid van de EU te beperken**. Zij heeft een netwerk van communicatiedeskundigen opgezet, met een onlineportaal waarop interactieve informatie beschikbaar is over EU-beleid en over de uitdagingen en maatschappelijke gevolgen van desinformatie. Ook is de Commissie in samenwerking met het Europees Parlement en de Europese Dienst voor extern optreden een reeks socialemediacampagnes gestart ter bestrijding van desinformatie[39].

V. UITVOERING VAN ANDERE PRIORITAIRE DOSSIERS OP HET GEBIED VAN VEILIGHEID

1. Uitvoering van wetgevingsmaatregelen in het kader van de Veiligheidsunie

De maatregelen die in de Veiligheidsunie zijn overeengekomen, zullen de veiligheid alleen volledig ten goede komen als alle lidstaten ervoor zorgen dat zij snel en volledig worden uitgevoerd. Met het oog daarop ondersteunt de Commissie de lidstaten actief bij de uitvoering van EU-wetgeving, bijvoorbeeld door financiering te verstrekken en de uitwisseling van goede praktijken te faciliteren. De Commissie maakt gebruik van alle bevoegdheden die haar krachtens de Verdragen voor de handhaving van het EU-recht ter beschikking staan, inclusief inbreukprocedures, in voorkomend geval.

De termijn voor de omzetting van de **EU-richtlijn betreffende persoonsgegevens van passagiers**[40] is op 25 mei 2018 verstreken. Tot op heden hebben 25 lidstaten kennis gegeven

[38] www.euvsdisinfo.eu

[39] https://europa.eu/euprotects/

[40] Richtlijn (EU) 2016/681 van 27.4.2016. Denemarken nam niet deel aan de aanneming van deze richtlijn, die derhalve niet bindend is voor en niet van toepassing is op Denemarken.

van volledige omzetting[41]. Dit is een belangrijke vooruitgang ten opzichte van juli 2018, toen de Commissie tegen 14 lidstaten een inbreukprocedure inleidde[42]. Twee lidstaten moeten nog kennisgeving doen van volledige omzetting, de op 19 juli 2018 ingeleide inbreukprocedures ten spijt[43]. Tegelijkertijd blijft de Commissie alle lidstaten steunen bij hun inspanningen om de ontwikkeling van hun systemen voor de registratie van persoonsgegevens van passagiers af te ronden, onder meer door de uitwisseling van informatie en beste praktijken te bevorderen.

De termijn voor de omzetting van de **richtlijn terrorismebestrijding**[44] is verstreken op 8 september 2018. Tot op heden hebben 22 lidstaten kennis gegeven van volledige omzetting. Dit is een belangrijke vooruitgang ten opzichte van november 2018, toen de Commissie tegen 16 lidstaten een inbreukprocedure inleidde[45]. Drie lidstaten moeten nog kennisgeven van volledige omzetting, de lopende inbreukprocedures ten spijt[46]. Op 25 juli 2019 stuurde de Commissie aan twee lidstaten met redenen omklede adviezen wegens niet-mededeling van volledige omzetting van de richtlijn[47]. Daarop kondigden beide lidstaten aan de wetgevingswerkzaamheden voor het eind van dit jaar te zullen afronden.

De termijn voor de omzetting van de **richtlijn inzake de controle op de verwerving en het voorhanden hebben van wapens**[48] is verstreken op 14 september 2018. Inmiddels hebben 13 lidstaten kennis gegeven van volledige omzetting van de richtlijn. 15 lidstaten moeten nog kennisgeven van volledige omzetting, de op 22 november 2018 ingeleide inbreukprocedures ten spijt[49]. Op 25 juli 2019 heeft de Commissie aan 20 lidstaten met redenen omklede adviezen gestuurd wegens niet-mededeling van volledige omzetting van de richtlijn. Daarop gaven vijf lidstaten kennis van de volledige omzetting van de richtlijn[50].

De termijn voor de omzetting van de **richtlijn wetshandhaving**[51] is op 6 mei 2018 verstreken. Tot op heden hebben 25 lidstaten kennis gegeven van volledige omzetting. Dit is een belangrijke vooruitgang ten opzichte van juli 2018, toen de Commissie tegen 19 lidstaten een inbreukprocedure inleidde[52]. Drie lidstaten moeten nog kennisgeven van volledige

---

41 De verwijzingen naar de melding van de volledige omzetting zijn gebaseerd op de door de lidstaten verstrekte informatie en laten de verificatie van de omzetting door de diensten van de Commissie onverlet (stand van zaken op 17.10.2019).

42 Zie het zestiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2018) 690 final van 10.10.2018).

43 Slovenië heeft gedeeltelijke omzetting gemeld. Spanje heeft geen kennisgeving van omzetting gedaan (stand van zaken op 17.10.2019).

44 Richtlijn (EU) 2017/541 van 15.3.2017. De richtlijn is niet van toepassing in het Verenigd Koninkrijk, Ierland en Denemarken.

45 Zie het zeventiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2018) 845 final van 11.12.2018).

46 Griekenland en Luxemburg hebben geen kennis gegeven van nationale uitvoeringsmaatregelen. Polen heeft kennis gegeven van nationale maatregelen die neerkomen op gedeeltelijke omzetting (stand van zaken op 17.10.2019).

47 Griekenland en Luxemburg.

48 Richtlijn (EU) 2017/853 van 17.5.2017.

49 België, Tsjechië, Estland, Polen, Zweden, Slowakije en het Verenigd Koninkrijk hebben omzettingsmaatregelen gemeld voor een deel van de nieuwe bepalingen. Cyprus, Duitsland, Griekenland, Spanje, Luxemburg, Hongarije, Roemenië en Slovenië hebben geen kennisgeving van omzetting gedaan (stand van zaken op 17.10.2019).

50 Finland, Ierland, Litouwen, Nederland en Portugal (stand van zaken op 17.10.2019).

51 Richtlijn (EU) 2016/680 van 27.4.2016.

52 Zie het zestiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2018) 690 final van 10.10.2018).

omzetting, de lopende inbreukprocedures ten spijt[53]. Op 25 juli 2019 besloot de Commissie twee lidstaten[54] naar het Hof van Justitie van de Europese Unie te verwijzen wegens niet-omzetting van de richtlijn en zond zij één lidstaat een met redenen omkleed advies[55] toe wegens onvolledige omzetting van de richtlijn[56].

De Commissie beoordeelt de omzetting van de **vierde antiwitwasrichtlijn**[57] en gaat ook na of de lidstaten de regels correct toepassen. De lidstaten moesten de richtlijn vóór 26 juni 2018 omzetten. De Commissie zet de inbreukprocedures tegen 21 lidstaten door, aangezien zij van oordeel is dat aan de hand van de kennisgevingen die zij van de lidstaten heeft ontvangen, niet kan worden vastgesteld dat de richtlijn volledig is omgezet[58].

De Commissie heeft bovendien de omzetting beoordeeld van de **richtlijnen in verband met cybercriminaliteit**. In juli en oktober 2019 heeft zij inbreukprocedures ingeleid tegen 23 lidstaten[59], omdat zij van oordeel was dat de nationale omzettingswetgeving die door die lidstaten was gemeld, geen correcte omzetting inhield van de **richtlijn ter bestrijding van seksueel misbruik van kinderen**[60]. Evenzo heeft de Commissie in juli en oktober 2019 inbreukprocedures ingeleid tegen vier lidstaten[61], omdat zij van oordeel was dat de nationale omzettingswetgeving die door die lidstaten was gemeld, geen correcte omzetting inhield van de **richtlijn over aanvallen op informatiesystemen**[62].

De Commissie roept de lidstaten op met spoed de nodige maatregelen te nemen om de volgende richtlijnen volledig in nationaal recht om te zetten en de Commissie daarvan in kennis te stellen:

- de **EU-richtlijn betreffende persoonsgegevens van passagiers**: één lidstaat moet nog kennisgeving doen van omzetting in nationaal recht en één lidstaat moet nog kennisgeving doen van de vervollediging van de omzetting[63];
- de **richtlijn terrorismebestrijding**: twee lidstaten moeten nog kennisgeving doen van omzetting in nationaal recht en één lidstaat moet nog kennisgeving doen van de vervollediging van de omzetting[64];
- de **richtlijn inzake de controle op de verwerving en het voorhanden hebben van**

53 Slovenië heeft gedeeltelijke omzetting gemeld. Spanje heeft geen kennis gegeven van omzetting. Duitsland heeft volledige omzetting gemeld, maar de Commissie beschouwt de omzetting niet als volledig (stand van zaken op 17.10.2019).

54 Griekenland en Spanje.

55 Duitsland.

56 Griekenland heeft kennis gegeven van volledige omzetting; de Commissie werkt aan de beoordeling ervan.

57 Richtlijn (EU) 2015/849 van 20.5.2015.

58 België, Bulgarije, Tsjechië, Denemarken, Duitsland, Estland, Ierland, Frankrijk, Italië, Cyprus, Letland, Litouwen, Hongarije, Nederland, Oostenrijk, Polen, Roemenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk (stand van zaken op 17.10.2019). Eerder werden zeven inbreukprocedures in verband met de richtlijn gesloten.

59 België, Bulgarije, Tsjechië, Duitsland, Estland, Griekenland, Spanje, Frankrijk, Kroatië, Italië, Letland, Litouwen, Luxemburg, Hongarije, Malta, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland en Zweden.

60 Richtlijn (EU) 2011/93 van 13.12.2011.

61 Bulgarije, Italië, Portugal en Slovenië.

62 Richtlijn (EU) 2013/40 van 12.8.2013.

63 Slovenië heeft gedeeltelijke omzetting gemeld. Spanje heeft geen kennisgeving van omzetting gedaan (stand van zaken op 17.10.2019).

64 Griekenland en Spanje hebben geen kennisgeving van omzetting gedaan. Poland heeft kennis gegeven van gedeeltelijke omzetting (stand van zaken op 17.10.2019).

wapens: acht lidstaten moeten nog kennisgeving doen van omzetting in nationaal recht en zeven lidstaten moeten nog kennisgeving doen van de vervollediging van de omzetting[65];

- de **richtlijn gegevensbescherming bij rechtshandhaving**: één lidstaat moet nog kennisgeving doen van omzetting in nationaal recht en twee lidstaten moeten nog kennisgeving doen van de vervollediging van de omzetting[66];
- de **vierde antiwitwasrichtlijn**: 21 lidstaten moeten nog vervollediging van de omzetting melden[67];
- de **richtlijn ter bestrijding van seksueel misbruik van kinderen**: tegen 23 lidstaten zijn inbreukprocedures wegens onjuiste omzetting ingeleid[68];
- de **richtlijn over aanvallen op informatiesystemen**: tegen vier lidstaten zijn inbreukprocedures wegens onjuiste omzetting ingeleid[69].

2. Paraatheid en bescherming

Het versterken van de weerbaarheid tegen veiligheidsdreigingen is een wezenlijk onderdeel van het streven naar een echte en doeltreffende Veiligheidsunie. De Commissie steunt de lidstaten en de lokale overheden bij het verbeteren van de bescherming van openbare ruimten door uitvoering te geven aan het actieplan van oktober 2017 en het partnerschap voor veiligheid in publieke ruimten van januari 2019 in het kader van de stedelijke agenda voor de EU. Bij dit werk zijn de steden betrokken die de Commissie hebben verzocht om ondersteuning bij de aanpak van de problemen die zij ondervonden bij de bescherming van openbare ruimten.

De uitwisseling van beste praktijken door lokale overheden en met particuliere exploitanten is van cruciaal belang voor het verbeteren van de beveiliging van openbare ruimten. Dit thema stond centraal tijdens de **Europese week van de veiligheid** die van 14 tot en met 18 oktober 2019 in Nice (Frankrijk) werd georganiseerd in het kader van het door de EU gefinancierde project "Protect Allied Cities against Terrorism in Securing Urban Areas". Dit evenement werd bijgewoond door 500 vertegenwoordigers van steden in heel Europa, nationale autoriteiten en onderzoeksinstellingen. Benadrukt werd het belang van nauwe samenwerking tussen alle – zowel publieke als private – belanghebbende partijen en de rol van nieuwe technologie bij het beter beschermen van steden. De bescherming van openbare ruimten kwam ook aan de orde tijdens de **Europese week van regio's en steden**, die van 7 tot en met 10 oktober 2019 in Brussel werd gehouden en een workshop omvatte over de stedelijke agenda voor het EU-partnerschap inzake beveiliging in openbare ruimten. Tijdens deze workshop werd ingegaan op de rol van de lokale overheid bij beveiligingsbeleid, EU-

[65] België, Tsjechië, Estland, Polen, Zweden, Slowakije en het Verenigd Koninkrijk hebben omzettingsmaatregelen voor een deel van de nieuwe bepalingen gemeld. Cyprus, Duitsland, Griekenland, Spanje, Luxemburg, Hongarije, Roemenië en Slovenië hebben geen kennisgeving van omzetting gedaan (stand van zaken op 17.10.2019).

[66] Slovenië heeft gedeeltelijke omzetting gemeld. Spanje heeft geen kennis gegeven van omzetting. Duitsland heeft volledige omzetting gemeld, maar de Commissie beschouwt de omzetting niet als volledig (stand van zaken op 17.10.2019).

[67] België, Bulgarije, Tsjechië, Denemarken, Duitsland, Estland, Ierland, Frankrijk, Italië, Cyprus, Letland, Litouwen, Hongarije, Nederland, Oostenrijk, Polen, Roemenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk (stand van zaken op 17.10.2019).

[68] België, Bulgarije, Tsjechië, Duitsland, Estland, Griekenland, Spanje, Frankrijk, Kroatië, Italië, Letland, Litouwen, Luxemburg, Hongarije, Malta, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland en Zweden.

[69] Bulgarije, Italië, Portugal en Slovenië.

regelgeving en -financiering in verband met belangrijke beveiligingskwesties in stedelijke openbare ruimten, en kernthema's zoals innovatie door middel van slimme oplossingen en technologieën, waaronder het begrip beveiliging door ontwerp, preventie en sociale inclusie. Met haar laatste oproep tot het indienen van voorstellen voor stedelijke innovatieve acties, waarvan de resultaten in augustus 2019 werden bekendgemaakt, stimuleert de Commissie steden ook om op dit gebied te innoveren. In het kader van de geselecteerde projecten zullen drie steden (Piraeus in Griekenland, Tampere in Finland en Turijn in Italië) nieuwe oplossingen voor stedelijke beveiliging uitproberen[70].

Om **de bescherming van gebedshuizen** te verbeteren en de behoeften van verschillende religieuze groepen te verkennen, organiseerde de Commissie op 7 oktober 2019 een bijeenkomst met vertegenwoordigers van de joodse, islamitische, christelijke en boeddhistische gemeenschappen. Deze bijeenkomst maakte deel uit van de uitvoering van het EU-actieplan 2017 ter ondersteuning van de bescherming van openbare ruimten. Qua beveiligingsbewustzijn en paraatheid bleken er aanzienlijke verschillen te bestaan tussen de religieuze gemeenschappen. Het is dan ook zaak goede praktijken te blijven uitwisselen. Ook werd duidelijk dat de invoering van elementaire beveiligingsmaatregelen en de ontwikkeling van een beter beveiligingsbewustzijn niet onverenigbaar zijn met het open en toegankelijke karakter van gebedshuizen. De Commissie zal goede praktijken en voorlichtingsmateriaal bijeenbrengen op haar elektronische deskundigenplatform en de zaak onder de aandacht brengen van de beveiligingsinstanties van de lidstaten, via het publiek-private forum voor de bescherming van openbare ruimten.

Een specifiek gebied dat meer aandacht vereist, is de toenemende veiligheidsdreiging die **drones** vormen voor kritieke infrastructuur en openbare ruimten. In aanvulling op de recente EU-wetgeving[71] inzake veilige dronevluchten in de luchtruimte voor bemande luchtvaart, en zonder afbreuk te doen aan de nuttige gebruiksmogelijkheden van drones, ondersteunt de Commissie de lidstaten bij het opsporen van trends in het kwaadwillig gebruik van drones. Daartoe financiert zij onderzoek en bevordert zij het testen van tegenmaatregelen. De uitwisseling van ervaringen en beste praktijken is van cruciaal belang, zoals bleek tijdens de op 17 oktober 2019 in Brussel gehouden internationale conferentie op hoog niveau over de bestrijding van de dreiging die uitgaat van onbemande luchtvaartuigsystemen. Op dit door de Commissie georganiseerde evenement kwamen namens de lidstaten, internationale organisaties, partners uit derde landen, het bedrijfsleven, de academische wereld en het maatschappelijk middenveld 250 deelnemers bijeen om de veiligheidsproblemen rond drones te bespreken en over mogelijke oplossingen na te denken. Duidelijk werd dat de risico's in verband met drones regelmatig moeten worden beoordeeld en dat bij de ontwikkeling van Europese wetgeving inzake veilig droneverkeer nauwe samenwerking geboden is tussen de luchtvaart- en rechtshandhavingsinstanties. Ook dienen maatregelen tegen drones verder te worden getest door middel van een gecoördineerde Europese aanpak. Voorts was er overeenstemming over het feit dat nauwe samenwerking tussen de autoriteiten en de sector van essentieel belang is om ervoor te zorgen dat drones veilig, goed beveiligd en operationeel betrouwbaar zijn en moeilijk voor kwaadaardige doeleinden kunnen worden misbruikt.

---

70 De stedelijke innovatie acties (Urban Innovative Actions) worden medegefinancierd door het Europees Fonds voor regionale ontwikkeling. Zie voor meer informatie: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

71 Uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen.

3. Externe dimensie

Aangezien de meeste veiligheidsrisico's waarmee de Unie wordt geconfronteerd, niet stoppen bij de grenzen van de EU, maar mondiale bedreigingen vormen, speelt de samenwerking met partnerlanden en -organisaties en relevante belanghebbenden een essentiële rol bij de totstandbrenging van een doeltreffende en echte Veiligheidsunie.

De uitwisseling van informatie staat bij deze samenwerking centraal. Samen met dit verslag heeft de Commissie een aanbeveling goedgekeurd voor een besluit van de Raad waarbij machtiging wordt verleend tot het openen van onderhandelingen over een **overeenkomst tussen de EU en Nieuw-Zeeland over de uitwisseling van persoonsgegevens voor de bestrijding van zware criminaliteit en terrorisme** tussen de bevoegde autoriteiten van Europol en Nieuw-Zeeland. Een dergelijke overeenkomst zal Europol in staat stellen nog beter met Nieuw-Zeeland samen te werken om misdrijven waarvan de bestrijding binnen de doelstellingen van Europol valt, te voorkomen en tegen te gaan. Hoewel de werkovereenkomst tussen Europol en Nieuw-Zeeland van april 2019 een kader verschaft voor een gestructureerde samenwerking op strategisch niveau, biedt deze geen rechtsgrondslag voor de uitwisseling van informatie over persoonsgegevens. Voor doeltreffende operationele politiesamenwerking is het van essentieel belang dat de uitwisseling van persoonsgegevens geheel in overeenstemming is met het EU-recht en de grondrechten. Eerder heeft de Commissie op basis van terroristische dreiging, migratiegerelateerde uitdagingen en de operationele behoeften van Europa acht prioritaire landen in de regio Midden-Oosten/Noord-Afrika aangewezen waarmee als eerste onderhandelingen moeten worden gestart[72]. Gelet op de operationele behoeften van rechtshandhavingsinstanties in de EU en de potentiële voordelen van nauwere samenwerking op dit gebied – die onder meer zichtbaar werden in de nasleep van de aanslag in Christchurch van maart 2019 – acht de Commissie het nodig om ook Nieuw-Zeeland aan te merken als een prioritair land waarmee op korte termijn onderhandelingen moeten worden begonnen.

Een andere hoeksteen van de samenwerking tussen de Unie en derde landen is de doorgifte van **persoonsgegevens van passagiers**. Op 27 september 2019 keurde de Commissie een aanbeveling goed voor een besluit van de Raad waarbij machtiging wordt verleend tot het openen van onderhandelingen over een overeenkomst tussen de **EU en Japan** over de uitwisseling van persoonsgegevens ter voorkoming en bestrijding van terrorisme en zware grensoverschrijdende criminaliteit, met volledige inachtneming van de waarborgen inzake gegevensbescherming en de grondrechten.[73]. De aanbeveling wordt momenteel op het niveau van de werkgroepen van de Raad besproken en de Commissie roept de Raad op om snel een mandaat voor de onderhandelingen met Japan vast te stellen. Het zou uit beveiligingsoogpunt pure winst zijn als er nog voor de Olympische Spelen van 2020 regelingen zouden zijn getroffen.

Op mondiaal niveau ondersteunt de Commissie de werkzaamheden van de **Internationale Burgerluchtvaartorganisatie** (ICAO) om een norm vast te stellen voor de verwerking van persoonsgegevens van passagiers. Hiermee wordt gehoor gegeven aan de in Resolutie 2396 van de VN-Veiligheidsraad vervatte oproep aan alle lidstaten van de Verenigde Naties om de

[72] Zie het elfde voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2017) 608 final van 18.10.2017). De prioritaire landen zijn Algerije, Egypte, Israël, Jordanië, Libanon, Marokko, Tunesië en Turkije.

[73] COM(2019) 420 final (27.9.2019).

capaciteit te ontwikkelen voor het verzamelen, verwerken en analyseren van persoonsgegevens van passagiers. Op 13 september 2019 presenteerde de Commissie een voorstel[74] voor een besluit van de Raad betreffende het namens de EU in de Raad van de Internationale Burgerluchtvaartorganisatie in te nemen standpunt met betrekking tot normen en aanbevolen praktijken op het gebied van persoonsgegevens van passagiers. Dit voorstel wordt momenteel op het niveau van de groepen van de Raad besproken en de Commissie pleit voor een snelle goedkeuring van het besluit van de Raad. Het standpunt van de Unie en haar lidstaten is ook uiteengezet in een informatieve nota over normen en beginselen inzake het verzamelen, gebruiken, verwerken en beschermen van persoonsgegevens van passagiers, die is ingebracht op de veertigste vergadering van de Internationale Burgerluchtvaartorganisatie.

Wat betreft de werkzaamheden met betrekking tot een nieuwe overeenkomst over persoonsgegevens van passagiers met **Canada**, streeft de Commissie naar een vlotte afronding. Afgelopen zomer werd begonnen aan de gecombineerde gezamenlijke beoordeling en gezamenlijke evaluatie van de overeenkomst inzake persoonsgegevens van passagiers met **Australië** alsook de gezamenlijke evaluatie van de overeenkomst inzake persoonsgegevens van passagiers met de **Verenigde Staten**, met bezoeken aan Canberra en Washington in respectievelijk augustus en september 2019. De Commissie heeft de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement op 14 oktober 2019 achter gesloten deuren geïnformeerd over de stand van zaken wat betreft de werkzaamheden met Japan, Australië en Canada inzake persoonsgegevens van passagiers.

Ook is er vooruitgang geboekt op het gebied van de samenwerking met de partners op de **Westelijke Balkan** bij de uitvoering van het gezamenlijk actieplan inzake terrorismebestrijding voor de Westelijke Balkan van oktober 2018. Op 9 oktober heeft de Commissie twee niet-verbindende bilaterale terrorismebestrijdingsregelingen ondertekend met Albanië en Noord-Macedonië[75]. Deze regelingen bevatten prioritaire maatregelen op maat die moeten worden genomen door de autoriteiten van het betrokken partnerland. Ze bestrijken de vijf doelstellingen van het gezamenlijk actieplan[76] en vermelden welke steun de Commissie voornemens is te verlenen. Naar verwachting zullen de komende weken soortgelijke regelingen worden ondertekend met de overige partners op de Westelijke Balkan. Verder heeft de Commissie op 7 oktober 2019 een overeenkomst ondertekend met Montenegro over samenwerking op het gebied van grensbeheer tussen Montenegro en het Europees Grens- en kustwachtagentschap. Op grond van deze overeenkomst kan het agentschap Montenegro bijstand verlenen bij het grensbeheer, teneinde irreguliere migratie en grensoverschrijdende criminaliteit aan te pakken en zo de beveiliging van de buitengrens van de EU te verbeteren.

Teneinde de samenwerking met partnerlanden bij de aanpak van gezamenlijke veiligheidsdreigingen te versterken, roept de Commissie de Raad op om:

- machtiging te verlenen tot het openen van onderhandelingen over een overeenkomst tussen de EU en **Nieuw-Zeeland** over de uitwisseling van persoonsgegevens voor de

[74] COM(2019) 416 final (13.9.2019).

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

[76] Het gezamenlijke actieplan voorziet in acties rond de volgende vijf doelstellingen: een solide kader voor terrorismebestrijding, doeltreffende preventie en bestrijding van gewelddadig extremisme, doeltreffende informatie-uitwisseling en operationele samenwerking, opbouw van de capaciteit om terrorismefinanciering en witwassen van geld te bestrijden, en versterking van de bescherming van burgers en infrastructuur.

bestrijding van zware criminaliteit en terrorisme;

- machtiging te verlenen tot het openen van onderhandelingen over een overeenkomst tussen de EU en **Japan** over de doorgifte van persoonsgegevens;
- goedkeuring te hechten aan het voorgestelde **besluit van de Raad betreffende het namens de EU in de Raad van de Internationale Burgerluchtvaartorganisatie in te nemen standpunt** met betrekking tot normen en aanbevolen praktijken op het gebied van persoonsgegevens van passagiers.

VI. CONCLUSIE

Dit verslag beschrijft de uiteenlopende maatregelen die de EU heeft genomen om gemeenschappelijke dreigingen in Europa aan te pakken en onze collectieve veiligheid te versterken. Er is een gedeeld besef dat de huidige veiligheidsuitdagingen het best kunnen worden aangepakt wanneer de lidstaten samenwerken – onderling en met derde landen. De vooruitgang in de richting van een echte en doeltreffende Veiligheidsunie is dan ook het resultaat van nauwe samenwerking tussen uiteenlopende actoren, die vertrouwen opbouwen, middelen delen en samen het hoofd bieden aan dreigingen. Daarbij gaat het om alle overheidsniveaus – van steden en andere lokale actoren tot regio's en nationale autoriteiten – en om EU-instellingen als het Europees Parlement en de Raad. Het is een zaak van overheidsdiensten, EU-agentschappen, particuliere actoren en het maatschappelijk middenveld. En daarbij wordt gebruik gemaakt van expertise, instrumenten en middelen op tal van beleidsterreinen, waaronder vervoer, de digitale eengemaakte markt en het cohesiebeleid. De ontwikkeling van de Veiligheidsunie maakt dan ook integraal deel uit van de bescherming van de grondrechten en het vrijwaren en bevorderen van onze waarden.

Het werk aan een echte en doeltreffende Veiligheidsunie moet worden voortgezet. Er moet snel overeenstemming worden bereikt over belangrijke hangende initiatieven. Daarbij gaat het met name om: 1) het wetgevingsvoorstel inzake het verwijderen van terroristische online-inhoud, 2) het wetgevingsvoorstel om de toegang van rechtshandhavingsinstanties tot elektronisch bewijsmateriaal te verbeteren, 3) het wetgevingsvoorstel voor het opzetten van een Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en een netwerk van nationale coördinatiecentra, en 4) de hangende wetgevingsvoorstellen inzake krachtigere en slimmere informatiesystemen voor veiligheid, grensbeheer en migratiebeheer. De overeengekomen maatregelen en instrumenten moeten nu concreet en operationeel worden. De winst uit beveiligingsoogpunt zal optimaal zijn als alle lidstaten de EU-wetgeving tijdig en volledig ten uitvoer leggen. Het is met name van belang dat alle lidstaten de onlangs overeengekomen wetgeving over de interoperabiliteit van de EU-informatiesystemen voor veiligheid, grens- en migratiebeheer uitvoeren, zodat de ambitieuze doelstelling om tegen 2020 tot volledige operabiliteit te komen, wordt verwezenlijkt. Ten slotte dient Europa waakzaam blijven ten aanzien van opkomende en veranderende dreigingen en te blijven samenwerken om de veiligheid van alle burgers te versterken.