EUROPESE
COMMISSIE

Brussel, 24.7.2019
COM(2019) 353 final

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

Negentiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie

I. INLEIDING

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

De Europeanen verwachten terecht dat de Unie hen beschermt. Voor de Commissie-Juncker was veiligheid van meet af aan een topprioriteit. In het document "Een nieuwe strategische agenda 2019-2024" heeft de Europese Raad "onze burgers en vrijheden beschermen" opgenomen als eerste van vier kernprioriteiten voor de Unie[1]. Voorts heeft de Europese Raad in de strategie aangekondigd de strijd tegen terrorisme en grensoverschrijdende criminaliteit te zullen opvoeren en uitbreiden, onder meer door de samenwerking en informatie-uitwisseling te verbeteren en de gemeenschappelijke instrumenten verder te ontwikkelen.

Dankzij de nauwe samenwerking tussen het Europees Parlement, de Raad en de Commissie heeft de EU aanzienlijke vooruitgang met de gezamenlijke werkzaamheden voor de totstandbrenging van een echte en doeltreffende Veiligheidsunie geboekt door een aantal initiatieven op het gebied van prioritaire wetgeving te nemen en uiteenlopende niet-wetgevende maatregelen ten uitvoer te leggen om de lidstaten te ondersteunen en de veiligheid voor alle burgers te verbeteren[2]. De Unie heeft doortastende maatregelen genomen om de armslag van terroristen en criminelen te beperken door de verwerving en het gebruik van bepaalde vuurwapens en explosieven te verbieden en de toegang tot financiering te beperken en op die manier terroristen te beletten zich de middelen voor het plegen van aanslagen te verschaffen. De EU heeft ook de informatie-uitwisseling tussen de lidstaten verbeterd en lacunes en blinde vlekken op het gebied van informatie verholpen in het kader van haar inspanningen om radicalisering te bestrijden, Europeanen online te beschermen, cyberdreigingen aan te pakken, het beheer van de buitengrenzen van de Unie te versterken en de internationale samenwerking op het gebied van veiligheid te verbeteren.

Een aantal andere prioritaire initiatieven op het gebied van de Veiligheidsunie wachten nog op goedkeuring door de medewetgevers. Rekening houdend met de start van de negende zittingsperiode van het Europees Parlement op 2 juli 2019 bevat dit verslag:

- een overzicht van de maatregelen die de medewetgevers moeten nemen om onmiddellijke dreigingen aan te pakken. Met name moet dringend actie worden ondernomen om **terroristische propaganda en radicalisering via internet tegen te gaan**;
- een overzicht van de prioritaire initiatieven op het gebied van de Veiligheidsunie die nog in behandeling zijn en verdere actie van de medewetgevers vereisen (verbetering van de **cyberbeveiliging**, vergemakkelijking van de toegang tot **elektronisch bewijsmateriaal** en afronding van de werkzaamheden inzake krachtigere en slimmere informatiesystemen voor veiligheid, grensbeheer en migratiebeheer);
- een update over de gezamenlijke, urgente werkzaamheden die in maart 2019 van start zijn gegaan om de **beveiliging van 5G-netwerken** te beoordelen en te versterken, uitgaande van de nationale risicobeoordelingen die de lidstaten uiterlijk op 15 juli 2019 hebben ingediend;
- uitleg over een pakket van vier verslagen over de **bestrijding van het witwassen van geld**, dat op 24 juli 2019 door de Commissie is goedgekeurd en waarin de actuele risico's en kwetsbaarheden op het gebied van witwasactiviteiten worden geanalyseerd en wordt

[1] https://www.consilium.europa.eu/media/39933/a-new-strategic-agenda-2019-2024-nl.pdf

[2] Voor een overzicht, zie het factsheet "Veiligheidsunie: een Europa dat bescherming biedt" (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_nl.pdf) en het achttiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2019) 145 final van 20.3.2019).

beoordeeld hoe het betrokken EU-regelgevingskader in de particuliere en de openbare sector wordt toegepast;

- een update over de vooruitgang die sinds maart 2019[3] is geboekt bij de uitvoering van wetgevingsmaatregelen op het gebied van de Veiligheidsunie. Interoperabiliteit van de informatiesystemen is in dit verband een van de topprioriteiten voor een snelle en volledige uitvoering door de lidstaten;
- een balans van de lopende werkzaamheden om desinformatie tegen te gaan en verkiezingen te beschermen tegen cyberdreigingen, van de inspanningen om de paraatheid en de bescherming tegen veiligheidsdreigingen te verbeteren, en van de samenwerking met internationale partners op het gebied van veiligheidskwesties.

II. UITVOERING VAN WETGEVINGSPRIORITEITEN

1. Radicalisering via internet en in gemeenschappen voorkomen

Het voorkomen van radicalisering, zowel via internet als in gemeenschappen, staat centraal in de reactie van de EU op terrorisme.

De aanslag van 15 maart 2019 in Christchurch (Nieuw-Zeeland) heeft nogmaals op gruwelijke wijze aangetoond hoe het internet kan worden gebruikt voor terroristische doeleinden, ongeacht de ideologie die eraan ten grondslag ligt (jihadisme, rechts-extremisme of een andere extremistische strekking). Dat de livestreamvideo van de aanslag zo snel en op zo grote schaal zijn weg naar de internetplatforms vond, toont aan hoe cruciaal het is dat deze platforms adequaat zijn toegerust om de snelle verspreiding van dit soort inhoud tegen te gaan.

De staatshoofden en regeringsleiders van een aantal lidstaten en derde landen, voorzitter Juncker en online-platforms hebben op 15 mei 2019 hun steun uitgesproken voor de "**Christchurch Call to Action**"[4], een oproep tot collectieve acties om terroristische en gewelddadige extremistische inhoud van het internet te weren. Ook de G7[5] en de G20[6] zijn in dit verband verbintenissen aangegaan.

De Commissie heeft al op het duidelijke en reële gevaar van terroristische online-inhoud gereageerd met het **wetgevingsvoorstel** dat voorzitter Juncker in zijn Staat van de Unie 2018 had aangekondigd en waarin een duidelijk en geharmoniseerd rechtskader wordt voorgesteld om misbruik van aanbieders van hostingdiensten voor de verspreiding van terroristische online-inhoud te voorkomen[7]. Op grond van de voorgestelde maatregelen zouden internetplatforms terroristische inhoud moeten verwijderen binnen één uur nadat zij daartoe een bevel van een bevoegde autoriteit in een lidstaat hebben ontvangen. Platforms die worden misbruikt voor de verspreiding van terroristische inhoud, zouden bovendien proactieve maatregelen (met duidelijke regels en waarborgen) moeten nemen om deze inhoud op te sporen en te voorkomen dat deze opnieuw wordt geüpload. De autoriteiten van de lidstaten moeten voorzien in speciale rechtshandhavingscapaciteit met de nodige middelen om terroristische inhoud op doeltreffende wijze op te sporen en verwijderingsbevelen uit te vaardigen.

---

3 Zie het achttiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2019) 145 final van 20.3.2019).

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. De Franse president Emmanuel Macron en de Nieuw-Zeelandse premier Jacinda Ardern hadden de leiders en online-platforms uitgenodigd voor de lancering van dit initiatief op 15 mei 2019 in Parijs.

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

6 Tijdens de G20 (Osaka, 28-29 juni 2019) hebben de leiders hun belofte herhaald om mensen te beschermen tegen het gebruik van het internet voor terrorisme en gewelddadig extremisme dat de voedingsbodem vormt voor terrorisme (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final van 12.9.2018.

Dit zal een snel, doeltreffend en voor de hele Unie geldend systeem opleveren met solide waarborgen, waaronder de mogelijkheid om een beroep te doen op doeltreffende klachtenmechanismen en op rechtsmiddelen.
De voorgestelde maatregelen zullen bijdragen tot de goede werking van de digitale eengemaakte markt. Tegelijkertijd wordt online de veiligheid verhoogd en het vertrouwen versterkt en worden de waarborgen voor de vrijheid van meningsuiting en van informatie versterkt.

De ministers van Justitie en Binnenlandse Zaken hebben in december 2018 in de Raad overeenstemming bereikt over een algemene aanpak voor het voorstel. In april 2019 heeft het Europees Parlement zijn advies in eerste lezing uitgebracht. Met het oog op een spoedig akkoord over een EU-regelgevingskader met duidelijke regels en waarborgen **roept de Commissie beide medewetgevers op om zo snel mogelijk interinstitutionele onderhandelingen op te starten over dit prioritaire initiatief voor het verwijderen van terroristische online-inhoud**.

Parallel hiermee zet de Commissie de samenwerking met onlineplatforms voort in het kader van het **EU-internetforum**[8]. Zoals aangekondigd door voorzitter Juncker op de bijeenkomst van 15 mei 2019 in Parijs over de "Christchurch Call to Action", is de Commissie samen met Europol begonnen aan de ontwikkeling van een **EU-crisisprotocol** dat overheden en internetplatforms in staat moet stellen snel en gecoördineerd te reageren op de verspreiding van terroristische online-inhoud, bijvoorbeeld onmiddellijk na een terroristische aanslag. Deze werkzaamheden maken deel uit van de internationale inspanningen voor de uitvoering van de "Christchurch Call to Action". Naast verdere besprekingen met de lidstaten en de sector en een voor september 2019 geplande oefening om een noodsituatie te simuleren, zal de Commissie op 7 oktober 2019 een ministeriële bijeenkomst van het EU-internetforum beleggen met het oog op de bekrachtiging van het EU-crisisprotocol.

Bovendien blijft de Commissie **ondersteuning verlenen aan de lidstaten en lokale actoren bij het voorkomen en tegengaan van radicalisering** op het terrein in lokale gemeenschappen in heel Europa. Hiervoor zijn duurzame inspanningen op de lange termijn vereist waarbij alle relevante actoren op lokaal, nationaal en EU-niveau worden betrokken. De **stuurgroep voor EU-maatregelen ter voorkoming en bestrijding van radicalisering**, die in augustus 2018 is opgericht om de Commissie te adviseren over de wijze waarop de beleidsrespons van de EU op dit gebied kan worden versterkt, heeft op 17 juni 2019 haar tweede vergadering gehouden over verdere acties op prioritaire gebieden, zoals de bestrijding van radicalisering in gevangenissen en van extremistische ideologieën. Aangezien eerstelijns- en veldwerkers vaak het best geplaatst zijn om voortekens van radicalisering te herkennen en aan te pakken, blijft het door de EU gefinancierde **netwerk voor voorlichting over radicalisering**[9] ondersteuning bieden aan eerstelijnshulpverleners. Het netwerk verbindt ca. 5 000 beroepsmensen uit maatschappelijke organisaties, scholen en de politie, alsook nationale coördinatoren en beleidsmakers.

De recente samenwerking tussen eerstelijnswerkers binnen het netwerk heeft de extreemrechtse problematiek inzichtelijker gemaakt. Dit jaar zal het netwerk voor voorlichting over radicalisering informatiebladen publiceren om beleidsmakers en beroepsmensen te helpen de belangrijkste vormen en uitingen van rechts-extremisme en islamitisch extremisme te herkennen aan de hand van sleutelverhalen, taal, vormen, symbolen, typologieën, strategieën en zo meer. Tot slot steunt de

---

8 Het **EU-internetforum** fungeert sinds 2015 als kader voor een vrijwillig partnerschap tussen de ministers van Binnenlandse Zaken van de EU, de internetsector en andere belanghebbenden, met als doel het misbruik van het internet door terroristische groepen aan te pakken en de burgers te beschermen.

9 De Commissie heeft het **netwerk voor voorlichting over radicalisering** in 2011 opgericht om eerstelijns- en veldwerkers samen te brengen. In 2015 heeft de Commissie het netwerk versterkt met het kenniscentrum voor voorlichting over radicalisering, om meer gerichte begeleiding, ondersteuning en adviesverlening voor de belanghebbenden in de lidstaten te ontwikkelen en de deskundigheid en vaardigheden van verschillende actoren te vergroten. Voor meer informatie over de activiteiten van het netwerk voor voorlichting over radicalisering, zie: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

Commissie door **steden** geleide initiatieven voor de bestrijding van radicalisering, aangezien lokale actoren en steden de frontlinie vormen als het erop aankomt radicalisering te voorkomen en tegen te gaan. Naar aanleiding van de conferentie over "EU-steden tegen radicalisering" van 26 februari 2019 heeft op 8 juli 2019 de eerste vergadering plaatsgevonden van een proefgroep van ongeveer 20 steden. Deze werd georganiseerd door de burgemeester van Straatsburg en had tot doel de uitwisseling van beste praktijken en de inspanningen van de steden op dit gebied te intensiveren.

Tegelijkertijd wordt voortgewerkt aan het ondersteunen van partnerlanden bij het aanpakken van potentieel tot terrorisme leidende radicalisering, onder meer in gevangenissen.

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

- onderhandelingen te beginnen over het wetgevingsvoorstel om de verspreiding van **terroristische online-inhoud** te voorkomen, met het oog op een snel akkoord over een EU-regelgevingskader met duidelijke regels en waarborgen.

2. Cyberbeveiliging verbeteren

Cyberbeveiliging blijft een essentiële uitdaging op het gebied van veiligheid. De EU heeft grote vooruitgang[10] geboekt bij het aanpakken van "klassieke", op systemen en data gerichte cyberbedreigingen, door de maatregelen uit te voeren die zijn opgenomen in de gezamenlijke mededeling[11] van september 2017 "Weerbaarheid, afschrikking en defensie: bouwen aan sterke cyberbeveiliging voor de EU". In dit verband is onder meer de EU-cyberbeveiligingsverordening[12] vastgesteld, die het Agentschap van de Europese Unie voor cyberbeveiliging een permanent mandaat verleent, de rol van het agentschap versterkt en een EU-kader voor cyberbeveiligingscertificering invoert. De Commissie heeft zich ook gebogen over sectorspecifieke vereisten, bijvoorbeeld in haar aanbeveling van 3 april 2019 over cyberbeveiliging in de energiesector[13]. Omdat de activiteiten van kwaadwillige actoren ten aanzien van uiteenlopende doelwitten en slachtoffers echter verder toenemen, blijft het voor het EU een prioriteit om op te treden tegen cybercriminaliteit en de cyberbeveiliging te verbeteren.

Het Europees Parlement en de Raad moeten nog overeenstemming bereiken over het prioritaire initiatief van de Commissie inzake het **Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra**[14]. Het voorstel heeft tot doel de technologische en industriële capaciteiten voor cyberbeveiliging te ondersteunen en het concurrentievermogen van de cyberbeveiligingssector van de Unie te vergroten. Beide medewetgevers hebben hun onderhandelingsmandaat in maart 2019 vastgesteld. Aangezien de interinstitutionele onderhandelingen niet meer konden worden afgerond voor het einde van de vorige zittingsperiode van het Europees Parlement, heeft het Europees Parlement zijn standpunt formeel vastgesteld in eerste lezing. In de tussentijd worden de besprekingen tussen de lidstaten in de Raad voortgezet, met bijzondere aandacht voor de interactie tussen de voorgestelde verordening tot

[10] Voor meer informatie, zie de brochure over "Bouwen aan sterke cyberbeveiliging in de Europese Unie: weerbaarheid, afschrikking en defensie": https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

[11] JOIN(2017) 450 final van 13.9.2017.

[12] Met de EU-cyberbeveiligingsverordening (Verordening (EU) 2019/881 van 17 april 2019) worden voor het eerst EU-brede regels ingevoerd voor de cyberbeveiligingscertificering van producten, processen en diensten. Daarnaast voorziet de cyberbeveiligingsverordening in een nieuw permanent mandaat voor het Agentschap van de Europese Unie voor cyberbeveiliging en wijst zij meer middelen aan het agentschap toe om het in staat te stellen zijn doelstellingen te verwezenlijken. Voor meer informatie over de oproep tot het indienen van voorstellen, zie: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

[13] C(2019) 2400 final van 3.4.2019 en SWD(2019) 1240 final van 3.4.2019.

[14] COM(2018) 630 final van 12.9.2018.

oprichting van het kenniscentrum en het netwerk voor cyberbeveiliging enerzijds, en de programma's Horizon Europa en Digitaal Europa anderzijds. **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.**

Intussen blijft de Commissie **steun** verlenen **voor onderzoek en innovatie** in verband met cyberbeveiliging, door binnen het huidig meerjarig financieel kader 135 miljoen EUR uit te trekken voor projecten op het gebied van cyberbeveiliging in kritieke infrastructuren, intelligente beveiliging en privacybeheer, en instrumenten die specifiek bedoeld zijn voor burgers en kleine en middelgrote ondernemingen[15]. In juli 2019 heeft de Commissie in het kader van het programma *Connecting Europe Facility* een nieuwe oproep tot het indienen van voorstellen gelanceerd, in het kader waarvan 10 miljoen EUR aan EU-financiering beschikbaar wordt gesteld voor belangrijke actoren die worden vermeld in de richtlijn inzake de beveiliging van netwerk- en informatiesystemen (NIS-richtlijn)[16], zoals Europese *computer security incident response teams*, aanbieders van essentiële diensten (zoals banken, ziekenhuizen, nutsbedrijven, spoorwegen, luchtvaartmaatschappijen, aanbieders van domeinnamen) en diverse overheidsinstanties. Voor het eerst kunnen de Europese autoriteiten voor cyberbeveiligingscertificering nu ook een aanvraag voor dit programma indienen. Deze mogelijkheid is gecreëerd om hen in staat te stellen de EU-cyberbeveiligingsverordening ten uitvoer te leggen.

Op 17 mei 2019 heeft de Raad een **sanctieregeling** vastgesteld op grond waarvan de EU gerichte beperkende maatregelen kan opleggen om cyberaanvallen die een externe bedreiging voor de EU of haar lidstaten vormen, te ontmoedigen en af te weren. De nieuwe sanctieregeling maakt deel uit van het **EU-instrumentarium voor cyberdiplomatie**[17], een kader voor een gezamenlijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten[18] dat de EU in staat stelt de maatregelen in het kader van het gemeenschappelijk buitenlands en veiligheidsbeleid optimaal in te zetten om kwaadwillige cyberactiviteiten te ontmoedigen en erop te reageren.

De EU neemt niet alleen maatregelen tegen cyberbedreigingen die gericht zijn op systemen en gegevens, maar ook tegen de complexe en veelzijdige uitdagingen die gepaard gaan met **hybride dreigingen**[19]. In zijn conclusies van 21 juni 2019[20] onderstreept de Europese Raad dat de EU *"een gecoördineerde respons op hybride en cyberdreigingen* [moet] *bieden en intensiever* [moet] *samenwerken met de betrokken internationale actoren"*. De Commissie is verheugd dat de bestrijding van hybride dreigingen ook een prioriteit is van het Finse voorzitterschap van de Raad en dat tijdens de informele bijeenkomst van de ministers van Justitie en Binnenlandse Zaken in Helsinki op 18-19 juli 2019 een op scenario's gebaseerde beleidsbespreking over hybride dreigingen heeft plaatsgevonden. Ook de directeuren defensiebeleid van de EU en de politieke directeuren van de EU hebben dergelijke op scenario's gebaseerde besprekingen gevoerd, respectievelijk op 7-8 juli 2019 en op 9-10 juli 2019. Tijdens een gezamenlijke informele bijeenkomst van de ministers van Buitenlandse Zaken en van Defensie op 29-30 augustus 2019 zal daarover verslag worden uitgebracht.

---

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Richtlijn (EU) 2016/1148 van 6.7.2016.

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/nl/pdf

18 Hieronder vallen zowel cyberaanvallen als pogingen tot cyberaanvallen met potentieel aanzienlijke gevolgen, onder meer door middel van toegang tot informatiesystemen of interceptie van gegevens via digitale infrastructuur zoals 5G-netwerken (zie ook deel III over de verbetering van de beveiliging van digitale infrastructuur).

19 Zie het verslag over de tenuitvoerlegging van het gezamenlijk kader van 2016 voor de bestrijding van hybride dreigingen en de gezamenlijke mededeling van 2018 over het opbouwen van weerbaarheid en reactiecapaciteit tegen hybride bedreigingen (SWD(2019) 200 final van 28.5.2019). Zie ook het wetgevingsvoorstel van september 2016 voor een verordening tot instelling van een EU-regeling voor controle op de uitvoer, de overbrenging, de tussenhandel, de technische bijstand en de doorvoer van producten voor tweeërlei gebruik (herschikking) (COM(2016) 616 final van 28.9.2016).

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-nl.pdf

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**.

3. De toegang van rechtshandhavingsinstanties tot elektronisch bewijsmateriaal verbeteren

De EU heeft verdere actie ondernomen om terroristen en criminelen af te snijden van de middelen voor hun activiteiten, door de toegang tot precursoren voor explosieven[21], financiering van hun activiteiten[22] en mogelijkheden om onopgemerkt te reizen[23] voor hen te bemoeilijken.

De onderhandelingen over de voorstellen van de Commissie van april 2018 om de **toegang** van rechtshandhavingsinstanties **tot elektronisch bewijsmateriaal** te verbeteren, moeten zo snel mogelijk worden afgerond. In meer dan de helft van alle strafrechtelijke onderzoeken wordt tegenwoordig een grensoverschrijdend verzoek om toegang tot elektronisch bewijsmateriaal ingediend[24]. De Raad heeft zijn onderhandelingsstandpunt bepaald ten aanzien van de voorstellen voor een verordening[25] ter verbetering van de grensoverschrijdende toegang tot elektronisch bewijsmateriaal in het kader van strafrechtelijk onderzoek, en voor een richtlijn[26] tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures. Gezien het cruciale belang van efficiënte toegang tot elektronisch bewijsmateriaal voor het onderzoek en de vervolging van grensoverschrijdende criminaliteit zoals terrorisme of cybercriminaliteit, verzoekt de Commissie het Europees Parlement met klem om vaart te zetten achter de behandeling van dit voorstel met het oog op een snelle vaststelling ervan door de medewetgevers.

Tegelijkertijd streeft de Commissie ernaar de **internationale uitwisseling van elektronisch bewijsmateriaal** te verbeteren en van de nodige waarborgen te voorzien. Zij doet dit in het kader van de lopende onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit en in de onderhandelingen met de Verenigde Staten, en houdt zich daarbij aan de onderhandelingsmandaten die de Raad tijdens de zitting van de Raad Justitie en Binnenlandse Zaken van 6-7 juni 2019 heeft aangenomen[27]. De Commissie heeft op 9-11 juli 2019 deelgenomen aan de laatste ronde van de onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest van de Raad van Europa inzake cybercriminaliteit. De Commissie en de Verenigde Staten treffen momenteel de technische voorbereidingen voor het officiële begin van de onderhandelingen over een onderlinge overeenkomst over grensoverschrijdende toegang tot elektronisch bewijsmateriaal.

---

21 Verordening (EU) 2019/1148 van 20 juni 2019 over het op de markt brengen en het gebruik van precursoren voor explosieven.

22 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.

23 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.

24 In ongeveer 85 % van de strafrechtelijke onderzoeken is elektronisch bewijsmateriaal nodig en in twee derde van deze onderzoeken moet bewijsmateriaal worden aangevraagd bij aanbieders van onlinediensten die in een ander rechtsgebied gevestigd zijn. Zie de effectbeoordeling bij het wetgevingsvoorstel (SWD(2018) 118 final van 17.4.2018).

25 COM(2018) 225 final van 17.4.2018. De Raad heeft tijdens de Raad Justitie en Binnenlandse Zaken van 7 december 2018 zijn onderhandelingsmandaat voor het voorstel voor een verordening aangenomen.

26 COM(2018) 226 final van 17.4.2018. De Raad heeft tijdens de Raad Justitie en Binnenlandse Zaken van 8 maart 2019 zijn onderhandelingsstandpunt over het voorstel voor een richtlijn bepaald.

27 https://www.consilium.europa.eu/nl/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

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

- zijn onderhandelingsmandaat goed te keuren voor de wetgevingsvoorstellen inzake **elektronisch bewijsmateriaal**, zodat de trialoogbesprekingen met de Raad spoedig van start kunnen gaan *(prioriteit van de gezamenlijke verklaring).*

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

De Commissie heeft regels voor de **interoperabiliteit van informatiesystemen**[28] vastgesteld die informatielacunes zullen opvullen en blinde vlekken zullen wegnemen door meervoudige identiteiten te helpen opsporen en identiteitsfraude tegen te gaan. Kort daarna heeft zij een reeks initiatieven gelanceerd om de lidstaten te ondersteunen bij het uitvoeringsproces, onder meer door waar nodig financiering te verstrekken en door workshops te organiseren om de uitwisseling van expertise en beste praktijken te vergemakkelijken. 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.

Om dit doel te bereiken, is het bovendien noodzakelijk snel en volledig uitvoering te geven aan de onlangs vastgestelde wetgeving voor de invoering van nieuwe informatiesystemen (het inreis-uitreissysteem van de EU[29] en het Europees systeem voor reisinformatie en -autorisatie[30]), voor de versterking van het Schengeninformatiesysteem[31] en voor de uitbreiding van het Europees Strafregisterinformatiesysteem[32] tot onderdanen van derde landen. De nieuwe architectuur voor krachtigere en slimmere informatiesystemen voor veiligheid, grens- en migratiebeheer zal op het terrein alleen een verschil kunnen maken als alle componenten op het niveau van de Unie en door elke lidstaat volledig en volgens het overeengekomen tijdschema worden geïmplementeerd.

Tegelijkertijd moeten de medewetgevers verdere actie ondernemen om de werkzaamheden op het gebied van de krachtigere en slimmere informatiesystemen voor veiligheids-, grens- en migratiebeheer te voltooien.
De Commissie heeft in het kader van de technische uitvoering van het **Europees systeem voor reisinformatie en -autorisatie** op 7 januari 2019 twee voorstellen ingediend met technische wijzigingen van de betrokken verordening[33] die nodig zijn om het systeem volledig op te zetten. De Commissie roept de medewetgevers op om hun werkzaamheden met betrekking tot de technische wijzigingen voort te zetten teneinde zo snel mogelijk tot een akkoord te komen, zodat het Europees systeem voor reisinformatie en -autorisatie snel en tijdig kan worden ingevoerd en begin 2021 operationeel kan worden.

In mei 2018 heeft de Commissie een voorstel ter **versterking van het bestaande Visuminformatiesysteem**[34] ingediend dat voorziet in een grondiger onderzoek van de antecedenten van visumaanvragers en dat informatielacunes opvult door een betere uitwisseling van informatie tussen de lidstaten.
De Raad heeft zijn onderhandelingsmandaat vastgesteld op 19 december 2018 en op 13 maart 2019 heeft het Europees Parlement in plenaire zitting zijn verslag over het voorstel in stemming gebracht en

28 Verordening (EU) 2019/817 van 20.5.2019 en Verordening (EU) 2019/818 van 20.5.2019.
29 Verordening (EU) 2017/2226 van 30.11.2017.
30 Verordening (EU) 2018/1240 van 12.9.2018 en Verordening (EU) 2018/1241 van 12.9.2018.
31 Verordening (EU) 2018/1860 van 28.11.2018, Verordening (EU) 2018/1861 van 28.11.2018, Verordening (EU) 2018/1862 van 28.11.2018.
32 Verordening (EU) 2019/816 van 17.4.2019.
33 COM(2019) 3 final en COM(2019) 4 final van 7.1.2019.
34 COM(2018) 302 final van 16.5.2018.

daarmee zijn eerste lezing afgerond. De Commissie roept de medewetgevers op om tijdens de volgende zittingsperiode van het Europees Parlement snel met de onderhandelingen van start te gaan.

In mei 2016 heeft de Commissie voorgesteld het toepassingsgebied van **Eurodac**[35] uit te breiden zodat niet alleen de identificatie van asielzoekers eronder valt, maar ook die van onderdanen van derde landen die illegaal in de EU verblijven en/of de EU op irreguliere wijze binnenkomen. In overeenstemming met de conclusies van de Europese Raad van december 2018[36] en de mededeling van de Commissie van 6 maart 2019 met het voortgangsverslag over de uitvoering van de Europese migratieagenda[37] roept de Commissie de medewetgevers op het voorstel vast te stellen. De vaststelling van dit wetgevingsvoorstel is nodig om Eurodac in te bedden in de toekomstige architectuur van interoperabele EU-informatiesystemen en in dit systeem ook de cruciale gegevens te integreren van onderdanen van derde landen die illegaal in de EU verblijven en/of de EU op irreguliere wijze binnenkomen.

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

- het wetgevingsvoorstel betreffende **Eurodac** vast te stellen *(prioriteit van de gezamenlijke verklaring)*;
- vooruitgang te boeken teneinde snel een akkoord te bereiken over de voorgestelde technische wijzigingen die nodig zijn voor de invoering van het **Europees systeem voor reisinformatie en -autorisatie**.

III. VERBETERING VAN DE BEVEILIGING VAN DIGITALE INFRASTRUCTUUR

De robuustheid van onze digitale infrastructuur is cruciaal voor de overheid, het bedrijfsleven, de veiligheid van onze persoonsgegevens en de werking van onze democratische instellingen. De **netwerken van de vijfde generatie (5G)** die de komende jaren worden uitgerold, zullen de digitale ruggengraat van onze samenlevingen en economieën vormen en zullen miljarden burgers, objecten en systemen, onder meer in kritieke sectoren zoals energie, vervoer, bankieren en gezondheidszorg, verbinden, evenals industriële besturingssystemen die gevoelige informatie doorgeven en veiligheidssystemen ondersteunen.

Naar verwachting zal de wereldwijde 5G-omzet in 2025 zo'n 225 miljard euro bedragen. Daarom is 5G voor Europa een belangrijke troef om op de wereldmarkt te kunnen concurreren en is **de beveiliging van 5G-netwerken cruciaal voor de strategische autonomie van de Unie**. Het waarborgen van een hoog niveau van cyberbeveiliging vereist gecoördineerde maatregelen op nationaal en Europees niveau, aangezien elke kwetsbaarheid in de 5G-netwerken van één lidstaat de Unie in haar geheel zou treffen.

Na de steun van de staatshoofden en regeringsleiders te hebben gekregen tijdens de bijeenkomst van de Europese Raad in maart 2019[38], heeft de Commissie op 26 maart 2019 een **aanbeveling over de cyberbeveiliging van 5G-netwerken**[39] gepresenteerd waarin maatregelen zijn opgenomen om de cyberbeveiligingsrisico's voor 5G-netwerken te beoordelen en de preventieve maatregelen te versterken. De aanbevelingen bouwen voort op de gecoördineerde EU-maatregelen voor risicobeoordeling en risicobeheer, een doeltreffend kader voor samenwerking en informatie-uitwisseling en een gezamenlijk situationeel bewustzijn van de EU ten aanzien van kritieke communicatienetwerken.

---

35 COM(2016) 272 final van 4.5.2016.

36 https://www.consilium.europa.eu/nl/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/

37 COM(2019) 126 final van 6.3.2019.

38 https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/nl/pdf

39 C(2019) 2335 final van 26.3.2019.

In de **eerste fase** van het proces dat met de aanbeveling van start is gegaan, hebben alle lidstaten uiterlijk op 15 juli 2019 hun **nationale risicobeoordeling** afgerond en hun bevindingen aan de Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging voorgelegd, of te kennen gegeven dat zij dit binnenkort zouden doen. Om de consistentie te bevorderen en de uitwisseling van informatie over de nationale resultaten op EU-niveau te vergemakkelijken, hebben de lidstaten en de Commissie vooraf een leidraad en een gemeenschappelijk rapportagemodel uitgewerkt voor het opstellen van de nationale risicobeoordelingen. Onder meer de volgende parameters werden in alle lidstaten beoordeeld:

- de belangrijkste dreigingen en dreigingsactoren op het gebied van 5G-netwerken;
- de gevoeligheid van componenten en functies van 5G-netwerken en andere apparatuur; en
- kwetsbaarheden van uiteenlopende aard (technische of andere), onder meer in verband met de 5G-toeleveringsketen.

Het feit dat tal van verantwoordelijke actoren uit de lidstaten (waaronder voor cyberbeveiliging en telecommunicatie bevoegde autoriteiten en veiligheids- en inlichtingendiensten) betrokken zijn bij de werkzaamheden op het gebied van de nationale risicobeoordelingen, heeft bijgedragen tot de onderlinge samenwerking en coördinatie tussen deze instanties. Parallel met deze werkzaamheden hebben sommige lidstaten in het licht van hun tijdschema voor de uitrol van 5G al stappen ondernomen om de beveiligingseisen op dit gebied te versterken, en hebben andere te kennen gegeven dat zij plan zijn in de nabije toekomst nieuwe maatregelen te overwegen.

Op basis van de resultaten van de nationale risicobeoordeling zullen de cyberbeveiligingsautoriteiten van de lidstaten in de Groep voor samenwerking op het gebied van de beveiliging van netwerk- en informatiesystemen[40] uiterlijk op 1 oktober 2019 een **gezamenlijke evaluatie van de risico's op EU-niveau** opstellen. Dit is de tweede fase van het proces dat in het kader van de aanbeveling is opgestart. Op basis daarvan zal de samenwerkingsgroep in de derde fase uiterlijk op 31 december 2019 een **gemeenschappelijk EU-instrumentarium van risicobeperkende maatregelen** voorbereiden om de vastgestelde risico's aan te pakken. De Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging zullen de uitvoering van de aanbeveling blijven ondersteunen.

De werkzaamheden van de Groep voor samenwerking op het gebied van de beveiliging van netwerk- en informatiesystemen worden ondersteund door verschillende andere fora. Het Orgaan van Europese regelgevende instanties voor elektronische communicatie werkt aan een overzicht van alle bestaande beveiligingsmaatregelen die relevant kunnen zijn voor 5G. Binnen het Agentschap van de Europese Unie voor cyberbeveiliging is een nieuwe specifieke deskundigengroep begonnen met de werkzaamheden aan het 5G-dreigingslandschap. Daarnaast zullen de Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging na de inwerkingtreding van de cyberbeveiligingsverordening op 27 juni 2019 alle maatregelen nemen die nodig zijn om het EU-brede certificeringskader op te zetten. De lidstaten zijn in juni 2019 in het Comité voor normen bijeengekomen voor een bespreking over cyberbeveiliging en normalisatie. Aanleiding daarvoor was de aanbeveling zich te bezinnen over de toekomstige uitdagingen op het gebied van normalisatie inzake cyberbeveiliging, onder meer van 5G-netwerken, alsook over passende beleidsinitiatieven op EU-niveau.

[40] De Groep voor samenwerking op het gebied van de beveiliging van netwerk- en informatiesystemen is opgericht in het kader van Richtlijn (EU) 2016/1148 van 6 juli 2016 inzake de beveiliging van netwerk- en informatiesystemen. Zoals beoogd in de aanbeveling, is binnen de samenwerkingsgroep een specifieke werkstroom opgezet, onder leiding van verschillende lidstaten. De groep is al drie keer bijeengekomen – in april, mei en juli 2019 – om informatie over de aanpak van de lidstaten uit te wisselen en te bespreken hoe de voorbereiding van de gecoördineerde risicobeoordeling van de EU kan worden vergemakkelijkt.

De beveiliging van 5G-netwerken is van strategisch belang voor de Unie. Buitenlandse investeringen in strategische sectoren, verwerving van kritieke activa, technologie en infrastructuur in de Unie en levering van kritieke uitrusting kunnen ook potentiële risico's voor de veiligheid van de Unie vormen.

Het nieuwe **EU-kader voor de screening van buitenlandse directe investeringen**[41] is op 10 april 2019 officieel in werking getreden. De Commissie en de lidstaten zullen de komende 18 maanden de nodige maatregelen treffen om ervoor te zorgen dat de EU de verordening inzake de screening van investeringen met ingang van 11 oktober 2020 volledig kan toepassen.

IV. BESTRIJDING VAN WITWASSEN

Omdat het criminelen en terroristen slechts enkele uren tijd kost om geld tussen bankrekeningen over te maken, kunnen zij hun terreurdaden gemakkelijker voorbereiden of de opbrengsten van misdrijven illegaal witwassen, over de grenzen van verschillende lidstaten heen. Om dit probleem aan te pakken, heeft de Unie een solide **regelgevingskader voor de bestrijding van het witwassen van geld en de financiering van terrorisme** ontwikkeld, overeenkomstig de door de Financiële-actiegroep aangenomen internationale normen.

Gezien de noodzaak om gelijke tred te houden met de evoluerende trends, de technologische ontwikkelingen en de vindingrijkheid van criminelen om hiaten of lacunes in het systeem te benutten, heeft de Commissie op 24 juli 2019 een **pakket van vier verslagen** goedgekeurd waarin de bestaande risico's en kwetsbaarheden in verband met witwassen worden geanalyseerd en wordt beoordeeld hoe het kader door de relevante actoren in zowel de particuliere als de publieke sector wordt toegepast[42].

Het pakket omvat een **beoordeling van de mogelijke koppeling van nationale centrale registers van bankrekeningen en systemen voor gegevensontsluiting** in de EU. Met dergelijke nationale gecentraliseerde systemen is het mogelijk natuurlijke of rechtspersonen te identificeren die houder zijn van of zeggenschap hebben over betaalrekeningen, bankrekeningen en kluizen – informatie die voor de bevoegde autoriteiten vaak van cruciaal belang is in de strijd tegen witwassen en de financiering van terrorisme. Op grond van de vijfde antiwitwasrichtlijn[43] zijn de lidstaten verplicht dergelijke nationale gecentraliseerde systemen in te voeren en hun nationale financiële-inlichtingeneenheden rechtstreeks toegang te verlenen. Op grond van de onlangs aangenomen regels om het gebruik van financiële informatie ter bestrijding van zware criminaliteit te vergemakkelijken[44], krijgen aangewezen rechtshandhavingsinstanties en bureaus voor de ontneming van vermogensbestanddelen rechtstreeks toegang tot hun respectieve nationale centrale registers van bankrekeningen. Op basis daarvan gaat het

---

41 Verordening (EU) 2019/452 van 19 maart 2019 tot vaststelling van een kader voor de screening van buitenlandse directe investeringen in de Unie. Met het nieuwe kader wordt een samenwerkingsmechanisme opgezet dat de lidstaten en de Commissie de mogelijkheid biedt informatie uit te wisselen en problemen met betrekking tot specifieke investeringen aan de orde te stellen. De Commissie zal in het kader van het mechanisme adviezen kunnen uitbrengen als de veiligheid of de openbare orde van meer dan één lidstaat door een investering in het gedrang komt of als een investering een project of programma dat voor de hele EU van belang is zou kunnen ondermijnen. De lidstaat waar de investering wordt gedaan, heeft het laatste woord over de wijze waarop de investering moet worden behandeld.

42 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 final van 24.7.2019 – niet beschikbaar in het Nederlands), verslag over de koppeling van nationale gecentraliseerde automatische mechanismen (centrale registers of centrale elektronische systemen voor gegevensontsluiting) op bankrekeningen (COM(2019) 372 final van 24.7.2019 – niet beschikbaar in het Nederlands), verslag over de beoordeling van recente gevallen van witwaspraktijken waarbij kredietinstellingen van de EU betrokken zouden zijn (COM(2019) 373 final van 24.7.2019 – niet beschikbaar in het Nederlands), verslag over de beoordeling van het kader voor samenwerking tussen financiële-inlichtingeneenheden (COM(2019) 371 final van 24.7.2019 – niet beschikbaar in het Nederlands).

43 Richtlijn (EU) 2015/849 van 20.5.2015.

44 Richtlijn (EU) 2019/1153 van 20.6.2019.

verslag, overeenkomstig de vereiste uit hoofde van de antiwitwasrichtlijn, in op verschillende IT-oplossingen op EU-niveau die al operationeel zijn of zich nog in de ontwikkelingsfase bevinden en die kunnen dienen als model voor een mogelijke koppeling van de nationale gecentraliseerde systemen. Aangezien een toekomstige EU-brede koppeling van de gecentraliseerde mechanismen de toegang tot financiële informatie zou versnellen en de grensoverschrijdende samenwerking van de bevoegde autoriteiten zou vergemakkelijken, is de Commissie van plan verder overleg te plegen met de relevante belanghebbenden, overheden, financiële-inlichtingeneenheden, rechtshandhavingsinstanties en bureaus voor de ontneming van vermogensbestanddelen, aangezien dit de potentiële "eindgebruikers" van een systeem voor interconnectie zijn.

In het kader van het beraad van de Commissie over het werk van de financiële-inlichtingeneenheden wordt in een verslag waarin de **samenwerking tussen de financiële-inlichtingeneenheden** wordt beoordeeld, gekeken naar de samenwerking binnen de Unie en met derde landen[45]. In het verslag worden bepaalde tekortkomingen aan het licht gebracht die waarschijnlijk zullen blijven bestaan totdat de taken en de plichten van de financiële-inlichtingeneenheden op het gebied van grensoverschrijdende samenwerking duidelijker worden omschreven in het EU-rechtskader voor de bestrijding van witwassen en van de financiering van terrorisme. Uit de beoordeling blijkt ook dat er behoefte is aan een sterker mechanisme voor de coördinatie en ondersteuning van grensoverschrijdende samenwerking en analyse.

Parallel met de bestaande inspanningen om witwassen en de financiering van terrorisme aan te pakken, zal de Commissie – tevens naar aanleiding van een oproep van het Europees Parlement[46] – de noodzaak, de technische haalbaarheid en de evenredigheid van aanvullende maatregelen voor het traceren van terrorismefinanciering in de EU blijven beoordelen[47].

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

1. Uitvoering van wetgevingsmaatregelen in het kader van de Veiligheidsunie

Een akkoord over maatregelen in het kader van de Veiligheidsunie is niet het einde van het proces – het is van essentieel belang, wil men ervoor zorgen dat de maatregelen snel en volledig door de lidstaten worden uitgevoerd en optimaal voordeel opleveren. Met het oog daarop ondersteunt de Commissie de lidstaten hier actief bij, bijvoorbeeld door financiering te verstrekken en de uitwisseling van goede praktijken te faciliteren. De Commissie staat echter ook klaar om, waar nodig, gebruik te maken 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 tenuitvoerlegging van de **EU-richtlijn betreffende persoonsgegevens van passagiers**[48] is op 25 mei 2018 verstreken. Tot nu toe hebben 25 lidstaten de Commissie ervan in kennis gesteld dat zij de richtlijn volledig hebben omgezet[49]. In twee lidstaten is de omzetting nog niet

---

45 Deze beoordeling is vereist op grond van artikel 65, lid 2, van de vijfde antiwitwasrichtlijn (Richtlijn (EU) 2018//843 van 30.5.2018).

46 In haar in december 2018 aangenomen eindverslag heeft de Bijzondere Commissie terrorisme van het Europees Parlement opgeroepen tot de oprichting van een Europees systeem voor het traceren van terrorismefinanciering, dat gericht is op transacties van particulieren met banden met terrorisme en de financiering daarvan in de gemeenschappelijke eurobetalingsruimte.

47 Zie het achttiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2019) 145 final van 20.3.2019).

48 Richtlijn (EU) 2016/681 van 27.4.2016.

49 De verwijzingen naar de melding van 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.

volledig, ondanks de inbreukprocedures die op 19 juli 2018 zijn ingeleid[50]. 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**[51] is verstreken op 8 september 2018. Tot nu toe hebben 22 lidstaten de Commissie ervan in kennis gesteld dat zij de richtlijn volledig hebben omgezet. Drie lidstaten hebben nog steeds geen kennisgeving gedaan van de vaststelling van nationale wetgeving waarbij de richtlijn volledig wordt omgezet – en dit ondanks de inbreukprocedures die op 22 november 2018 zijn ingeleid[52].

De termijn voor de omzetting van de **richtlijn inzake de controle op de verwerving en het voorhanden hebben van wapens**[53] is verstreken op 14 september 2018. Tot nu toe hebben acht lidstaten de Commissie ervan in kennis gesteld dat zij de richtlijn volledig hebben omgezet. Twintig lidstaten hebben nog steeds geen kennisgeving gedaan van de vaststelling van nationale wetgeving waarbij de richtlijn volledig wordt omgezet – en dit ondanks de inbreukprocedures die op 22 november 2018 zijn ingeleid[54].

De termijn voor de omzetting in nationaal recht van de **richtlijn gegevensbescherming bij rechtshandhaving**[55] is verstreken op 6 mei 2018. Tot nu toe hebben twintig lidstaten de Commissie ervan in kennis gesteld dat zij de richtlijn volledig hebben omgezet[56]. Zeven lidstaten hebben nog steeds geen kennisgeving gedaan van de vaststelling van nationale wetgeving waarbij de richtlijn volledig wordt omgezet – en dit ondanks de inbreukprocedures die de Commissie op 19 juli 2018 heeft ingeleid[57].

De lidstaten hadden tot en met 9 mei 2018 de tijd om de **richtlijn inzake de beveiliging van netwerk- en informatiesystemen**[58] in nationaal recht om te zetten. Tot nu toe hebben 26 lidstaten de Commissie in kennis gesteld van de volledige omzetting van de richtlijn en hebben twee lidstaten de richtlijn gedeeltelijk omgezet[59]. Bovendien moesten de lidstaten uiterlijk op 9 november 2018 in overeenstemming met de richtlijn aanbieders van essentiële diensten identificeren. Uiterlijk op 9 mei 2019 moest de Commissie bij het Europees Parlement en de Raad een verslag indienen over de coherentie bij de identificatie van aanbieders van essentiële diensten op het grondgebied van de lidstaten. Aangezien een aantal lidstaten nog geen volledige informatie over het identificatieproces had verstrekt, heeft de Commissie de verslaglegging echter moeten uitstellen.

De Commissie beoordeelt de omzetting van de **vierde antiwitwasrichtlijn**[60] en gaat ook na of de lidstaten de regels correct toepassen. De Commissie heeft tegen 24 lidstaten inbreukprocedures

---

50 Slovenië heeft gedeeltelijke omzetting gemeld. Spanje heeft geen kennisgeving van omzetting gedaan (stand van zaken op 24 juli 2019).

51 Richtlijn (EU) 2017/541 van 15.3.2017.

52 Polen heeft gedeeltelijke omzetting gemeld. Griekenland en Luxemburg hebben geen kennisgeving van omzetting gedaan (stand van zaken op 24 juli 2019).

53 Richtlijn (EU) 2017/853 van 17.5.2017.

54 België, Tsjechië, Estland, Litouwen, Polen, Portugal, Zweden en het Verenigd Koninkrijk hebben gedeeltelijke omzetting gemeld. Duitsland, Ierland, Griekenland, Spanje, Cyprus, Luxemburg, Hongarije, Nederland, Roemenië, Slovenië, Slowakije en Finland hebben geen kennisgeving van omzetting gedaan (stand van zaken op 24 juli 2019).

55 Richtlijn (EU) 2016/680 van 27.4.2016.

56 Twintig lidstaten hebben de omzetting afgerond (stand van zaken op 24 juli 2019).

57 Letland, Portugal, Slovenië en Finland hebben gedeeltelijke omzetting gemeld. Griekenland en Spanje hebben geen kennisgeving van omzetting gedaan. Duitsland heeft volledige omzetting gemeld, maar de Commissie beschouwt de omzetting niet als volledig (stand van zaken op 24 juli 2019).

58 Richtlijn (EU) 2016/1148 van 27.4.2016.

59 België en Hongarije hebben de richtlijn gedeeltelijk omgezet (stand van zaken op 24 juli 2019).

60 Richtlijn (EU) 2015/849 van 20.5.2015.

ingeleid, 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[61].

De Commissie roept de lidstaten op om 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[62];
- 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[63];
- de **richtlijn inzake de controle op de verwerving en het voorhanden hebben van wapens**: twaalf lidstaten moeten nog kennisgeving doen van omzetting in nationaal recht en acht lidstaten moeten nog kennisgeving doen van de vervollediging van de omzetting[64];
- de **richtlijn gegevensbescherming bij rechtshandhaving**: twee lidstaten moeten nog kennisgeving doen van omzetting in nationaal recht en vijf lidstaten moeten nog kennisgeving doen van de vervollediging van de omzetting[65];
- de **richtlijn inzake de beveiliging van netwerk- en informatiesystemen**: twee lidstaten moeten nog kennisgeving doen van de vervollediging van de omzetting[66]; en
- de **vierde antiwitwasrichtlijn**: 24 lidstaten moeten nog vervollediging van de omzetting melden[67].

2. Desinformatie bestrijden en verkiezingen beschermen tegen andere cyberdreigingen

De bescherming van democratische processen en instellingen tegen desinformatie en daarmee verbonden inmenging is overal ter wereld een grote maatschappelijke uitdaging. De EU heeft een **solide kader voor gecoördineerde actie tegen desinformatie** uitgewerkt, met volledige inachtneming van de Europese waarden en grondrechten[68]. Zoals wordt uiteengezet in de gezamenlijke mededeling van 14 juni 2019 over de uitvoering van het actieplan tegen desinformatie[69], heeft het werk dat op verschillende complementaire actiegebieden is geleverd, geholpen om de mogelijkheden tot desinformatie te beperken en de integriteit van de Europese verkiezingen te waarborgen.

61 België, Bulgarije, Tsjechië, Denemarken, Duitsland, Estland, Ierland, Spanje, Frankrijk, Italië, Cyprus, Letland, Litouwen, Hongarije, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk (stand van zaken op 24 juli 2019).

62 Slovenië heeft gedeeltelijke omzetting gemeld. Spanje heeft geen kennisgeving van omzetting gedaan (stand van zaken op 24 juli 2019).

63 Polen heeft gedeeltelijke omzetting gemeld. Griekenland en Luxemburg hebben geen kennisgeving van omzetting gedaan (stand van zaken op 24 juli 2019).

64 België, Tsjechië, Estland, Litouwen, Polen, Portugal, Zweden en het Verenigd Koninkrijk hebben gedeeltelijke omzetting gemeld. Duitsland, Ierland, Griekenland, Spanje, Cyprus, Luxemburg, Hongarije, Nederland, Roemenië, Slovenië, Slowakije en Finland hebben geen kennisgeving van omzetting gedaan (stand van zaken op 24 juli 2019).

65 Letland, Portugal, Slovenië en Finland hebben gedeeltelijke omzetting gemeld. Griekenland en Spanje hebben geen kennisgeving van omzetting gedaan. Duitsland heeft volledige omzetting gemeld, maar de Commissie beschouwt de omzetting niet als volledig (stand van zaken op 24 juli 2019).

66 België en Hongarije hebben de richtlijn gedeeltelijk omgezet (stand van zaken op 24 juli 2019).

67 België, Bulgarije, Tsjechië, Denemarken, Duitsland, Estland, Ierland, Spanje, Frankrijk, Italië, Cyprus, Letland, Litouwen, Hongarije, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk (stand van zaken op 24 juli 2019).

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

69 JOIN(2019) 12 final van 14.6.2019.

In zijn conclusies van 21 juni 2019[70] toont de Raad zich ingenomen met het voornemen van de Commissie om grondig te evalueren in hoeverre de toezeggingen van onlineplatforms en andere ondertekenaars van de **praktijkcode tegen desinformatie**[71] zijn uitgevoerd, en vraagt hij de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid om een continue beoordeling van en passende respons op *"het veranderende karakter van de dreigingen en het toenemende risico van kwaadwillige inmenging en onlinemanipulatie waarmee de ontwikkeling van kunstmatige intelligentie en technieken voor gegevensverzameling gepaard gaat"*.

De Commissie en de hoge vertegenwoordiger zullen de werkzaamheden op dit gebied voortzetten overeenkomstig de conclusies van de Europese Raad. In maart 2019 hebben de Commissie en de hoge vertegenwoordiger een **systeem voor snelle waarschuwing** opgezet om de lidstaten en de EU-instellingen in staat te stellen gemakkelijker inzichten in verband met desinformatiecampagnes uit te wisselen en de reactie daarop te coördineren. De eerste vergadering van de contactpunten van de lidstaten na de verkiezingen voor het Europees Parlement vond op 3 en 4 juni 2019 plaats in Tallinn. Om het systeem voor snelle waarschuwing verder te versterken, zullen de hoge vertegenwoordiger en de Commissie, in nauwe samenwerking met de lidstaten, de werking van het systeem in het najaar van 2019 evalueren. Voorts zullen zij een gemeenschappelijke methodologie ontwikkelen om desinformatiecampagnes te analyseren en aan het licht te brengen, en zullen zij nauwere partnerschappen met internationale partners zoals de G7 en de NAVO aangaan.

Ook in het kader van het **Europees samenwerkingsnetwerk voor de verkiezingen**[72] worden de werkzaamheden voortgezet. Het netwerk heeft op 7 juni 2019 een eerste vergadering gehouden om de balans op te maken van de verkiezingen voor het Europees Parlement. Deze overwegingen zullen, samen met bijdragen van de relevante nationale autoriteiten, politieke partijen en onlineplatforms, meegenomen worden in het uitgebreide verslag van de Commissie over de verkiezingen voor het Europees Parlement, dat in oktober 2019 zal worden aangenomen. Het feit dat de lidstaten het netwerk ook bij andere verkiezingen dan die voor het Europees Parlement hebben gebruikt, bewijst het ruimere nut ervan voor het waarborgen van de integriteit van de democratie in de EU.

De Commissie zal ook de uitvoering van de verbintenissen die de platforms in de **praktijkcode tegen desinformatie** zijn aangegaan, blijven monitoren en bevorderen.
Uit de rapporten van Google, Twitter en Facebook in het kader van de praktijkcode blijkt dat alle platforms voorafgaand aan de verkiezingen voor het Europees Parlement actie hebben ondernomen door politieke advertenties te labelen en openbaar beschikbaar te maken in doorzoekbare advertentieregisters. Niettemin is er ruimte voor verbetering, zoals de Europese Groep van

---

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-nl.pdf De oproep van de Europese Raad bouwt voort op input die het Roemeense voorzitterschap van de Raad, de Commissie en de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid hebben geleverd over de lessen die zijn getrokken in verband met desinformatie en het waarborgen van vrije en eerlijke verkiezingen – zoals de gezamenlijke mededeling over de uitvoering van het actieplan tegen desinformatie.

71 De praktijkcode is in oktober 2018 ondertekend door de onlineplatforms Facebook, Google en Twitter, Mozilla, adverteerders en de reclamesector en bevat zelfregulerende normen ter bestrijding van desinformatie. Om de doelstellingen van de mededeling van de Commissie over de bestrijding van online-desinformatie (COM(2018) 236 final van 26.4.2018) te halen, zijn in de praktijkcode uiteenlopende verbintenissen opgenomen, zoals transparantie van politieke advertenties, het afsluiten van nepaccounts en de demonetisering van verspreiders van desinformatie.

72 In dit netwerk worden de contactpunten van de nationale netwerken voor samenwerking op het gebied van verkiezingen samengebracht. Deze nationale netwerken bestaan op hun beurt uit de instanties die bevoegd zijn voor electorale aangelegenheden en de instanties die belast zijn met het toezicht op en de handhaving van regels inzake onlineactiviteiten die relevant zijn in een electorale context. Het Europees samenwerkingsnetwerk voor de verkiezingen dient voor het geven van waarschuwingen over dreigingen, het uitwisselen van beste praktijken tussen nationale netwerken, het bespreken van gemeenschappelijke oplossingen voor de geconstateerde problemen en het aanmoedigen van gezamenlijke projecten en oefeningen.

regelgevende instanties voor audiovisuele mediadiensten heeft vastgesteld[73]. Met name schort het aan toegang tot de gedetailleerde onbewerkte gegevens die nodig zijn voor een alomvattend toezicht. Tot slot moeten de platforms de onderzoeksgemeenschap op een nuttige manier toegang geven tot gegevens, in overeenstemming met de regels inzake de bescherming van persoonsgegevens. Later dit jaar zal de Commissie uitgebreid evalueren hoe de verbintenissen die in het kader van de praktijkcode zijn aangegaan, gedurende het eerste jaar van toepassing van de code zijn uitgevoerd. Op basis daarvan kan de Commissie overwegen verdere maatregelen, onder meer van regelgevende aard, te nemen om de reactie van de EU op desinformatie op de lange termijn te verbeteren.

3. Paraatheid en bescherming

Het versterken van de weerbaarheid en veerkracht tegen veiligheidsdreigingen is een belangrijk aspect van het streven naar een doeltreffende en echte Veiligheidsunie. Met het oog daarop krijgen de lidstaten en de lokale overheden van de lidstaten steun van de Commissie om de **bescherming van openbare ruimten**[74] te verbeteren, en krijgen de lidstaten steun om de paraatheid bij **veiligheidsrisico's op chemisch, biologisch, radiologisch en nucleair gebied**[75] te versterken, door uitvoering te geven aan de twee actieplannen op dit gebied en de behoefte aan responscapaciteit in het kader van rescEU te analyseren[76]. Wat de evoluerende chemische dreigingen[77] betreft, heeft de Commissie, in samenwerking met de lidstaten en in overleg met internationale partners, een lijst opgesteld van chemische stoffen die uit het oogpunt van misbruik voor terroristische doeleinden het meest aanleiding tot zorg geven. De EU-lijst dient als basis voor verdere werkzaamheden om de toegankelijkheid van deze stoffen te beperken en om in samenwerking met de fabrikanten de detectiecapaciteit te verbeteren.

De technologieën voor onbemande luchtvaartuigen maken een breed scala van mogelijke vluchtuitvoeringen mogelijk. De afgelopen jaren is de markt van onbemande luchtvaartuigsystemen voor militaire, civiele, commerciële en recreatieve doeleinden in snel tempo gegroeid. **Drones** bieden kansen, maar vormen ook een toenemende dreiging voor de veiligheid van kritieke infrastructuur (zoals de luchtvaart), openbare ruimten en evenementen, gevoelige locaties en personen. In Europa zijn drones gebruikt om het luchtverkeer en rechtshandhavingsoperaties te verstoren, om kritieke

---

73 Deze groep bestaat uit de hoofden of vertegenwoordigers op hoog niveau van nationale onafhankelijke regelgevende instanties op het gebied van audiovisuele diensten en adviseert de Commissie over de uitvoering van de EU-richtlijn inzake audiovisuele mediadiensten (Richtlijn 2010/13/EU van 10.3.2010). Op 20 en 21 juni 2019 heeft de groep op haar bijeenkomst in Bratislava de balans van de werkzaamheden op het gebied van desinformatie opgemaakt, met bijzondere aandacht voor de verkiezingen van 2019 voor het Europees Parlement en de daarmee verband houdende kwesties van politieke en thematisch georiënteerde advertenties.

74 Zie de "Goede praktijken voor overheidsinstanties en particuliere beheerders ten behoeve van een betere beveiliging van openbare ruimten" in het achttiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2019) 145 final van 20.3.2019). Dit bouwt voort op het actieplan van oktober 2017 ter ondersteuning van de bescherming van openbare ruimten (COM(2017) 612 final van 18.10.2017). Op 5 juni 2019 vond de derde bijeenkomst van het forum van beheerders van het EU-forum voor de bescherming van openbare ruimten plaats, met vertegenwoordigers van de EU-lidstaten en particuliere beheerders van openbare ruimten. Op deze bijeenkomst waren 14 Europese verenigingen vertegenwoordigd, die actief zijn op tal van gebieden: horeca, liveoptredens, muziek en amusement, pretparken en bezienswaardigheden, luchtvaart, spoorvervoer, winkelcentra, telecommunicatie, particuliere beveiligingsdiensten en de productie van beveiligingsapparatuur.

75 Met name door uitvoering te geven aan het actieplan van oktober 2017 ter verbetering van de paraatheid bij veiligheidsrisico's op chemisch, biologisch, radiologisch en nucleair gebied (COM(2017) 610 final van 18.10.2017).

76 Zie artikel 12, lid 2, van Besluit nr. 1313/2013/EU betreffende het Uniemechanisme voor civiele bescherming (17.12.2013), als gewijzigd bij Besluit (EU) 2019/420 (13.3.2019).

77 Zie de versterkte maatregelen tegen chemische dreigingen, zoals uiteengezet in het vijftiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie (COM(2018) 470 final van 13.6.2018).

infrastructuur in de gaten te houden en om smokkelwaar in gevangenissen en over de grens te brengen.

De Commissie steunt de lidstaten bij het aanpakken van de toenemende dreiging die drones vormen voor burgers en kritieke maatschappelijke functies, zonder daarbij echter het nut van drones, onder meer bij noodhulpoperaties, uit het oog te verliezen. Om het risico van kwaadwillig gebruik te beperken, heeft de Commissie onlangs **gemeenschappelijke EU-brede regels voor de veilige exploitatie van drones**[78] vastgesteld, waaronder bepalingen om de registratie van de exploitant verplicht te stellen en identificatie op afstand mogelijk te maken. Bovendien ondersteunt de Commissie de lidstaten door tendensen in de ontwikkeling van de dreiging die samenhangt van drones, te monitoren, relevante onderzoeksprojecten en maatregelen voor capaciteitsopbouw te financieren en de uitwisseling tussen de lidstaten en andere belanghebbenden te vergemakkelijken. Om deze steun op te voeren, zal de Commissie op 17 oktober 2019 een internationale conferentie op hoog niveau organiseren om de risico's die samenhangen met drones, aan te pakken.

Gezien de behoefte aan een brede kijk op het EU-beleid inzake de **bescherming van kritieke infrastructuur**[79], is de Commissie op 23 juli 2019 gekomen met een evaluatie van de richtlijn betreffende de Europese kritieke infrastructuur[80] (het rechtskader voor de identificatie van Europese kritieke infrastructuren en de aanmerking van infrastructuren als Europese kritieke infrastructuren) en met een beoordeling van de noodzaak de bescherming van deze infrastructuur te verbeteren. Volgens de evaluatie is de context waarin kritieke infrastructuren in Europa werken, sinds de inwerkingtreding van de richtlijn sterk veranderd – onder meer als gevolg van de ontwikkeling van de wetgeving in sectoren die een grote rol spelen in de richtlijn, zoals energie[81] – en zijn de bepalingen van de richtlijn in dat veranderde landschap slechts ten dele relevant. Dit neemt niet weg dat er bij de lidstaten nog steeds een draagvlak bestaat voor een EU-beleid op het gebied van de bescherming van kritieke infrastructuur dat het subsidiariteitsbeginsel in acht neemt en een toegevoegde waarde biedt.

4. Externe dimensie

Aangezien de meeste veiligheidsdreigingen waarmee de Unie wordt geconfronteerd, grensoverschrijdend en mondiaal zijn, vormt samenwerking met internationale organisaties en partnerlanden van buiten de EU een integrerend deel van de werkzaamheden voor de totstandbrenging van een doeltreffende en echte Veiligheidsunie.

Met het oog daarop moet gebruik worden gemaakt van de baten van multilaterale samenwerking, onder meer de samenwerking tussen de EU en de VN, die onlangs is versterkt met de ondertekening van het **kader van de Verenigde Naties en de Europese Unie voor terrorismebestrijding**. De ondertekening vond op 24 april 2019 in New York plaats, ter gelegenheid van de tweede politieke dialoog op hoog niveau die de VN en de EU over terrorismebestrijding hebben gehouden[82]. Het kader bevordert de samenwerking op het gebied van capaciteitsopbouw voor de bestrijding van terrorisme en de preventie en bestrijding van gewelddadig extremisme in Afrika, het Midden-Oosten en Azië. In het kader zijn de gebieden voor samenwerking tussen de VN en de EU en de prioriteiten tot 2020

78 Uitvoeringsverordening (EU) 2019/947 van de Commissie van 24 mei 2019 inzake de regels en procedures voor de exploitatie van onbemande luchtvaartuigen (PB L 152 van 11.6.2019).

79 In de uitgebreide beoordeling van het veiligheidsbeleid van de EU die in 2017 is verricht (SWD(2017) 278 final van 26.7.2017) wordt gewezen op de behoefte aan een brede kijk op het EU-beleid inzake de bescherming van kritieke infrastructuur.

80 Richtlijn 2008/114/EG van de Raad van 8 december 2008 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. Deze richtlijn heeft ten doel de bescherming van kritieke infrastructuren in de Europese Unie te verbeteren.

81 Met name Verordening (EU) 2017/1938 (25.10.2017) betreffende maatregelen tot veiligstelling van de gasleveringszekerheid en Verordening (EU) 2019/941 (5.6.2019) betreffende risicoparaatheid in de elektriciteitssector.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

vastgelegd.

De **samenwerking op veiligheidsgebied met de Westelijke Balkan** is een bijzondere regionale prioriteit en moet uitvoering geven aan een aantal prioritaire acties op het gebied van veiligheid die zijn vastgesteld in de strategie van 2018 voor deze regio[83]. Met het oog daarop heeft de Commissie op 4 april 2019 de eerste bijeenkomst georganiseerd van de agentschapsoverkoepelende taskforce voor de Westelijke Balkan. Vertegenwoordigers van zeven EU-agentschappen wisselden er ervaringen uit en versterkten de operationele samenwerking met partners in de regio, onder meer in het kader van de bestrijding van georganiseerde misdaad, terrorisme, vuurwapens, drugs, migrantensmokkel en mensenhandel. In samenwerking met de zes landen van de Westelijke Balkan zijn analyses van hybride risico's opgezet. Een ander tastbaar voorbeeld van de samenwerking met de regio is de statusovereenkomst tussen de EU en Albanië inzake de Europese Grens- en kustwacht. Kort na de inwerkingtreding van de overeenkomst op 1 mei 2019 zijn teams van het Europees Grens- en kustwachtagentschap ingezet aan de grens met Griekenland. Dit is de eerste keer dat een dergelijke overeenkomst met een derde land is gesloten en dat een dergelijk team in een derde land is ingezet. Binnen afzienbare tijd zouden met andere landen in de regio soortgelijke overeenkomsten moeten worden ondertekend.

Bovendien werd in juli 2019 in Albanië een verbindingsofficier van Europol ingezet om de Albanese autoriteiten verder te helpen bij hun inspanningen om georganiseerde criminaliteit te voorkomen en te bestrijden. Om de strijd tegen de illegale handel in vuurwapens op te voeren, heeft de Commissie op 27 juni 2019 een evaluatie gepresenteerd van het actieplan voor de **bestrijding van de illegale handel in vuurwapens** tussen de EU en het zuidoostelijke deel van Europa (voor de periode 2015-2019)[84]. Uit de evaluatie blijkt dat samenwerking een toegevoegde waarde heeft, maar ook dat er nog meer inspanningen moeten worden geleverd, bijvoorbeeld door de invoering van efficiënte nationale coördinatiecentra voor vuurwapens op te zetten of door het verzamelen van informatie en het rapporteren over de inbeslagname van vuurwapens te harmoniseren.

De EU geeft evenveel prioriteit aan het ontwikkelen van de **samenwerking met landen uit het Midden-Oosten en Noord-Afrika** op het gebied van veiligheid. De EU is een veiligheidsdialoog met Tunesië en Algerije aangegaan. Op 12 juni vond in Tunis de derde dialoog over veiligheid en terrorismebestrijding tussen de EU en Tunesië plaats. De EU en Algerije hielden hun tweede dialoog op 12 november 2018 in Algiers. Sinds de EU en Marokko op de bijeenkomst van de associatieraad van 27 juni laatstleden het belang van nauwere samenwerking op het gebied van veiligheid hebben erkend, zijn er besprekingen gaande over het opstarten van een gestructureerde veiligheidsdialoog om de gemeenschappelijke problemen aan te pakken. Daarnaast worden er besprekingen gevoerd met Egypte over de ontwikkeling van een gestructureerde veiligheidsdialoog, zoals op 10 juli in Caïro werd bevestigd op de meest recente bijeenkomst van hoge ambtenaren.

Op basis van het mandaat van de Raad is de Commissie begonnen met informele besprekingen met de meeste landen in het **Midden-Oosten en Noord-Afrika** om formele onderhandelingen op te starten over een internationale overeenkomst voor de uitwisseling van persoonsgegevens tussen het Agentschap van de Europese Unie voor samenwerking op het gebied van rechtshandhaving (**Europol**) en de autoriteiten die in deze landen bevoegd zijn voor de bestrijding van zware criminaliteit en terrorisme. De Commissie stimuleert in dit verband ook het rechtstreeks sluiten van werkafspraken tussen Europol en partnerinstanties in de landen uit het **Midden-Oosten en Noord-Afrika**, om een formeel kader te creëren voor regelmatige samenwerking op strategisch niveau.

De EU en de **Verenigde Staten** werken in het kader van een hecht en strategisch partnerschap samen om gemeenschappelijke dreigingen aan te pakken en de veiligheid te verbeteren. Tijdens hun

---

83 COM(2018) 65 final van 6.2.2018.

84 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_en.pdf

bijeenkomst van de ministers van Justitie en Binnenlandse Zaken op 19 juni 2019 bevestigden de EU en de Verenigde Staten opnieuw dat de strijd tegen terrorisme tot hun topprioriteiten behoort. Wat de overeenkomst inzake persoonsgegevens van passagiers tussen de EU en de VS[85] betreft, wezen beide partijen nogmaals op het belang van de overeenkomst en zegden zij toe in september 2019 te beginnen met een gezamenlijke evaluatie van de uitvoering ervan, overeenkomstig de bepalingen van de overeenkomst. Voorts verbonden beide partijen zich ertoe hun gezamenlijke inspanningen in de strijd tegen terrorisme op te voeren, onder andere door meer informatie uit conflictgebieden te delen zodat deze kan worden gebruikt bij onderzoeken en gerechtelijke vervolgingen.

Om deze samenwerking te intensiveren, heeft de Commissie op 10 juli 2019 in Brussel een workshop op hoog niveau over slagveldinformatie georganiseerd in samenwerking met de EU-coördinator voor terrorismebestrijding. Hoge ambtenaren van de ministeries van Defensie, Binnenlandse Zaken en Justitie van de lidstaten en de Verenigde Staten, Europol, Eurojust en vertegenwoordigers van internationale organisaties kwamen er bijeen om van gedachten te wisselen over het gebruik van slagveldinformatie en over de procedurele, juridische en operationele problemen waarmee zij momenteel te maken hebben bij het opsporen en berechten van terroristen. Eerder in het jaar, op 14 en 15 mei, waren de EU en de Verenigde Staten al samen in Brussel voor een dialoog over capaciteitsopbouw op chemisch, biologisch, radiologisch en nucleair gebied, met het oog op het coördineren van hun inspanningen om de door massavernietigingswapens veroorzaakte dreigingen te verminderen en de veiligheid op chemisch, biologisch, radiologisch en nucleair gebied te verhogen.

De **overeenkomst tussen de EU en de Verenigde Staten inzake het programma voor het traceren van terrorismefinanciering**[86] is sinds 2010 van kracht en regelt de doorgifte en verwerking van gegevens met het oog op het identificeren, opsporen en vervolgen van terroristen en hun netwerken. De overeenkomst voorziet in garanties die moeten zorgen voor de bescherming van de gegevens van de EU-burgers, en in een regelmatige evaluatie van de waarborgen, beschermingsmaatregelen en wederkerigheidsbepalingen. In het verslag van 22 juli 2019 over de regelmatige evaluatie[87] gaf de Commissie te kennen ervan overtuigd te zijn dat de overeenkomst en de bijbehorende waarborgen en beschermingsmaatregelen naar behoren worden uitgevoerd. De Commissie toonde zich in het verslag ook verheugd over de aanhoudende transparantie van de Amerikaanse autoriteiten bij het delen van informatie, waaruit de waarde blijkt die het programma voor het traceren van terrorismefinanciering heeft voor de internationale bestrijding van terrorisme. De informatie die in het kader van de overeenkomst werd verstrekt, was essentieel voor de voortgang van specifieke onderzoeken naar terroristische aanslagen op Europese bodem, waaronder die van 2017 in Stockholm, Barcelona en Turku. De lidstaten en Europol maken frequenter gebruik van het mechanisme en de gegevens die het programma voor het traceren van terrorismefinanciering heeft opgeleverd, hebben zeven keer meer aanwijzingen voor het onderzoek opgeleverd dan in de vorige verslagperiode. De volgende gezamenlijke evaluatie van de overeenkomst is gepland voor 2021.

Wat de internationale samenwerking op het gebied van de **uitwisseling van persoonsgegevens van passagiers met het oog op de bestrijding van terrorisme en zware criminaliteit** betreft, toonden de EU en Canada zich bij hun zeventiende topontmoeting, op 17 en 18 juli 2019 in Montreal, verheugd over het afronden van de onderhandelingen over een nieuwe overeenkomst inzake persoonsgegevens van passagiers. De partijen erkenden dat deze overeenkomst een essentiële rol speelt in het versterken van de veiligheid, met inachtneming van de privacy en de bescherming van persoonsgegevens, en verbinden zich ertoe om de overeenkomst zo spoedig mogelijk af te ronden, onder voorbehoud van de verplichte juridische toetsing door Canada. Wat de bestaande overeenkomst tussen de EU en Australië over persoonsgegevens van passagiers[88] betreft, zal een EU-team in augustus 2019 een bezoek aan Canberra afleggen in het kader van de gezamenlijke evaluatie van de overeenkomst.

---

85 PB L 215 van 11.8.2012, blz. 5.
86 PB L 195 van 27.7. 2010, blz. 5.
87 COM(2019) 342 final van 22.7.2019.
88 PB L 186 van 14.7.2012, blz. 4.

De Commissie werkt in de Raad ook samen met de lidstaten aan een EU-standpunt voor de veertigste vergadering van de **Internationale Burgerluchtvaartorganisatie (ICAO)**, die zal plaatsvinden van 24 september tot en met 4 oktober 2019. Op die bijeenkomst zal de politieke koers worden uitgezet en zullen instructies aan de ICAO-raad worden gegeven inzake de technische werkzaamheden op het gebied van de ICAO-normen voor de verwerking van persoonsgegevens van passagiers. De Raad heeft zijn goedkeuring gehecht aan een door de Commissie opgesteld informatiedocument waarin het standpunt van de Unie wordt geschetst ten aanzien van de kernbeginselen die ten grondslag moeten liggen aan toekomstige mondiale normen op het gebied van persoonsgegevens van passagiers. Het informatiedocument zal aan de instantie worden voorgelegd ten behoeve van de aangesloten landen die niet tot de EU behoren.

VI. CONCLUSIE

Dankzij de nauwe samenwerking tussen het Europees Parlement, de Raad, de lidstaten en de Commissie heeft de EU de afgelopen jaren aanzienlijke vooruitgang geboekt bij de gezamenlijke werkzaamheden voor de totstandbrenging van een doeltreffende en echte Veiligheidsunie, en heeft zij overeenstemming bereikt over een aantal prioritaire wetgevingsinitiatieven. De lidstaten voeren, met de steun van de Commissie, ook diverse niet-wetgevende operationele maatregelen uit om de veiligheid voor alle burgers te versterken. Een aantal andere prioritaire initiatieven op het gebied van de Veiligheidsunie, met name voor het aanpakken van onmiddellijke dreigingen, wachten echter nog op verdere actie van de medewetgevers. De Commissie roept het Europees Parlement en de Raad op de nodige stappen te ondernemen om snel tot een akkoord te komen over de wetgevingsvoorstellen om terroristische propaganda en radicalisering via het internet te bestrijden, de cyberbeveiliging te verbeteren, de toegang tot elektronisch bewijsmateriaal te vergemakkelijken en het werk aan krachtigere en slimmere informatiesystemen voor veiligheid, grens- en migratiebeheer te voltooien.

De Commissie roept de lidstaten op alle wetgeving die in het kader van de Veiligheidsunie is vastgesteld, snel en volledig uit te voeren, zodat deze optimaal voordeel kan opleveren. Voorts roept de Commissie de lidstaten op om de cruciale werkzaamheden met betrekking tot praktische maatregelen ter verbetering van de beveiliging van digitale infrastructuur voort te zetten en te intensiveren, om desinformatie en andere cyberdreigingen tegen te gaan, om de paraatheid en de bescherming te verbeteren, en om de samenwerking met partners buiten de Unie in de strijd tegen gezamenlijke bedreigingen te versterken. Dit samenstel van maatregelen zal de veiligheid van alle burgers versterken.