EUROPESE
COMMISSIE

Brussel, 20.3.2019
COM(2019) 145 final

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

Achttiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie

{SWD(2019) 140 final}

I. INLEIDING

Dit is het achttiende voortgangsverslag over de totstandbrenging van een echte en doeltreffende Veiligheidsunie. De ontwikkelingen op het gebied van twee belangrijke pijlers komen aan bod: de bestrijding van terrorisme, georganiseerde criminaliteit en de middelen ter ondersteuning daarvan, en de verbetering van onze weerbaarheid en veerkracht tegenover die dreigingen.

In de aanloop naar de verkiezingen voor het Europees Parlement van mei 2019 wordt in dit verslag gewezen op de belangrijke werkzaamheden die op verschillende niveaus zijn verricht om cyberdreigingen en desinformatie bij de verkiezingen aan te pakken en te voorkomen. Naar aanleiding van de oproep van de Europese Raad tot maatregelen om de democratische stelsels van de Unie te beschermen en desinformatie in de aanloop naar de komende verkiezingen te bestrijden, heeft de Unie aanzienlijke vooruitgang geboekt in de richting van meer gecoördineerde maatregelen op het gebied van electorale weerbaarheid. De Unie zal haast moeten maken, wil ze goed voorbereid zijn wanneer de Europese kiezer in mei 2019 naar de stembus gaat. Daarom roept de Commissie alle betrokken actoren – overheidsinstanties, politieke partijen en met name onlineplatforms – op zich dubbel zo hard in te zetten vóór electorale weerbaarheid en tegen desinformatie. De voortgang op dit gebied zal besproken worden tijdens de komende Europese Raad op 21 en 22 maart 2019. In de aanloop naar die bijeenkomst roept de Commissie de lidstaten op om hun coördinatie bij de bestrijding van desinformatie en de bescherming van de verkiezingen voor het Europees Parlement op te voeren.

De EU heeft aanzienlijke vooruitgang geboekt bij de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Zo is er overeenstemming bereikt over een aantal prioritaire wetgevingsinitiatieven die de veiligheid voor alle burgers zullen verbeteren. De afgelopen maanden[1] hebben het Europees Parlement en de Raad overeenstemming bereikt over de interoperabiliteit van de EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer, en over nieuwe EU-regels om de armslag van terroristen en criminelen te beperken door de toegang tot precursoren voor explosieven, de financiering van hun activiteiten en de mogelijkheden om onopgemerkt te reizen, te bemoeilijken. Door een akkoord te bereiken over 15 van de 22 wetgevingsinitiatieven die de Commissie in het kader van de Veiligheidsunie heeft voorgesteld (zie de lijst van alle initiatieven inzake de Veiligheidsunie in *bijlage I*), komt de EU haar beloften na op een gebied dat zowel voor het Europees Parlement en de Raad als voor de Commissie van prioritair belang is[2].

Dit neemt niet weg dat er nog meer inspanningen vereist zijn. Met name moeten de medewetgevers, binnen het huidige wetgevingsmandaat, het urgente gevaar van terroristische online-inhoud aanpakken en daartoe overeenstemming bereiken over het voorstel van de Commissie. Voorts dienen het Europees Parlement en de Raad het eens te worden over het voorstel van de Commissie voor een versterkte Europese grens- en kustwacht teneinde de veiligheid te verbeteren door middel van een verscherpte bescherming van de buitengrenzen

---

[1] Hierbij wordt voortgebouwd op wat eerder is verwezenlijkt in het kader van de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Voor een volledig overzicht, zie de vorige voortgangsverslagen over de totstandbrenging van de Veiligheidsunie: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

[2] Zie de gezamenlijke verklaring over de wetgevingsprioriteiten van de EU voor 2018-19: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

van de Unie.

De tragische gebeurtenissen van 15 maart 2019 in Christchurch (Nieuw-Zeeland) tonen aan dat de terroristische dreiging nog steeds een duidelijk en reëel gevaar vormt, gevoed door extreemrechtse of andere extremistische ideologieën. Dat het problematisch blijkt om live gestreamde inhoud van internetplatforms te verwijderen en te voorkomen dat deze weer opduikt, onderstreept het fundamentele belang van het voorstel van de Commissie inzake terroristische online-inhoud. Het is cruciaal dat de medewetgevers onverwijld overeenstemming bereiken over de voorgestelde regels inzake het verwijderen van terroristische online-inhoud. Even belangrijk in de strijd tegen terrorisme in al zijn vormen is dat alle lidstaten uitvoering geven aan al de wetgeving die de EU met name naar aanleiding van de terroristische aanslagen in Europa heeft vastgesteld om de armslag voor terroristen te beperken, meer bepaald de richtlijn terrorismebestrijding en de richtlijn inzake de controle op de verwerving en het voorhanden hebben van vuurwapens. In het kader van de strijd tegen extremisme heeft de Commissie zich ook gebogen over het probleem van illegale haatzaaiende uitingen op internet, islamofobie en antisemitisme en heeft zij maatregelen in dit verband genomen.

In dit verslag wordt ook uiteengezet welke vorderingen er zijn gemaakt met andere prioritaire dossiers op het gebied van veiligheid, met name wat betreft maatregelen ter ondersteuning van de bescherming van openbare ruimten. Om de voordelen van een doeltreffende en echte Veiligheidsunie ten volle te kunnen benutten, moet er in de allereerste plaats voor worden gezorgd dat de overeengekomen maatregelen volledig en correct worden uitgevoerd. De Commissie ondersteunt de lidstaten hier actief bij, bijvoorbeeld met financiering en door de uitwisseling van goede praktijken te faciliteren. Zo nodig maakt de Commissie gebruik van alle bevoegdheden die haar krachtens de Verdragen voor de handhaving van het EU-recht ter beschikking staan, inclusief inbreukprocedures in voorkomend geval.

Dit verslag moet worden bezien tegen de achtergrond van de vijftiende Europese Herdenkingsdag voor de Slachtoffers van Terrorisme op 11 maart 2019, vijftien jaar na de bomaanslagen van 11 maart 2004 in Madrid en drie jaar na de dodelijke aanslagen in Brussel en Zaventem van 22 maart 2016. Het verlenen van steun aan de slachtoffers van terroristische aanslagen is een belangrijk onderdeel van de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Om deze steun nog verder op te voeren, heeft de Commissie op 31 januari 2019 een besluit goedgekeurd over de financiering van het proefproject "Oprichting van een EU-kenniscentrum voor slachtoffers van terrorisme"[3]. Het EU-kenniscentrum zal fungeren als expertisecentrum en platform voor mensen die beroepsmatig te maken hebben met slachtoffers van terrorisme.

De Commissie is verheugd over het verslag van het Europees Parlement over conclusies en aanbevelingen van de Bijzondere Commissie terrorisme[4] en beschouwt dit als een waardevolle bijdrage aan de gezamenlijke werkzaamheden voor de totstandbrenging van een echte en doeltreffende Veiligheidsunie.

[3] C(2019) 636 van 31.1.2019.

[4] Resolutie van het Europees Parlement van 12 december 2018 over conclusies en aanbevelingen van de Bijzondere Commissie terrorisme (2018/2044(INI).

II. UITVOERING VAN WETGEVINGSPRIORITEITEN

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

Informatie-uitwisseling is een centraal onderdeel van de ondersteuning die de EU de nationale autoriteiten biedt in de strijd tegen terrorisme en zware criminaliteit. De interoperabiliteit van de EU-brede informatiesystemen staat borg voor de nauwkeurigheid en volledigheid van de betrokken gegevens en betekent een omslag in de manier waarop gegevens aan de nationale autoriteiten worden verstrekt. De medewetgevers hebben een politiek akkoord bereikt over de prioritaire wetgevingsvoorstellen inzake de **interoperabiliteit van de EU-informatiesystemen** voor veiligheid, grensbeheer en migratiebeheer[5]. De voorgestelde maatregelen zullen zorgen voor een meer intelligente en gerichte communicatie tussen de EU-informatiesystemen, met volledige inachtneming van de grondrechten. Dankzij een optimaal gebruik van bestaande gegevens zal de interoperabiliteit informatielacunes opvullen en blinde vlekken wegnemen door meervoudige identiteiten te helpen opsporen en identiteitsfraude tegen te gaan. Zodra de medewetgevers de nieuwe regels formeel vaststellen, zal de Commissie klaar staan om de lidstaten bij de uitvoering ervan te ondersteunen. Om de ambitieuze doelstelling – volledige interoperabiliteit van de EU-informatiesystemen voor veiligheid, grensbeheer en migratiebeheer tegen 2020 – te halen, is nauwe samenwerking vereist met de EU-agentschappen, alle lidstaten en de met Schengen geassocieerde landen. Ter voorbereiding daarop is op 5 maart 2019 een eerste workshop met deskundigen van de lidstaten gehouden om een doeltreffende coördinatie op gang te brengen.

Volgens de huidige stand van zaken zal de toekomstige architectuur van interoperabele EU-informatiesystemen bestaan uit het versterkte **Schengeninformatiesysteem**[6], het bestaande **Visuminformatiesysteem**[7], de onlangs overeengekomen uitbreiding van het **Europees Strafregisterinformatiesysteem**[8] tot onderdanen van derde landen, het onlangs ingestelde **inreis-uitreissysteem van de EU**[9] en het eveneens nieuwe **Europees systeem voor reisinformatie en -autorisatie (ETIAS)**[10].

In het kader van de technische implementatie van het Europees systeem voor reisinformatie en -autorisatie heeft de Commissie op 7 januari 2019 een voorstel met technische wijzigingen van de betrokken verordening ingediend[11]. De voorgestelde wijzigingen hebben betrekking op de rechtshandelingen voor de EU-informatiesystemen die zoekopdrachten van het Europees systeem voor reisinformatie en -autorisatie zullen ontvangen wanneer niet-visumplichtige onderdanen van derde landen voorafgaand aan hun reis naar het Schengengebied moeten

---

5 COM(2017) 793 final van 12.12.2017, COM(2017) 794 final van 12.12.2017, COM(2018) 478 final van 13.6.2018 en COM(2018) 480 final van 13.6.2018. Het politieke akkoord van 5 februari 2019 is op 13 februari 2019 bekrachtigd door het Comité van permanente vertegenwoordigers van de Raad en op 19 februari 2019 door de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement.

6 Verordening (EU) 2018/1860 van 28.11.2018, Verordening (EU) 2018/1861 van 28.11.2018, Verordening (EU) 2018/1862 van 28.11.2018.

7 Verordening (EG) nr. 767/2008 van 9.7.2008.

8 De medewetgevers hebben op 11 december 2018 een politiek akkoord bereikt over dit prioritaire voorstel (COM(2017) 344 final van 29.6.2017). Het Comité van permanente vertegenwoordigers van de Raad heeft het akkoord op 19 december 2018 bekrachtigd. Het Europees Parlement heeft het akkoord in plenaire zitting bekrachtigd op 11 maart 2019.

9 Verordening (EU) 2017/2226 van 30.11.2017.

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

11 COM(2019) 4 final van 7.1.2019.

worden beoordeeld op risico's uit het oogpunt van veiligheid of irreguliere migratie. De voorgestelde wijzigingen zijn noodzakelijk voor de volledige invoering van het Europees systeem voor reisinformatie en -autorisatie. 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**[12] 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 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**[13] 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[14] en de mededeling van de Commissie van 6 maart 2019 met het voortgangsverslag over de uitvoering van de Europese migratieagenda[15] roept de Commissie de medewetgevers op het voorstel onverwijld vast te stellen. Dankzij dit wetgevingsvoorstel kan Eurodac deel gaan uitmaken van de toekomstige architectuur van interoperabele EU-informatiesystemen en worden in dit systeem ook de cruciale gegevens geïntegreerd 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:

- voor de verkiezingen voor het Europees Parlement hun goedkeuring te hechten aan het wetgevingsvoorstel betreffende **Eurodac**, waarover al bijna overeenstemming is bereikt *(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**.

2. Meer veiligheid door beter beheer van de buitengrenzen

Krachtige bescherming van de buitengrenzen is een vereiste voor een veilige ruimte van vrij verkeer zonder controles aan de binnengrenzen. Deze taak valt onder de verantwoordelijkheid van de lidstaten, die zowel in hun eigen als in het algemeen belang het beheer van hun buitengrenzen moeten waarborgen, met de hulp van de **Europese grens- en kustwacht**. Naar aanleiding van de conclusies van de Europese Raad van juni 2018[16] heeft de Commissie in september 2018 voorgesteld de capaciteiten van de Europese grens- en kustwacht te

12 COM(2018) 302 final van 16.5.2018.
13 COM(2016) 272 final van 4.5.2016.
14 https://www.consilium.europa.eu/media/37545/13-14-euco-final-conclusions-nl.pdf
15 COM(2019) 126 final van 6.3.2019.
16 https://www.consilium.europa.eu/media/35951/28-euco-final-conclusions-nl.pdf

versterken[17]. Dit houdt in dat het agentschap een nieuwe operationele fase zou ingaan en de beschikking zou krijgen over een permanent korps van 10 000 grenswachters, met uitvoerende bevoegdheden en hun eigen uitrusting, zonder dat afbreuk wordt gedaan aan de grondrechten en aan de soevereiniteit van de lidstaten.

De wetgevingswerkzaamheden met betrekking tot het voorstel vorderen goed en de onderhandelingen tussen de medewetgevers zijn inmiddels de cruciale fase ingegaan. Het Europees Parlement heeft op 11 februari 2019 zijn onderhandelingsmandaat vastgesteld en de Raad heeft zijn mandaat op 20 februari 2019 ontvangen. Op 27 februari 2019 en 12 maart 2019 hebben twee trialoogvergaderingen plaatsgevonden. De Commissie verwelkomt en steunt de vooruitgang die met dit prioritaire dossier is geboekt. Daaruit blijkt dat alle instellingen nog vóór de verkiezingen voor het Europees Parlement in 2019 werk willen maken van de goedkeuring van dit voorstel.

Om de veiligheid te versterken door beter beheer van de buitengrenzen, roept de Commissie het Europees Parlement en de Raad op om:

- het wetgevingsvoorstel ter versterking van de **Europese grens- en kustwacht** nog tijdens de huidige zittingsperiode van het Europees Parlement vast te stellen *(initiatief genoemd in de Staat van de Unie 2018).*

3. Radicalisering voorkomen

Het aanpakken van terroristische online-inhoud blijft een essentiële uitdaging in de strijd tegen terrorisme en radicalisering. Inhoud van deze strekking heeft een rol gespeeld bij de meeste aanslagen die de afgelopen twee jaar op Europese bodem zijn gepleegd – hetzij door aan te zetten tot het plegen van een aanslag, instructies voor de uitvoering te verspreiden of de dodelijke afloop te verheerlijken. Om het duidelijke en reële gevaar dat met dergelijke inhoud samenhangt, aan te pakken, ging de toespraak van voorzitter Juncker over de staat van de Unie van 2018 vergezeld van een voorstel[18] voor een verordening betreffende **terroristische online-inhoud**. Hierin werd een juridisch kader voorgesteld om misbruik van aanbieders van hostingdiensten voor de verspreiding van terroristische online-inhoud te voorkomen. De toekomstige regels moeten, met volledige inachtneming van de vrijheid van meningsuiting en andere grondrechten, voorzien in doeltreffende maatregelen om terroristische online-inhoud te verwijderen. Dat moet zo snel mogelijk gebeuren, aangezien de potentiële schade toeneemt naarmate die inhoud langer online blijft.

De Raad heeft zijn onderhandelingsmandaat in december 2018 vastgesteld. Het Parlement werkt nog aan zijn onderhandelingsmandaat en zal dit hopelijk in maart 2019 kunnen goedkeuren[19]. Gezien het cruciale belang van een EU-regelgevingskader met duidelijke voorschriften en waarborgen voor het verwijderen van terroristische online-inhoud, roept de Commissie beide medewetgevers op om nog tijdens de huidige zittingsperiode van het Europees Parlement een akkoord over de voorgestelde wetgeving te bereiken.

---

17 COM(2018) 631 final van 12.9.2018.

18 COM(2018) 640 final van 12.9.2018.

19 De Commissie interne markt en consumentenbescherming van het Europees Parlement heeft op 4 maart 2019 gestemd over haar advies. De Commissie cultuur en onderwijs van het Europees Parlement heeft op 11 maart 2019 over haar rapport gestemd. Verwacht wordt dat de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement op 21 maart 2019 over haar rapport zal stemmen.

Tegelijkertijd blijft de Commissie de lidstaten ondersteunen bij hun inspanningen om **radicalisering te voorkomen**. Een speciaal EU-mechanisme voor samenwerking brengt de nationale vertegenwoordigers samen en draagt ertoe bij dat de op EU-niveau verleende steun tegemoet komt aan de behoeften van de lidstaten[20]. Recente voorbeelden hiervan zijn een conferentie over "EU-steden tegen radicalisering", die op 26 februari 2019 samen met het Comité van de Regio's is georganiseerd. Op 13 maart 2019 heeft de Commissie een vergadering met nationale beleidsmakers op deskundigenniveau belegd om na te gaan welke praktische maatregelen kunnen worden genomen om de gevangenis- en reclasseringsdiensten verder te ondersteunen. De resultaten van deze werkzaamheden zullen worden verwerkt in een handleiding die momenteel door het netwerk voor voorlichting over radicalisering wordt opgesteld en die betrekking heeft op de rehabilitatie en re-integratie van plegers van terroristische misdrijven, terugkerende buitenlandse terroristische strijders en in de gevangenis geradicaliseerde personen (zie ook punt IV.4).

Om radicalisering te voorkomen, roept de Commissie het Europees Parlement op om:

- prioriteit te geven aan het vaststellen van zijn onderhandelingsmandaat voor het wetgevingsvoorstel inzake het voorkomen van de verspreiding van **terroristische online-inhoud**, zodat de medewetgevers nog tijdens de huidige zittingsperiode van het Europees Parlement overeenstemming over de wetgeving kunnen bereiken *(initiatief genoemd in de Staat van de Unie 2018).*

4. Cyberbeveiliging verbeteren

Het aantal gevallen waarin systemen en gegevens te maken krijgen met klassieke cyberdreigingen, stijgt nog steeds. In 2018 bleken kwaadwillige actoren weer actiever te zijn geworden en een breed spectrum van doelwitten en slachtoffers te bestrijken. Cybercriminaliteit tegengaan en zorgen voor een betere cyberbeveiliging blijven daarom prioritaire actieterreinen voor de EU. De EU heeft tastbare vooruitgang geboekt bij het verbeteren van haar cyberbeveiliging, door de maatregelen uit te voeren die zijn opgenomen in de gezamenlijke mededeling[21] van september 2017 "Weerbaarheid, afschrikking en defensie: bouwen aan een sterke cyberbeveiliging voor de EU".

Op 12 maart 2019 heeft het Europees Parlement in plenaire zitting het door de medewetgevers bereikte politieke akkoord over de **cyberbeveiligingsverordening** bevestigd. Deze verordening, die naar verwachting in mei 2019 in werking zal treden, zal leiden tot een toename van de capaciteiten en de paraatheid van de lidstaten en het bedrijfsleven op het gebied van cyberbeveiliging. Met de verordening wordt een EU-kader voor cyberbeveiligingscertificering vastgesteld voor producten, systemen en diensten op het gebied van informatie- en communicatietechnologie. Ook de samenwerking en coördinatie tussen de lidstaten en de EU-instellingen, -agentschappen en -organen, met name het EU-agentschap voor cyberbeveiliging (het vroeger Enisa), zullen er dankzij de verordening op vooruitgaan.

Anderzijds is verdere vooruitgang nodig met betrekking tot het voorstel van de Commissie van september 2018 inzake een **Europees kenniscentrum voor industrie, technologie en**

[20] De behoeften van de lidstaten op het gebied van de preventie van radicalisering zijn voor het eerst in kaart gebracht in de strategische richtsnoeren voor EU-preventiemaatregelen voor 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

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

onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra[22]. Het voorstel heeft tot doel de technologische en industriële capaciteiten voor cyberbeveiliging te ondersteunen en het concurrentievermogen van de cyberbeveiligingsindustrie van de Unie te vergroten. Het Europees Parlement en de Raad hebben op 13 maart 2019 hun onderhandelingsmandaat goedgekeurd. De eerste trialoog vond meteen al dezelfde dag plaats. De Commissie roept de medewetgevers op snel tot overeenstemming te komen over de voorgestelde wetgeving.

De EU heeft aanzienlijke vooruitgang geboekt met het verder operationeel maken van de **gemeenschappelijke diplomatieke EU-respons op kwaadwillige cyberactiviteiten** (het "instrumentarium voor cyberdiplomatie"), als reactie op de oproep van de Europese Raad[23] tot voortzetting van de werkzaamheden in verband met de capaciteit om te reageren op cyberaanvallen en deze door middel van beperkende EU-maatregelen tegen te gaan. De hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid en de Commissie hebben op 8 maart 2019 een gezamenlijk voorstel ingediend voor een verordening van de Raad betreffende beperkende maatregelen voor het afweren van cyberaanvallen die de Unie of haar lidstaten bedreigen. De Commissie en de hoge vertegenwoordiger pleiten voor een snelle goedkeuring van dit voorstel teneinde de weerbaarheid van de Unie tegen cyberaanvallen te versterken.

Om de cyberbeveiliging te verbeteren, roepen de Commissie en de hoge vertegenwoordiger de Raad op om:
• de verordening van de Raad betreffende **beperkende maatregelen voor het afweren van cyberaanvallen** die de Unie of haar lidstaten bedreigen, goed te keuren.

5. De armslag van terroristen beperken

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

Het Europees Parlement en de Raad hebben op 14 februari 2019 een politiek akkoord bereikt over het voorstel voor een verordening over **beperkingen inzake het op de markt brengen en het gebruik van precursoren voor explosieven**[24]. Eenmaal van toepassing zal deze verordening het huidige wetgevingskader aanzienlijk verbeteren door de toegang tot gevaarlijke precursoren voor explosieven die kunnen worden misbruikt voor de bouw van zelfgemaakte bommen, te beperken. Voorts zullen veiligheidslacunes door de verordening worden gedicht, dankzij maatregelen zoals een verbod op nog een aantal chemische stoffen, verplichte controles van het strafregister van personen die een vergunning aanvragen voor de aanschaf van stoffen waarvoor beperkingen gelden, en de verduidelijking dat regels die voor marktdeelnemers gelden, ook gelden voor ondernemingen die online actief zijn.

Bovendien hebben de medewetgevers in het kader van de strijd tegen de financiering van terrorisme overeenstemming bereikt over het voorstel voor een richtlijn **ter vergemakkelijking van het gebruik van financiële en andere informatie** voor het

22 COM(2018) 630 final van 12.9.2018.
23 Zie de conclusies van de Europese Raad van juni 2018 en oktober 2018.
24 COM(2018) 209 final van 17.4.2018.

voorkomen, opsporen, onderzoeken of vervolgen van ernstige strafbare feiten[25]. Op grond van deze richtlijn – die eerst nog formeel moet worden vastgesteld en uitgevoerd – krijgen de aangewezen rechtshandhavingsautoriteiten en de bureaus voor de ontneming van vermogensbestanddelen rechtstreeks toegang tot bankrekeninginformatie in de nationale centrale registers van bankrekeningen. De richtlijn zal ook de samenwerking tussen de nationale financiële-inlichtingeneenheden en rechtshandhavingsautoriteiten versterken en de toegang van Europol tot financiële informatie vergemakkelijken.

Op basis daarvan zal de Commissie zich verder beraden over de samenwerking tussen de financiële-inlichtingeneenheden van de verschillende lidstaten, onder meer in het kader van het komende verslag over de samenwerking tussen de financiële-inlichtingeneenheden, overeenkomstig de vijfde antiwitwasrichtlijn[26]. Daarnaast buigt de Commissie zich momenteel, eveneens overeenkomstig de vijfde antiwitwasrichtlijn, over de mogelijke koppeling van nationale centrale registers van bankrekeningen en systemen voor gegevensontsluiting in de EU. De Commissie is ook bezig met de analyse van maatregelen voor confiscatie zonder veroordeling in de Unie. Tot slot zal de Commissie, naar aanleiding van een oproep van het Europees Parlement[27], blijven nagaan of aanvullende maatregelen om terrorismefinanciering in de EU te traceren, noodzakelijk, technisch haalbaar en evenredig zijn.

In het kader van de strijd tegen documentenfraude hebben de medewetgevers op 19 februari 2019 een voorlopig akkoord bereikt over het voorstel voor een verordening om de **beveiliging van identiteitskaarten van burgers van de Unie en van verblijfsdocumenten** te versterken[28], teneinde frauduleus gebruik van deze documenten door criminelen en terroristen te beletten. De Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement heeft het akkoord op 11 maart 2019 bevestigd. Zodra deze verordening wordt vastgesteld, zullen op grond ervan minimale beveiligingskenmerken voor nationale identiteitskaarten worden ingevoerd, waaronder biometrische kenmerken (een gezichtsopname en twee vingerafdrukbeelden) op een contactloze chip. Hierdoor zullen nationale identiteitskaarten en verblijfsdocumenten veel beter beveiligd zijn en wordt het voor terroristen en andere criminelen moeilijker dergelijke documenten te misbruiken of te vervalsen om de EU binnen te komen of zich binnen de EU te verplaatsen. Beter beveiligde identiteitsdocumenten zullen bijdragen tot de versterking van het beheer van de EU-buitengrenzen. Tegelijkertijd zullen beter beveiligde en betrouwbaardere documenten het voor EU-burgers gemakkelijker maken om hun recht van vrij verkeer uit te oefenen.

---

[25] De medewetgevers hebben op 12 februari 2019 een politiek akkoord bereikt over het voorstel van de Commissie (COM(2018) 213 final van 17.4.2018). Het politieke akkoord is op 20 februari 2019 bekrachtigd door het Comité van permanente vertegenwoordigers van de Raad en op 26 februari 2019 door de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement.

[26] Krachtens artikel 65, lid 2, van Richtlijn (EU) 2018/843 van 19 juni 2018 moet de Commissie uiterlijk op 1 juni 2019 een beoordeling verrichten van het kader voor de samenwerking tussen financiële-inlichtingeneenheden en derde landen en de belemmeringen en mogelijkheden voor nauwere samenwerking tussen de financiële-inlichtingeneenheden in de Unie, met inbegrip van de mogelijkheid om een coördinatie- en ondersteuningsmechanisme in te stellen.

[27] 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.

[28] COM(2018) 212 final van 17.4.2018.

Wat de voorstellen van de Commissie van april 2018 inzake **toegang tot elektronisch bewijsmateriaal** betreft, zit onvoldoende schot in de zaak. In meer dan de helft van alle strafrechtelijke onderzoeken wordt tegenwoordig immers een grensoverschrijdend verzoek om toegang tot elektronisch bewijsmateriaal ingediend[29]. De Raad heeft zijn onderhandelingsmandaat vastgesteld voor voorstellen voor een verordening[30] ter verbetering van de grensoverschrijdende toegang tot elektronisch bewijs in het kader van strafrechtelijk onderzoek, en voor een richtlijn[31] tot vaststelling van geharmoniseerde regels inzake de aanwijzing van wettelijke vertegenwoordigers ten behoeve van de bewijsgaring in strafprocedures. In het Europees Parlement is sinds de vaststelling van de voorstellen door de Commissie in april 2018 echter zeer weinig vooruitgang geboekt. Gezien het cruciale belang van efficiënte toegang tot elektronisch bewijsmateriaal voor 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.

Tegelijkertijd werkt de Commissie aan haar **internationale initiatieven inzake toegang tot elektronisch bewijsmateriaal** in het kader van de lopende onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa en de onderhandelingen met de Verenigde Staten. In het kader daarvan heeft de Commissie op 5 februari 2019 aanbevelingen[32] vastgesteld voor een onderhandelingsmandaat voor deze twee internationale initiatieven. De Raad heeft de ontwerpmandaten momenteel in behandeling, onder meer in het kader van de vergadering van de Raad Justitie en Binnenlandse Zaken van 7 en 8 maart 2019. De Commissie verzoekt de Raad zijn goedkeuring te hechten aan het besluit waarbij machtiging wordt verleend tot deelname aan de onderhandelingen over een tweede aanvullend protocol bij het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa, alsmede het besluit waarbij machtiging wordt verleend tot het openen van onderhandelingen met de Verenigde Staten over grensoverschrijdende toegang tot elektronisch bewijsmateriaal. Het is belangrijk vaart achter de onderhandelingen 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 de EU-wetgeving.

Om de armslag van terroristen te beperken, roept de Commissie:

- **het Europees Parlement op** om met spoed zijn onderhandelingsmandaat goed te keuren voor de wetgevingsvoorstellen inzake **elektronisch bewijsmateriaal**, zodat de trialoogbesprekingen met de Raad onverwijld van start kunnen gaan *(prioriteit van de gezamenlijke verklaring);*
- **de Raad op** om zijn goedkeuring te hechten aan het besluit waarbij machtiging wordt verleend tot deelname aan de onderhandelingen over een **tweede aanvullend protocol bij**

[29] 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).

[30] 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.

[31] COM(2018) 226 final van 17.4.2018. De Raad heeft tijdens de Raad Justitie en Binnenlandse Zaken van 8 maart 2019 zijn onderhandelingsmandaat voor het voorstel voor een richtlijn aangenomen.

[32] COM(2019) 70 final van 5.2.2019 en COM(2019) 71 final van 5.2.2019.

het Verdrag van Boedapest inzake cybercriminaliteit van de Raad van Europa, alsmede het besluit waarbij machtiging wordt verleend tot het openen van **onderhandelingen met de Verenigde Staten** over grensoverschrijdende toegang tot elektronisch bewijsmateriaal.

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

De capaciteit van interne en externe partijen om zich in het openbare debat te mengen en verkiezingen te manipuleren is reëler dan ooit en kan nog verder toenemen bij de aanstaande verkiezingen voor het Europees Parlement. De mogelijke gevolgen – ondermijning van democratische instellingen en ondergraving van hun legitimiteit – vormen een ernstige en toenemende strategische dreiging en maken een essentieel onderdeel uit van de veiligheidsuitdagingen waarmee de EU momenteel over de nationale grenzen heen wordt geconfronteerd en waartegen gezamenlijk, over de nationale grenzen heen moet worden opgetreden.

De verkiezingscampagnes voor de verkiezingen voor het Europees Parlement zullen in maart echt van start gaan. In de aanloop naar de bijeenkomst van de Europese Raad op 21 en 22 maart 2019 roept de Commissie de lidstaten op hun coördinatie en informatie-uitwisseling te intensiveren om desinformatie tegen te gaan en de verkiezingen tegen cyberdreigingen te beschermen. De lidstaten moeten optimaal gebruik maken van de door de EU beschikbaar gestelde instrumenten en informatiekanalen, met name het recent ingevoerde systeem voor snelle waarschuwing[33]. Gezien de bezorgdheid over de huidige situatie dringt de Commissie bij de onlineplatforms aan op extra inspanningen in alle lidstaten om de integriteit van de verkiezingen voor het Europees Parlement in mei 2019 te helpen waarborgen.

Om deze inspanningen te ondersteunen en aan te moedigen, zullen de Commissie en de hoge vertegenwoordiger maatregelen tegen cyberdreigingen blijven nemen op twee op elkaar aansluitende terreinen: het tegengaan van desinformatie en het versterken van de electorale weerbaarheid.

1. Actie tegen desinformatie

De blootstelling van burgers aan grootschalige desinformatie, met inbegrip van misleidende of gewoonweg foute informatie, kan een ernstige soort cyberdreiging inhouden en is een grote uitdaging voor de komende Europese verkiezingen. De Commissie ziet nauwlettend toe op de uitvoering van de maatregelen die zij heeft opgenomen in haar **mededeling van april 2018 over de bestrijding van online-desinformatie**[34].

De Commissie volgt bovendien van nabij de vorderingen die worden gemaakt in het kader van de **praktijkcode betreffende desinformatie**, die in oktober 2018 is ondertekend door vertegenwoordigers van onlineplatforms, leidende sociale netwerken, adverteerders en de reclame-industrie. De Commissie zal een uitgebreide beoordeling verrichten na de eerste

[33] Het systeem voor snelle uitwisseling past in het actieplan tegen desinformatie dat de Commissie en de hoge vertegenwoordiger in december 2018 hebben voorgesteld (zie hieronder) en zal fungeren als een platform waar de lidstaten, de EU-instellingen en de partners informatie over de lopende desinformatiecampagnes kunnen uitwisselen en hun reactie kunnen coördineren. Het systeem is uitsluitend gebaseerd op niet-vertrouwelijke informatie uit open bronnen.

[34] COM(2018) 236 final van 26.4.2018, gevolgd door het uitvoeringsverslag COM(2018) 794 final van 5.12.2018.

periode van twaalf maanden van toepassing van de code. Mochten de uitvoering en de impact van de praktijkcode onvoldoende blijken, dan kan de Commissie verdere maatregelen voorstellen, ook van wetgevende aard.

Op basis van deze werkzaamheden en naar aanleiding van de oproep tot bescherming van de democratische stelsels van de Unie, die de leiders in juni 2018 deden in het kader van de Europese Raad, hebben de Commissie en de hoge vertegenwoordiger in december 2018 een **gezamenlijk actieplan tegen desinformatie**[35] gepresenteerd. In het actieplan wordt benadrukt dat desinformatie van de kant van de Russische Federatie volgens de **EU-Fusiecel voor analyse van hybride dreigingen** de grootste bedreiging voor de EU vormt. Het gebeurt systematisch, met grote middelen en op een andere schaal dan in andere landen. Om het hoofd te bieden aan de dreiging die van desinformatie uitgaat, voorziet het actieplan in uitbreiding van de middelen voor de bestrijding ervan, en met name voor de **taskforces strategische communicatie** van de Europese Dienst voor extern optreden (EDEO), waaronder de Taskforce strategische communicatie oost[36]. Het actieplan voorziet tevens in uitbreiding van de middelen die voor deze kwestie beschikbaar zijn en roept ertoe op deze middelen de komende twee jaar te versterken.

Het actieplan bevat concrete maatregelen voor het aanpakken van desinformatie, waaronder het opzetten van een **systeem voor snelle waarschuwing**. In verband met de verkiezingen voor het Europees Parlement is het systeem voor snelle waarschuwing opgezet in maart 2019. Het wordt gebruikt door de EU-instellingen en de lidstaten om de uitwisseling van gegevens over en beoordelingen van desinformatiecampagnes te faciliteren en waarschuwingen te geven voor desinformatiedreigingen.

Het actieplan voorziet in nauw toezicht op de uitvoering van de eerder genoemde door de onlineplatforms ondertekende praktijkcode. Op 29 januari 2019 heeft de Commissie de **verslagen bekendgemaakt die waren ingediend door de ondertekenaars van de praktijkcode**: Google, Facebook, Twitter, Mozilla en de beroepsorganisaties van de reclamebranche. De Commissie toonde zich verheugd met de geboekte vooruitgang, maar vroeg de ondertekenaars ook om zich in de aanloop naar de verkiezingen voor het Europees Parlement van mei 2019 meer in te spannen[37].

De Commissie heeft op 28 februari 2019 **verslagen van Facebook, Google en Twitter** gepubliceerd over de vorderingen die in januari 2019 zijn gemaakt wat betreft hun verbintenissen om desinformatie te bestrijden. De platforms hebben in die verslagen echter niet genoeg informatie verstrekt waaruit blijkt dat nieuwe beleidsmaatregelen en instrumenten in alle EU-lidstaten tijdig en met voldoende middelen worden ingezet. Er is voor alle ondertekenaars duidelijk ruimte voor verbetering[38]. Meer in het bijzonder roept de Commissie de platforms op om volledige transparantie van politieke advertenties vanaf het begin van de campagne voor de Europese verkiezingen in alle EU-lidstaten te waarborgen, passende toegang tot gegevens van platforms voor onderzoeksdoeleinden mogelijk te maken en te zorgen voor goede samenwerking tussen de platforms en de afzonderlijke lidstaten via de contactpunten van het systeem voor snelle waarschuwing.

---

35 JOIN(2018) 36 final van 5.12.2018.

36 Sinds de oprichting in 2015 heeft de Taskforce strategische communicatie oost bijna 5 000 voorbeelden van desinformatie door de Russische Federatie in kaart gebracht, geanalyseerd en openbaar gemaakt, waarbij een groot aantal desinformatieverhalen, instrumenten, technieken en intenties van desinformatiecampagnes aan het licht zijn gekomen.

37 Zie voor meer details het persbericht http://europa.eu/rapid/press-release_IP-19-746_nl.htm.

38 Zie voor meer details http://europa.eu/rapid/press-release_STATEMENT-19-1379_nl.htm.

De Commissie zal op 20 maart 2019 opnieuw verslag uitbrengen over de uitvoering van de praktijkcode.

2. Versterking van de electorale weerbaarheid

Op 12 september 2018 heeft de Commissie een maatregelenpakket goedgekeurd dat de weerbaarheid van onze electorale systemen moet versterken. Het pakket is gericht tot de lidstaten en de Europese en nationale politieke partijen en politieke stichtingen en omvat een aanbeveling over electorale samenwerkingsnetwerken, onlinetransparantie, bescherming tegen cyberaanvallen en bestrijding van desinformatiecampagnes, richtsnoeren voor de toepassing van de EU-gegevensbeschermingswetgeving[39] en een wetswijziging die de regels voor de financiering van Europese politieke partijen aanscherpt.

Het pakket werd door het Europees Parlement gunstig ontvangen in zijn resolutie van 28 oktober 2018. De Raad verwelkomde het pakket in zijn conclusies van 19 februari 2019 over vrije en eerlijke Europese verkiezingen, waarin alle lidstaten zich gezamenlijk verbonden tot een gecoördineerde Europese aanpak voor het beschermen van de integriteit van de aanstaande Europese verkiezingen. De Raad Justitie en Binnenlandse Zaken besprak de stand van zaken op 7 maart 2019.

De wijziging van de verordening betreffende **het statuut en de financiering van Europese politieke partijen en Europese politieke stichtingen**[40] maakt het mogelijk sancties op te leggen tegen het illegale gebruik van persoonsgegevens om doelbewust de uitslag van de verkiezingen voor het Europees Parlement te beïnvloeden. Nadat in januari 2019 een politiek akkoord[41] was bereikt, keurde het Europees Parlement in plenaire zitting de tekst van de wijziging goed op 12 maart 2019. De wijziging moet van toepassing worden voordat in mei 2019 de verkiezingen voor het Europees Parlement plaatsvinden.

De aanbeveling betreffende **electorale samenwerkingsnetwerken, onlinetransparantie, bescherming tegen cyberincidenten en bestrijding van desinformatiecampagnes in het kader van de verkiezingen voor het Europees Parlement**[42], die gericht is tot de lidstaten en de nationale en Europese politieke partijen en politieke stichtingen, presenteert concrete maatregelen die de betrokken actoren op de genoemde gebieden zouden moeten nemen. Met het oog op de uitvoering van de aanbeveling hebben de nationale electorale netwerken contactpunten opgezet voor de deelname aan een **Europees netwerk voor electorale samenwerking**. Dit netwerk dient voor het geven van waarschuwingen over dreigingen, het uitwisselen van beste praktijken door de nationale netwerken, het bespreken van gemeenschappelijke oplossingen voor de geconstateerde problemen en het aanmoedigen van gezamenlijke projecten en oefeningen. Op de eerste bijeenkomst van het netwerk op 21 januari 2019 kwamen de deelnemers overeen dat een alomvattende aanpak essentieel is voor het waarborgen van de integriteit van de verkiezingen met behoud van een open democratisch debat en een gelijk politiek speelveld. De tweede bijeenkomst van het netwerk, die op 27 februari 2019 plaatsvond, concentreerde zich op monitoring- en handhavingsgerelateerde onderwerpen die voor de electorale context relevant zijn, waaronder gegevensbescherming, regulering van de media, rechtshandhaving, transparantie en sociale media, en de betrokkenheid van de verschillende belanghebbenden bij de monitoringactiviteiten. Er werden

39 COM(2018) 638 final van 12.9.2018.

40 COM(2018) 636 final van 12.9.2018.

41 Het tussen de medewetgevers bereikte politieke akkoord van 16 januari 2019 is op 25 januari 2019 bekrachtigd door het Comité van permanente vertegenwoordigers van de Raad en op 29 januari 2019 door de Commissie constitutionele zaken van het Europees Parlement.

42 C(2018) 5949 final van 12.9.2018.

voorbereidingen getroffen voor de deelname van de leden aan een cyberweerbaarheidsoefening, die onmiddellijk na de geplande volgende bijeenkomst van het netwerk van 5 april 2019 zou moeten worden gehouden.

Op 19 februari 2019 werd een door het Europees Parlement en de Commissie gezamenlijk georganiseerde **workshop over versterking van de cyberweerbaarheid in de electorale context** gehouden, met als doel de electorale systemen en infrastructuren beter te beveiligen en weerbaarder te maken tegen de zich voortdurend ontwikkelende cyberdreigingen. De voor cyberbeveiliging bevoegde nationale autoriteiten van de lidstaten, het EU-agentschap voor netwerk- en informatiebeveiliging en de onlineplatforms hebben maatregelen besproken, met de nadruk op acties die dringend en relevant zijn voor het verzekeren van de integriteit van de verkiezingen voor het Europees Parlement van mei 2019.

De EU-instellingen en de lidstaten werken ook nauw samen op het gebied van andere **voorlichtingsactiviteiten** die gericht zijn op bescherming van de integriteit van het electorale proces en op de betrokkenheid van actoren van de openbare en de particuliere sector, inclusief media, onlineplatforms en maatschappelijke organisaties.

Om desinformatie te bestrijden en de electorale weerbaarheid te waarborgen, dringen de Commissie en de hoge vertegenwoordiger er bij de lidstaten op aan:

- de maatregelen van het **gezamenlijke actieplan tegen desinformatie** van december 2018 snel en doortastend uit te voeren.

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

1. Uitvoering van wetgevingsmaatregelen in het kader van de Veiligheidsunie

Om de voordelen van een doeltreffende en echte Veiligheidsunie ten volle te kunnen benutten, moet er in de allereerste plaats voor worden gezorgd dat de overeengekomen maatregelen volledig en correct worden uitgevoerd. De Commissie ondersteunt de lidstaten hier actief bij, bijvoorbeeld door financiering te verstrekken en de uitwisseling van goede praktijken te faciliteren. Zo nodig maakt de Commissie gebruik van alle bevoegdheden die haar krachtens de Verdragen voor de handhaving van het EU-recht ter beschikking staan, inclusief inbreukprocedures in voorkomend geval.

In verband met de tenuitvoerlegging van de **EU-richtlijn inzake persoonsgegevens van passagiers**[43] heeft de Commissie op 19 juli 2018 inbreukprocedures ingeleid tegen veertien lidstaten wegens het niet-melden van de vaststelling van nationale wetgeving tot volledige omzetting van die richtlijn[44], die een essentieel instrument is voor de bestrijding van terrorisme en zware criminaliteit. Sindsdien hebben negen van die lidstaten gemeld dat zij de richtlijn volledig hebben omgezet[45]. Met redenen omklede adviezen zijn gezonden aan de lidstaten die de richtlijn nog niet volledig hebben omgezet: Spanje (24 januari 2019) en Finland en Nederland (7 maart 2019). Tegelijkertijd blijft de Commissie alle lidstaten steunen bij hun inspanningen om de ontwikkeling van hun systemen voor de registratie van

43 Richtlijn (EU) 2016/681 van 27.4.2016.

44 Bulgarije, Tsjechië, Estland, Griekenland, Spanje, Frankrijk, Cyprus, Luxemburg, Nederland, Oostenrijk, Portugal, Roemenië, Slovenië en Finland.

45 Bulgarije, Estland, Griekenland, Frankrijk, Cyprus, Luxemburg, Oostenrijk, Portugal en Roemenië (stand van zaken op 11 maart 2019).

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**[46] is verstreken op 8 september 2018. De Commissie heeft op 22 november 2018 inbreukprocedures ingeleid tegen zestien lidstaten die geen melding hebben gemaakt van nationale wetgeving waarbij de richtlijn volledig is omgezet. Sindsdien hebben negen van deze lidstaten gemeld dat zij de richtlijn volledig hebben omgezet[47]. De Commissie dringt er bij de overige zeven lidstaten op aan dat zij zo snel mogelijk de nodige maatregelen nemen[48].

De termijn voor de omzetting van de **richtlijn inzake de controle op de verwerving en het voorhanden hebben van wapens**[49] is verstreken op 14 september 2018. Tot nu toe hebben zes lidstaten gemeld dat zij de richtlijn volledig hebben omgezet[50] en hebben vijf lidstaten gedeeltelijke omzetting gemeld[51]. Met inbegrip van de lidstaten die gedeeltelijke omzetting hebben gemeld, hebben 22 lidstaten[52] op 22 november 2018 een met redenen omkleed advies van de Commissie ontvangen.

In verband met de omzetting in nationaal recht van de **richtlijn gegevensbescherming bij rechtshandhaving**[53] heeft de Commissie op 19 juli 2018 inbreukprocedures ingeleid tegen negentien lidstaten die geen nationale wetgeving hebben gemeld tot volledige omzetting van die richtlijn[54]. Inmiddels hebben 17 lidstaten gemeld dat zij de richtlijn volledig hebben omgezet en hebben vijf lidstaten gedeeltelijke omzetting gemeld[55]. Tot dusver zijn de procedures tegen zes lidstaten beëindigd[56] en hebben negen lidstaten op 25 januari 2019 een met redenen omkleed advies gekregen[57].

De Commissie wordt verwacht uiterlijk op 9 mei 2019 verslag uit te brengen over de coherentie van de identificatie van aanbieders van essentiële diensten. Aan de hand van de kennisgevingen van de lidstaten is vastgesteld dat de **richtlijn inzake de beveiliging van netwerk- en informatiesystemen**[58] in 25 lidstaten volledig is omgezet en in één lidstaat

---

46 Richtlijn (EU) 2017/541 van 15.3.2017.

47 Bulgarije, Tsjechië, Duitsland, Estland, Spanje, Frankrijk, Kroatië, Italië, Letland, Litouwen, Hongarije, Malta, Nederland, Oostenrijk, Portugal, Slowakije, Finland en Zweden hebben omzetting gemeld (stand van zaken op 11 maart 2019).

48 België, Polen, Roemenië en Slovenië hebben gemeld dat zij de richtlijn gedeeltelijk hebben omgezet. Griekenland, Cyprus en Luxemburg hebben helemaal niets gemeld (stand van zaken op 11 maart 2019).

49 Richtlijn (EU) 2017/853 van 17.5.2017.

50 Denemarken, Frankrijk, Kroatië, Italië, Malta en Oostenrijk (stand van zaken op 11 maart 2019).

51 Tsjechië, Estland, Litouwen, Portugal en het Verenigd Koninkrijk (stand van zaken op 11 maart 2019).

52 België, Bulgarije, Tsjechië, Duitsland, Estland, Ierland, Griekenland, Spanje, Cyprus, Letland, Litouwen, Luxemburg, Hongarije, Nederland, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk (stand van zaken op 11 maart 2019).

53 Richtlijn (EU) 2016/680 van 27.4.2016.

54 België, Bulgarije, Tsjechië, Estland, Griekenland, Spanje, Frankrijk, Kroatië, Cyprus, Letland, Litouwen, Luxemburg, Hongarije, Nederland, Polen, Portugal, Roemenië, Slovenië en Finland. De Commissie ontvangt momenteel de antwoorden van de lidstaten, waaronder kennisgeving van de relevante wetgeving, en analyseert deze momenteel (stand van zaken op 11 maart 2019).

55 België, Duitsland, Estland, Ierland, Frankrijk, Kroatië, Italië, Litouwen, Luxemburg, Hongarije, Malta, Oostenrijk, Polen, Roemenië, Slowakije, Zweden en het Verenigd Koninkrijk hebben volledige omzetting gemeld. Tsjechië, Portugal, Finland, Slovenië en Nederland hebben gedeeltelijke omzetting gemeld. In Denemarken is de omzetting afgerond (stand van zaken op 11 maart 2019).

56 België, Frankrijk, Kroatië, Litouwen, Luxemburg en Hongarije (stand van zaken op 11 maart 2019).

57 Bulgarije, Tsjechië, Griekenland, Spanje, Cyprus, Letland, Nederland, Portugal en Slovenië (stand van zaken op 11 maart 2019).

58 Richtlijn (EU) 2016/1148 van 27.4.2016.

gedeeltelijk is omgezet[59]. De Commissie heeft in januari 2019 de inbreukprocedures wegens niet-kennisgeving van omzetting tegen zes lidstaten beëindigd[60]. Tegen negen lidstaten[61] loopt nog een inbreukprocedure omdat zij nog geen volledige omzetting van de richtlijn hebben gemeld. In verband met de omzetting van de richtlijn inzake de beveiliging van netwerk- en informatiesystemen hadden de lidstaten de Commissie uiterlijk 9 november 2018 moeten informeren over de op hun grondgebied geïdentificeerde aanbieders van essentiële diensten. De Commissie beoordeelt momenteel de door de lidstaten verstrekte informatie[62].

De Commissie beoordeelt bovendien de omzetting van de **vierde antiwitwasrichtlijn**[63] en controleert ook of de regels door de lidstaten worden toegepast. De Commissie heeft tegen alle 28 lidstaten inbreukprocedures 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[64]. Zij zal waar nodig haar bevoegdheden blijven gebruiken om de volledige tenuitvoerlegging van deze richtlijn te waarborgen.

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 inzake persoonsgegevens van passagiers**: drie lidstaten moeten nog kennisgeving doen van omzetting in nationaal recht en twee lidstaten moeten de kennisgeving van de omzetting nog vervolledigen[65];
- de **richtlijn inzake de beveiliging van netwerk- en informatiesystemen**: twee lidstaten moeten nog melding doen van omzetting in nationaal recht en één lidstaat moet nog melding doen van vervollediging van de omzetting[66];
- de **richtlijn terrorismebestrijding**: drie lidstaten moeten nog kennisgeving doen van omzetting in nationaal recht en vier lidstaten moeten nog vervollediging van de omzetting melden[67];
- de **richtlijn inzake de controle op de verwerving en het voorhanden hebben van**

59 Bulgarije, Tsjechië, Denemarken, Duitsland, Griekenland, Estland, Ierland, Spanje, Frankrijk, Kroatië, Italië, Cyprus, Letland, Litouwen, Malta, Nederland, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Finland, Zweden en het Verenigd Koninkrijk hebben volledige omzetting gemeld. Hongarije heeft gedeeltelijke omzetting gemeld. België en Luxemburg hebben aan de Commissie geen enkele nationale omzettingsmaatregel gemeld (stand van zaken op 11 maart 2019).

60 Ierland, Spanje, Frankrijk, Kroatië, Nederland en Portugal (stand van zaken op 11 maart 2019).

61 Bulgarije, België, Denemarken, Letland, Litouwen, Luxemburg, Hongarije, Oostenrijk en Roemenië (stand van zaken op 11 maart 2019).

62 Bulgarije, Denemarken, Duitsland, Tsjechië, Estland, Ierland, Spanje, Frankrijk, Kroatië, Italië, Cyprus, Litouwen, Hongarije, Malta, Nederland, Polen, Portugal, Slowakije, Finland, Zweden en het Verenigd Koninkrijk (stand van zaken op 11 maart 2019).

63 Richtlijn (EU) 2015/849 van 20.5.2015.

64 De Commissie heeft tegen alle lidstaten inbreukprocedures ingeleid wegens niet-melding van de nationale wetgeving tot volledige omzetting van de richtlijn, aangezien zij na beoordeling tot de conclusie is gekomen dat sommige bepalingen van de richtlijn niet zijn omgezet.

65 Spanje, Nederland en Finland moeten nog kennisgeving doen van omzetting. Tsjechië en Slovenië hebben gedeeltelijke, maar nog geen volledige omzetting gemeld (stand van zaken op 11 maart 2019). 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.

66 België en Luxemburg moeten nog melding doen van omzetting. Hongarije heeft gedeeltelijke omzetting gemeld en moet de omzetting nog vervolledigen (stand van zaken op 11 maart 2019).

67 Griekenland, Cyprus en Luxemburg moeten nog melding doen van omzetting. België, Polen, Roemenië en Slovenië hebben gedeeltelijke omzetting gemeld en moeten de omzetting nog vervolledigen (stand van zaken op 11 maart 2019).

wapens: 17 lidstaten hebben nog geen omzetting in nationaal recht gemeld en vijf lidstaten moeten de omzetting nog vervolledigen[68];

- de richtlijn **gegevensbescherming bij rechtshandhaving**: vijf lidstaten moeten nog omzetting in nationaal recht melden en vijf lidstaten moeten de omzetting nog vervolledigen[69]; en
- de **vierde antiwitwasrichtlijn**: één lidstaat moet nog vervollediging van de omzetting melden[70].

2. Bescherming van openbare ruimten: aanbevolen goede praktijken

In het kader van de praktische werkzaamheden om de bescherming te verbeteren en de weerbaarheid tegen terrorisme te versterken, blijft de Commissie steun verlenen aan de lidstaten en hun plaatselijke autoriteiten voor de **bescherming van openbare ruimten**. De werkzaamheden voor de uitvoering van het actieplan ter ondersteuning van de bescherming van openbare ruimten[71] van oktober 2017 zijn met name gericht op ontwikkelen en verzamelen van richtsnoeren en goede praktijken. In het zogenoemde forum van beheerders[72] werkt de Commissie samen met overheidsinstanties en particuliere beheerders van openbare ruimten. Zij heeft goede praktijken vastgesteld voor verschillende maatregelen die alle bij de bescherming van openbare ruimten betrokken beheerders en overheidsinstanties kunnen uitvoeren om de beveiliging te verbeteren[73]. De desbetreffende praktijken bieden eenvoudige stappen die als leidraad kunnen dienen voor het werk dat in de toekomst in alle relevante sectoren moet worden verricht om openbare ruimten beter te beschermen (zie kader hieronder).

Goede praktijken voor overheidsinstanties en particuliere beheerders ten behoeve van een betere beveiliging van openbare ruimten

Beoordeling en planning

- Kwetsbaarheidsbeoordelingen opstellen en uitvoeren om vast te stellen waar er sprake kan zijn van kwetsbaarheid voor aanvallen van buitenaf of van binnenuit.
- Voor de faciliteit of het evenement een beveiligingsplan ontwikkelen en uitvoeren, met inbegrip van voorbereidende maatregelen, noodmaatregelen en herstelmaatregelen, waarin

68 België, Bulgarije, Duitsland, Ierland, Griekenland, Spanje, Cyprus, Letland, Luxemburg, Hongarije, Nederland, Polen, Roemenië, Slovenië, Slowakije, Finland en Zweden moeten nog omzetting melden. Tsjechië, Estland, Litouwen, Portugal en het Verenigd Koninkrijk hebben gedeeltelijke, maar nog geen volledige omzetting gemeld (stand van zaken op 11 maart 2019). 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.

69 Bulgarije, Griekenland, Spanje, Cyprus en Letland moeten nog omzetting melden. Tsjechië, Nederland, Portugal, Slovenië en Finland hebben gedeeltelijke, maar nog geen volledige omzetting gemeld (stand van zaken op 11 maart 2019).

70 Roemenië heeft kennisgeving gedaan van gedeeltelijke omzetting, maar nog niet van volledige omzetting. Alle overige lidstaten hebben volledige omzetting gemeld. Volgens de beoordeling van de Commissie is echter een aantal bepalingen van de richtlijn nog niet volledig omgezet (stand van zaken op 11 maart 2019).

71 COM(2017) 612 final van 18.10.2017.

72 Het forum van beheerders is opgericht op grond van het actieplan ter ondersteuning van de bescherming van openbare ruimten van oktober 2017. De deelnemers zijn beleidsmakers van de lidstaten en particuliere beheerders in diverse sectoren, zoals massa-evenementen en amusement, horeca, winkelcentra, sport- en cultuurcentra, verkeersknooppunten en dergelijke.

73 Zie voor nadere bijzonderheden het werkdocument van de diensten van de Commissie over goede praktijken ter ondersteuning van de bescherming van openbare ruimten (SWD(2019) 140 van 20.3.2019).

passende beveiligingsmaatregelen voor de omgeving van de faciliteit of het evenement zijn opgenomen. De beveiligingsmaatregelen moeten doeltreffend, discreet en evenredig zijn en afgestemd zijn op het specifieke functioneren van de diverse omgevingen.

- Een persoon aanwijzen en opleiden die belast wordt met de coördinatie en uitvoering van de in het beveiligingsplan opgenomen maatregelen.
- Een crisismanagementplan ontwikkelen en uitvoeren.

Voorlichting en training

- Voorlichtingscampagnes opzetten over het melden van verdacht gedrag en hoe te reageren bij een aanslag op de beveiliging van een faciliteit of evenement.
- Een intern voorlichtingsprogramma inzake beveiliging voor alle werknemers opzetten en uitvoeren.
- Een bewustmakingsprogramma inzake dreigingen van binnenuit opzetten en uitvoeren om bij te dragen tot de bescherming van faciliteiten en evenementen tegen verschillende soorten dreigingen van binnenuit, zoals sabotage, diefstal van handelsgeheimen en terroristische aanslagen.
- Programma's voor basisopleiding van alle personeel inzake beveiliging opzetten en specifieke opleidingen inzake beveiliging verstrekken die bijdragen tot de ontwikkeling van een veiligheidscultuur in de organisatie. Activiteiten ontwikkelen die het personeel motiveren om solide beveiligingspraktijken toe te passen en een hoog niveau van waakzaamheid op het gebied van veiligheid in acht te nemen.
- Regelmatige beveiligingsoefeningen houden die bijdragen tot vaststelling van het niveau van paraatheid, waar het gaat om het afwenden van en reageren op aanslagen.

Fysieke beveiliging

- Problemen in verband met de beveiliging en fysieke bescherming beoordelen vanaf het begin van de ontwerpfase van nieuwe faciliteiten en evenementen.
- De noodzakelijke toegangscontroles en versperringen beoordelen en ervoor zorgen dat geen nieuwe kwetsbaarheden ontstaan. Toegangscontroles en versperringen mogen niet leiden tot een verschuiving van risico's en het ontstaan van nieuwe doelwitten.
- Beoordelen wat de meest geschikte technologie is voor de opsporing van explosieven, vuurwapens, steekwapens en chemische, biologische, radiologische en nucleaire agentia.

Samenwerking

- Contactpunten opzetten en de respectieve taken en verantwoordelijkheden vaststellen voor publiek-private samenwerking inzake veiligheidsaangelegenheden (bv. de samenwerking tussen beheerders, particuliere beveiligingsfirma's en rechtshandhavingsautoriteiten) en met het oog op betere communicatie en samenwerking op regelmatige basis.
- Betrouwbare en tijdige communicatie en samenwerking tot stand brengen om de verantwoordelijke overheidsinstanties, plaatselijke rechtshandhavingsautoriteiten en particuliere ondernemingen in staat te stellen specifieke risico- en dreigingsinformatie uit te wisselen.
- De werkzaamheden inzake de bescherming van openbare ruimten op lokaal, regionaal en nationaal niveau coördineren en zorgen voor communicatie en uitwisseling van goede praktijken op alle niveaus, inclusief op EU-niveau.
- Overheidsinstanties zouden samen met de beheerders praktische aanbevelingen en richtsnoeren moeten opstellen en publiceren voor het opsporen, terugdringen en beantwoorden van veiligheidsdreigingen.

3. Kwetsbaarheid van de digitale infrastructuur

Digitale weerbaarheid is essentieel voor de bescherming van de activiteiten van de overheid, industriële research, intellectuele eigendom, bedrijfsplannen, verkiezingen, democratische instellingen en onze eigen persoonsgegevens. Tot de belangrijkste kwesties op het gebied van cyberbeveiliging die momenteel veel aandacht krijgen in het publieke debat in de EU behoren de netwerken van de vijfde generatie (5G). Op de laatste informele ministerraad over telecommunicatie, die op 1 maart 2019 in Boekarest plaatsvond, spraken de ministers hun steun uit voor een gecoördineerde Europese aanpak om de digitale weerbaarheid in de EU met betrekking tot 5G-netwerken te versterken. De 5G-netwerkinfrastructuur vormt een belangrijke basis voor de digitale economie. 5G-technologie is er niet alleen voor consumentendiensten, maar is opgezet en bedoeld voor kritieke dienstverlening in verticale sectoren op het gebied van onder andere mobiliteit, energie en gezondheid. De normen voor 5G-netwerken gelden wereldwijd, en apparatuur en uitrusting zullen worden aangeboden door een aantal mondiaal actieve leveranciers.

De uitrol van 5G-netwerken gedurende de komende jaren betekent een grote stap voorwaarts in vergelijking met de eerdere netwerken. Dankzij dataopslag in de cloud kunnen miljarden apparaten met internet worden verbonden en worden nieuwe innovaties op het gebied van kunstmatige intelligentie mogelijk, waardoor voor burgers en bedrijven nieuwe kansen worden gecreëerd. Cyberbeveiliging is daarom van bijzonder belang, aangezien door misbruik van kwetsbaarheden zeer ernstige schade kan worden veroorzaakt. Aangezien het internet geen grenzen kent, heeft een beveiligingslek in één lidstaat potentieel ook gevolgen in vele andere.

Als bescherming tegen potentieel ernstige gevolgen voor de veiligheid van kritieke digitale infrastructuur moet er een gemeenschappelijke EU-benadering komen voor de beveiliging van 5G-netwerken. Als startsein zal de Commissie na de Europese Raad van 21 en 22 maart 2019 een aanbeveling vaststellen voor een gemeenschappelijke EU-benadering van de veiligheidsrisico's van 5G-netwerken. Die zal berusten op een gecoördineerde EU-risicobeoordeling en maatregelen voor risicobeheer, op een raamwerk voor effectieve samenwerking en informatie-uitwisseling, en op gedeeld situationeel bewustzijn van de EU ten aanzien van kritieke communicatienetwerken. Bij de discussie over mogelijke maatregelen moet ook worden gedacht aan de toepassing van kwantumtechnologieën voor netwerkbeveiliging en voor de bescherming van opgeslagen gegevens[74].

Het Europees Parlement heeft op 12 maart 2019 een resolutie aangenomen over de veiligheidsdreigingen in verband met de toenemende technologische aanwezigheid van China in de EU en mogelijke maatregelen op EU-niveau om deze tegen te gaan.

4. Extern

De onderhandelingen tussen de EU en Canada over **aanpassing van de overeenkomst inzake persoonsgegevens van passagiers** gaan goed vooruit. De aanstaande top tussen de EU en Canada, die op 11 en 12 april 2019 in Montreal zal plaatsvinden, kan een positieve impuls aan de onderhandelingen geven.

De Commissie werkt samen met de autoriteiten van de Verenigde Staten aan de komende gezamenlijke evaluatie van de **overeenkomst tussen de VS en de EU inzake**

[74] Zie ook de mededeling over het Europees cloudinitiatief – Bouwen aan een concurrentiële data- en kenniseconomie in Europa (COM(2016) 178 final van 19.4.2016).

persoonsgegevens van passagiers[75], die overeenkomstig de bepalingen van die overeenkomst zal worden verricht. Er wordt ook al gewerkt aan de vijfde gezamenlijke evaluatie van de **overeenkomst tussen de EU en de VS inzake het programma voor het traceren van terrorismefinanciering**[76]. Bij de gezamenlijke evaluatie wordt ook gekeken naar de bepalingen van de overeenkomst inzake waarborgen, beschermingsmaatregelen en wederkerigheid, waardoor ook de waarde van het programma voor de EU en de VS als instrument voor terrorismebestrijding wordt beoordeeld.

De lopende ontwikkelingen op het terrein in Syrië hebben de discussie over **buitenlandse terroristische strijders** die zich momenteel in conflictgebieden bevinden of daar vast worden gehouden, scherper onder de aandacht gebracht. De EU kan desgevraagd steun verlenen aan de lidstaten, met name wat betreft de informatie-uitwisseling en ondersteuning van strafrechtelijk onderzoek, en in het bijzonder de samenwerking met internationale partners en via Europol, alsmede op basis van de expertise en beste praktijken op het gebied van rehabilitatie en re-integratie die in het kader van het netwerk voor voorlichting over radicalisering zijn ontwikkeld. De EU kan ook ondersteuning voor capaciteitsopbouw bieden aan derde landen die bijzondere problemen hebben met terugkerende buitenlandse terroristische strijders. Het besluit om buitenlandse terroristische strijders en hun gezinsleden al dan niet te repatriëren uit conflictgebieden, moet door de betrokken lidstaten worden genomen.

De EU en Egypte traden gezamenlijk op als voorzitter van de plenaire vergadering van de werkgroep Oost-Afrika van het **Mondiaal Forum Terrorismebestrijding**, die op 20 februari 2019 plaatsvond in Nairobi. Aan die vergadering werd deelgenomen door een groot aantal vertegenwoordigers van politie en justitie uit Somalië, Kenia, Sudan, Uganda, Djibouti, Ethiopië, Jemen en Tanzania.

V. CONCLUSIE

De EU heeft aanzienlijke vooruitgang geboekt bij het gezamenlijke werk aan de totstandbrenging van een echte en doeltreffende Veiligheidsunie. Zo hebben het Europees Parlement en de Raad de afgelopen weken en maanden een aantal prioritaire wetgevingsinitiatieven vastgesteld. In de aanloop naar de verkiezingen voor het Europees Parlement in mei 2019 zijn echter verdere inspanningen nodig om spoedeisende beveiligingskwesties aan te pakken. Met name roept de Commissie de medewetgevers ertoe op onderhandelingen te openen over de voorgestelde regels inzake de verwijdering van terroristische online-inhoud, zodra het Europees Parlement zijn onderhandelingsmandaat heeft vastgesteld, zodat een akkoord nog tijdens de huidige zittingsperiode van het Europees Parlement kan worden bereikt. De onderhandelingen over het voorstel tot versterking van de Europese grens- en kustwacht verkeren reeds in de trialoogfase. Hieruit blijkt dat alle instellingen ernaar streven het voorstel nog vóór de verkiezingen voor het Europees Parlement goed te keuren. De Commissie roept ook alle lidstaten op alle EU-maatregelen uit te voeren die in het kader van de Veiligheidsunie zijn overeengekomen, zodat ze het beoogde effect sorteren voor de veiligheid van de burgers.

Omdat de Unie voorbereid moet zijn voordat de Europese kiezers in mei 2019 naar de stembus gaan en haar dus weinig tijd rest, roept de Commissie bovendien alle betrokkenen op om met het oog op de bestrijding van desinformatie nog intensiever te werken aan de electorale weerbaarheid. In de aanloop naar de Europese Raad van 21–22 maart 2019 moeten

[75] PB L 215 van 11.8.2012, blz. 5.
[76] PB L 195 van 27.7.2010, blz. 5.

de lidstaten hun inspanningen op het gebied van coördinatie en informatie-uitwisseling opvoeren om desinformatie te bestrijden en de verkiezingen te beschermen tegen andere cyberdreigingen, en daarbij alle middelen inzetten die de EU daarvoor biedt. Daarnaast moeten onlineplatforms zich in alle lidstaten intensiever inzetten om de integriteit van de verkiezingen voor het Europees Parlement van mei 2019 te waarborgen. Met het oog op de bescherming van die integriteit zal de Commissie deze werkzaamheden de komende weken en maanden blijven steunen en aanmoedigen.