Fiche 2: Mededeling Veiligheidsuniestrategie

1. Algemene gegevens

a) Titel voorstel

Mededeling betreffende de EU-strategie voor de veiligheidsunie

b) Datum ontvangst Commissiedocument

24 juli 2020

c) Nr. Commissiedocument

COM (2020) 605

d) EUR-Lex

https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52020DC0605&from=EN

e) Nr. impact assessment Commissie en Opinie Raad voor Regelgevingstoetsing

Niet opgesteld

f) Behandelingstraject Raad

Justitie en Binnenlandse Zaken Raad

g) Eerstverantwoordelijk ministerie

Ministerie van Justitie en Veiligheid

2. Essentie voorstel

Op 24 juli 2020 heeft de Commissie de Veiligheidsunie Strategie voor 2020-2025 (hierna de strategie) gepubliceerd. Tegelijkertijd presenteerde de Commissie een EU strategie voor de bestrijding van kindermisbruik[1], EU agenda en actieplan over Drugs[2] en EU actieplan op vuurwapens[3], waarover separaat BNC-fiches aan uw Kamer worden verzonden.

De strategie bestrijkt de periode 2020–2025 en bouwt voort op eerdere werkzaamheden van het Europees Parlement, de Raad en de Commissie. De Commissie stelt dat een sterke kern van instrumenten en beleidsmaatregelen in de praktijk nodig is voor een toekomstbestendige veiligheidsomgeving in de EU. De COVID-19 crisis heeft de noodzaak om de veiligheid te waarborgen, zowel fysiek als digitaal, des te urgenter gemaakt. De Commissie beoogt een multidisciplinaire, geïntegreerde EU aanpak en benoemt strategische prioriteiten en bijbehorende maatregelen.

De Commissie geeft aan dat de Strategie drie gemeenschappelijke doelstellingen heeft, te weten de opbouw van capaciteiten met het oog op vroegtijdige opsporing en preventie van en respons op

[1] COM (2020) 607
[2] COM (2020) 606
[3] COM (2020) 608

crises; nadruk op resultaten; en het samenbrengen van alle publieke en private actoren in een gezamenlijke inspanning. Daarbij gaat de Commissie uit van een samenlevings-brede aanpak van veiligheid, waarmee op gecoördineerde wijze een doeltreffende respons kan worden gegeven op snel veranderende dreigingssituaties.

In de strategie onderscheidt de Commissie vier strategische prioriteiten:

1. Een toekomstbestendige veiligheidsomgeving. Hierbij stelt de Commissie zich een robuuste bescherming van vitale infrastructuur ten doel en richt zij zich op maatregelen ten behoeve van weerbaarheid, zowel fysiek als digitaal. De Commissie roept op tot een samenlevings-brede aanpak van cyberveiligheid die moet samenkomen in een herziene EU Cyberveiligheid strategie. Tevens benoemt de Commissie de oprichting van de Joint Cyber Unit en het belang van 5G beveiliging in het licht van potentiële systemische verstoringen van vitale diensten. Tot slot stelt de Commissie dat de bescherming van publieke ruimten verbeterd moet worden.
2. Het aanpakken van veranderende dreigingen. In de strijd tegen cybercrime benoemt de Commissie twee prioriteiten: preventie door veilige infrastructuur en internationale samenwerking en versterking van de capaciteit van rechtshandhavingsautoriteiten in het digitale domein. Daarnaast zet de Commissie in op het tegengaan van illegale inhoud online, waaronder seksueel kindermisbruik en terroristische inhoud online, en de dreiging die uitgaat van hybride campagnes ingezet door (statelijke) actoren.
3. De bescherming tegen terrorisme en georganiseerde criminaliteit. Bij de strijd tegen terrorisme en radicalisering acht de Commissie EU-samenwerking en coördinatie noodzakelijk. Ook noemt de Commissie hier het mandaat van het Europees Openbaar Ministerie (EOM) te willen uitbreiden met de vervolging van grensoverschrijdende terroristische misdrijven.
   De Commissie stelt daarnaast dat de EU-strijd tegen georganiseerde criminaliteit moet worden versterkt. Deze inzet wordt samengebracht in een toekomstige EU-agenda voor de aanpak van georganiseerde criminaliteit. Voorts wordt de haalbaarheid onderzocht van een EU-systeem voor snelle waarschuwing bij cybercriminaliteit, dat bij een golf van cybercriminaliteit informatievoorziening en een snelle respons kan waarborgen. De Commissie gaat ook inzetten op de aanpak van drugshandel, mensenhandel en mensensmokkel, tegengaan van illegale handel in vuurwapens, milieucriminaliteit, het tegengaan van economische en financiële vormen van criminaliteit en corruptiebestrijding.
4. Een krachtig veiligheidsecosysteem. Hierbij wordt ingegaan op informatie-uitwisseling, met inzet op operationele samenwerking van rechtshandhavingsautoriteiten en versterking van samenwerking met en tussen relevante autoriteiten. De Commissie geeft aan dat het nodig kan zijn de Prüm-besluiten[4] te herzien en het doorgeven van persoonsgegevens van passagiers (PNR-gegevens)[5] aan derde landen te gaan evalueren. De Commissie wil het mandaat van Europol herzien en een innovatie hub voor interne veiligheid oprichten bij Europol. De Commissie benadrukt het belang van internationale samenwerking met derde

[4] De Prümbesluiten van 2008 zijn gericht op geautomatiseerde uitwisseling van DNA-, vingerafdruk- en kentekengegevens tussen deelnemende EU-lidstaten.
[5] In het kader van de PNR Richtlijn (2016/681) worden Passenger Name Records (een specifieke set passagiersgegevens) verzameld, verwerkt, opgeslagen en doorgegeven aan rechtshandhavingsinstanties voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

landen en effectief grensmanagement aan externe grenzen. Ook zet de Commissie in op het vergroten van vaardigheden en bewustzijn. Voorts zal de Commissie onderzoek doen naar een EU-code voor politiële samenwerking en politiecoördinatie in crisistijden. Tot slot noemt de Commissie toetreding van de EU tot het Verdrag van Istanboel[6] als prioriteit.

De Commissie concludeert in de strategie dat veiligheidsonderwerpen vanuit een breder perspectief moeten worden bezien en dat het onderscheid tussen de fysieke en digitale wereld oneigenlijk is. Ook is interne en externe veiligheid in toenemende mate met elkaar verweven. De EU zal daarom meer met internationale partners moeten samenwerken. Tot slot concludeert de Commissie dat beleid of acties alleen effectief zijn als ze ook daadwerkelijk worden geïmplementeerd en worden gehandhaafd.

3. Nederlandse positie ten aanzien van de mededeling/aanbeveling

a) Essentie Nederlands beleid op dit terrein

Op de voor het kabinet prioritaire thema's uit de Veiligheidsuniestrategie is de essentie van het Nederlands beleid als volgt.

In de aanpak van ondermijnende criminaliteit wordt ingezet op structurele versterking volgens het devies «oprollen, afpakken en voorkomen», onder andere met stevige structurele investeringen in Bewaken en Beveiligen en het Multidisciplinair Interventie Team (MIT). Ook worden gerichte impulsen gegeven, onder meer om de jongerenpreventie te verbeteren, om de financiële opsporing daadkrachtiger te maken en om voortgezet crimineel handelen in detentie tegen te gaan.[7] De Nederlandse benadering om (online) seksueel kindermisbruik tegen te gaan, geschiedt langs een drietal lijnen: een intensieve strafrechtelijke aanpak, preventie en publiek-private samenwerking.[8]

Voorts zet het kabinet in op versterking van de capaciteit van de rechtshandhavingsautoriteiten in het digitale domein, zoals door oprichting van het Nationaal Politielab AI waarbij de verdere ontwikkeling van AI-toepassingen binnen de politie wordt gestimuleerd en er ook stapsgewijs nieuwe concepten worden ontwikkeld in nauwe samenwerking met de wetenschap.[9] Ook de blijvende toename van cybercrime is een aandachtspunt voor het kabinet waarvoor een aanpak is opgezet bestaande uit preventie, opsporing, vervolging, sanctionering en verstoring. Daarbij moet ook aandacht zijn voor het slachtoffer.[10] Ten aanzien van encryptie is het kabinet momenteel aan het bezien hoe rechtmatige toegang tot versleutelde communicatie kan worden verkregen en betrekt daarbij de voor- en nadelen daarvan.[11] Hierbij wordt gestreefd naar oplossingen binnen de

[6] Verdrag inzake het voorkomen en bestrijden van geweld tegen vrouwen en huiselijk geweld
[7] Kamerbrief van 18 juni 2020, Tweede Kamer, vergaderjaar 2019–2020, 29 911, nr. 281
[8] Kamerbrief van 7 juli 2020, Tweede Kamer, vergaderjaar 2019-2020, 31015, nr. 201
[9] Kamerbrief van 3 december 2019, Tweede Kamer, Vergaderjaar 2019-2020, 26643 nr. 652
[10] Kamerbrief van 29 juni 2020, Tweede Kamer, Vergaderjaar 2019-2020, 26643 nr. 696
[11] Tweede Kamer 2019/2020, aanhangsel van de Handelingen 1480

kaders van het kabinetstandpunt van 2016[12] en bezien of een internationale oplossing mogelijk is.[13]

Het weerbaar maken van Nederland tegen digitale dreigingen wordt door het kabinet op geïntegreerde wijze geadresseerd met de Nederlandse Cyber Security Agenda.[14] De aanpak op het gebied van statelijke dreigingen bestaat uit maatregelen gericht op het verhogen van de weerbaarheid tegen verschillende uitingen van statelijke dreigingen. De accenten liggen hierbij op het tegengaan van ongewenste buitenlandse inmenging, beschermen van democratische processen en instituties, waaronder het tegengaan van desinformatie, en economische veiligheid.[15] Het kabinet acht het van belang om strategische afhankelijkheden in kaart te brengen zodat nationale veiligheidsrisico's kunnen worden onderkend en geadresseerd.[16] Om vitale infrastructuur te beschermen, zet het kabinet in op een versterkte aanpak om kennis, kunde en expertise te bundelen om nationale veiligheidsrisico's ten behoeve van de vitale infrastructuur adequaat te adresseren.[17]

Bestrijding van terrorisme en extremisme vergt onverminderd de aandacht. Het is van groot belang de versterkte inzet waar nodig op basis van actuele dreigingsbeelden te intensiveren. Daarnaast wordt ingezet op het toepassen van de integrale aanpak op alle vormen van extremisme, van welke ideologische signatuur dan ook, zodat ook 'nieuwe' dreigingen het hoofd geboden kunnen worden. [18]

b) Beoordeling + inzet ten aanzien van dit voorstel

Het kabinet verwelkomt de strategie waarin een multidisciplinaire, geïntegreerde EU aanpak is beoogd voor een toekomstbestendige veiligheidsomgeving in de EU. Dat neemt niet weg dat bij de verdere uitwerking van de strategie een aantal aandachtspunten geïdentificeerd zijn. Hieronder worden prioritaire thema's voor het kabinet uitgelicht en de aandachtspunten benoemd.

Op het gebied van de aanpak van ondermijnende criminaliteit is het kabinet positief over de strategie. Het kabinet is voorstander van aandacht voor preventie en het ontmantelen van het bedrijfsmodel van de georganiseerde criminaliteit in de aangekondigde Agenda voor de aanpak van georganiseerde criminaliteit. Wel is van belang dat deze Agenda goed aansluit bij andere initiatieven zoals het Actieplan Drugs[19] en het Actieplan Vuurwapenhandel.[20] Het kabinet hecht ook aan versterkte informatie-uitwisseling zoals door de modernisering van de Prüm-besluiten en de aandacht voor de financiële aanpak van veiligheidsrisico's, waarbij de aanpak van witwassen en

[12] Kabinetsstandpunt 2016 is dat het "op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan ten grondslag liggen uitdragen." Tweede Kamer 2015/16, 26 643, nr. 383
[13] Tweede Kamer 2019/2020, aanhangsel van de Handelingen 1095
[14] Kamerbrief van 20 april 2018, Tweede Kamer, Vergaderjaar 2017-2018, 26643, nr. 536 25 juni 2020, Tweede Kamer, Vergaderjaar 2019-2020, nr. 2020Z12222
[15] Kamerbrief van 18 april 2019, Tweede Kamer, vergaderjaar 2018-2019, 30821, nr. 72
[16] Kamerbrief van 9 juni 2019, Tweede Kamer, Vergaderjaar 2019-2020, 30821, nr. 81
[17] Kamerbrief van 9 juni 2019, Tweede Kamer, Vergaderjaar 2019-2020, 30821, nr. 81
[18] Kamerbrief van 9 juni 2019, Tweede Kamer, Vergaderjaar 2019-2020, 30821, nr. 81
[19] COM(2020) 606 Actieplan drugs
[20] COM (2020) 607 Actieplan vuurwapenhandel

het afpakken van crimineel vermogen centraal staat. Ook acht het kabinet het positief dat het jaarlijkse rapport van de toetsingscyclus voor de rechtsstaat wordt aangehaald bij de aanpak van corruptie en dat in de strategie expliciet de bestrijding van fraude wordt genoemd, in het bijzonder waar het gaat om EU-gelden.

Het kabinet verwelkomt de aandacht in de strategie voor versterking van de capaciteit van de rechtshandhavingsautoriteiten in het digitale domein waar het belang van aanpassing aan en benutten van nieuwe technologieën wordt benadrukt. Daarbij oordeelt het kabinet wel dat een hoger ambitieniveau zou moeten worden nagestreefd waarbij effectieve rechtshandhaving een integraal onderdeel is van de digitale toekomst van de EU. Veiligheid zou horizontaal terug moeten komen in al het EU beleid met een digitale component. Aandacht voor nieuwe samenwerkingen van of verhoudingen tussen de opsporing en private bedrijven is belangrijk. Verder steunt het kabinet het voorstel van de Commissie om technische, operationele en juridische oplossingen voor encryptie te onderzoeken waarbij de effectiviteit van digitale opsporing van misdrijven wordt vergroot en fundamentele rechten wordt gewaarborgd. Voorts is het kabinet voorstander van een bredere aanpak tegen illegale inhoud online.

Wat betreft cyberveiligheid kan het kabinet zich vinden in de benadering van de Commissie van het centraal stellen van de veiligheid en digitale weerbaarheid van vitale infrastructuur, het versterken van EU-coördinatie en aandacht voor afhankelijkheden van infrastructuur en diensten buiten de EU. Daarbij is het van belang dat de samenhang en consistentie voldoende wordt gewaarborgd tussen de verschillende wetgevende initiatieven gericht op het beschermen van de vitale infrastructuur, zoals de generieke wetgeving (bijv. NIB-richtlijn[21], Cybersecurity Act[22] en ECI-Richtlijn[23]) en sectorale wetgeving (bijv. energie, financiële sector). Bij het integreren van de verschillende perspectieven ten aanzien van de dreigingen wil de Commissie ook kijken naar onderwerpen als educatie, technologie en onderzoek (economische en kennisveiligheid). Deze geïntegreerde aanpak vindt het kabinet van belang en steunt dan ook de samenwerking tussen lidstaten in de Raadswerkgroep tegen statelijke dreigingen. Het kabinet wil specifiek inzetten op de versterking van samenwerking en informatie-uitwisseling onder andere via de Hybrid Fusion Cell[24]. Ook is het verbeteren van de samenwerking tussen de EU en de NAVO in de aanpak van hybride dreigingen is voor het kabinet een prioriteit. Voorts is van belang dat de nexus tussen de interne en de externe dimensie van cyberveiligheid voldoende aandacht krijgt; stevige inzet van de cyberdimensie van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (de *Cyber Diplomacy Toolbox*) kan een bijdrage leveren aan de EU-interne veiligheidsdoelstellingen die door middel van de strategie worden nagestreefd. Het kabinet is voorstander van een snelle ontwikkeling van cyberbeveiligingscertificeringsregelingen binnen het kader van de Cybersecurity Act, hiermee wordt ook meer digitale weerbaarheid teweeg gebracht.

[21] EU-Richtlijn 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016
[22] EU-Verordening 2019/881 van het Europees Parlement en de Raad van 17 april 2019
[23] EU-Richtlijn 2008/114/EG van de Raad van 8 December 2008
[24] De EDEO Hybrid Fusion Cell is in 2016 opgezet binnen het EU inlichtingen- en situatiecentrum (IntCen) om publieke en gerubriceerde informatie te analyseren en mogelijke hybride aanvallen te detecteren.

Het kabinet heeft ook enkele aandachtspunten bij de strategie. Zo is het van belang dat EU wetgeving op het gebied van bescherming van vitale infrastructuur en cyberveiligheid geen afbreuk doet aan nationale competenties op het gebied van het beschermen van vitale processen en de praktijk van de rechtshandhaving ondersteunt. Het kabinet heeft vragen bij de plannen omtrent een Joint Cyber Unit over de noodzaak tot een wederzijds bijstandsmechanisme. Voor het kabinet is het essentieel om eerst te bezien in hoeverre bestaande structuren en initiatieven benut kunnen worden.
Voorts wordt in de strategie de ambitie tot uitbreiding van het EOM mandaat met terrorismemisdrijven genoemd. Het kabinet is hier tegen gekant[25]. De bestrijding van terrorisme vraagt volgens het kabinet om een brede aanpak met een goede nationale en lokale aansluiting en aandacht voor preventie. Voor de opsporing en vervolging van terrorismeverdachten is internationale samenwerking cruciaal. Hiervoor zouden reeds bestaande structuren en instrumenten, zoals Europol en Eurojust, volgens het kabinet kunnen worden benut. Tevens vindt het kabinet dat het EOM zich allereerst moet richten op het huidige mandaat gericht op aanpak van fraude met EU-gelden langs strafrechtelijke weg.

Wat betreft de herziening van de Europolverordening streeft het kabinet ernaar dat deze goed aansluit bij de operationele behoeften van de rechtshandhavingsautoriteiten. Het kabinet is terughoudend wat betreft de in de strategie aangekondigde code voor politiële samenwerking en zal daarbij er zorg voor dragen dat bestaande bevoegdheidsverdelingen tussen de EU en de lidstaten niet wordt doorkruist. Een ander aandachtspunt voor het kabinet is de uitwerking van de door de Commissie aangekondigde voorstellen voor een breed crisismanagementsysteem binnen de EU, dat ook relevant zou kunnen zijn op veiligheidsgebied. Tot slot acht het kabinet het voor wat betreft het verbeteren van veiligheidsnormen voor reisdocumenten van belang dat de verordening tot standaardisatie van identiteitskaarten en verblijfsdocumenten[26] eerst wordt geëvalueerd alvorens nieuwe wetgeving wordt overwogen.

c) Eerste inschatting van krachtenveld
Naar verwachting zal een grote meerderheid van de EU-lidstaten de Veiligheidsuniestrategie ondersteunen. In algemene zin onderschrijven alle lidstaten het belang van het waarborgen van interne veiligheid in de EU. Zeker in het licht van de COVID-19 crisis is het belang van een toekomstbestendige veiligheidsomgeving in de lidstaten urgenter geworden. De verwachting is dat lidstaten, net als Nederland, beperkt commentaar en wensen tot aanscherpingen op onderdelen zullen hebben, in lijn met de eigen nationale prioriteiten. Naar verwachting zal de Veiligheidsuniestrategie op steun kunnen rekenen van het Europees Parlement.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen op het gebied van regeldruk en administratieve lasten

[25] Kamerbrief van 19 oktober 2018, Tweede Kamer, Vergaderjaar 2018-2019, 22112, nr. 2707
[26] Verordening (EU) 2019/1157 van het Europees Parlement en de Raad van 20 juni 2019

a) Bevoegdheid

Het kabinet heeft een positieve grondhouding ten aanzien van bevoegdheid van de EU voor wat het onderwerp van deze mededeling betreft. Op het terrein van de ruimte van vrijheid, veiligheid en recht is sprake van een gedeelde bevoegdheid tussen de EU en de lidstaten (artikel 4, lid 2, sub j, VWEU). De voorgestelde strategie omvat overigens slechts de aankondiging van concrete wetgevingsvoorstellen en is dus vooral beleidsmatig van aard.

Wel bevindt een aantal van de aangekondigde plannen en maatregelen zich dicht tegen of op het terrein van nationale veiligheid. Op grond van artikel 4, lid 2, VEU dient de EU de essentiële staatsfuncties, zoals de handhaving van de openbare orde en de bescherming van de nationale veiligheid te eerbiedigen. Met name de nationale veiligheid blijft de uitsluitende verantwoordelijkheid van elke lidstaat. Het kabinet zal er bij komende wetgevingsvoorstellen op toezien dat deze bevoegdheidsverdeling geëerbiedigd blijft.

b) Subsidiariteit

Het kabinet heeft een positieve grondhouding met kanttekening ten aanzien van de subsidiariteit. Gelet op de aard en omvang en het inherent grensoverschrijdende karakter van genoemde dreigingen op het gebied van interne veiligheid, waaronder cybercrime, georganiseerde en ondermijnende criminaliteit, terrorisme en cyberveiligheid, kunnen de gestelde doelstellingen volgens het kabinet beter worden verwezenlijkt op EU-niveau. De kanttekening betreft de ambitie tot uitbreiding van het EOM mandaat met terrorismemisdrijven. Het kabinet is van mening dat de opsporing en vervolging van terrorisme in de EU in de eerste plaats wordt aangepakt in samenwerking op het niveau van de lidstaten.

c) Proportionaliteit

Het kabinet heeft een positieve grondhouding met kanttekening ten aanzien van de proportionaliteit, omdat de meeste maatregelen en plannen die worden aangekondigd de toekomstbestendige veiligheidsomgeving in de EU op een geschikte en evenredige wijze betrachten te waarborgen. De kanttekening betreft de ambitie tot uitbreiding van het EOM mandaat met terrorismemisdrijven. Het kabinet is van mening dat er andere, minder vergaande, alternatieven zijn om de doelstelling die de Commissie hiermee heeft, te bereiken. Waaronder door de samenwerking van EU-lidstaten door middel van informatie-uitwisseling tussen de lidstaten onderling, via en tussen EU-agentschappen (met name Europol en Eurojust) en door middel van EU-informatiesystemen.

d) Financiële gevolgen

Er wordt geen concrete informatie gegeven over de eventueel te verwachten financiële impact op de hoogte van de EU-begroting. Nederland is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van het Meerjarig Financieel Kader (MFK) 2014-2020 en het toekomstige MFK 2021-2027, en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting.

Er wordt geen concrete informatie gegeven over de eventueel te verwachten financiële gevolgen voor de lidstaten. Eventuele budgettaire gevolgen worden ingepast op de begroting van het beleidsverantwoordelijke departement, conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk, administratieve lasten en concurrentiekracht
De mededeling zelf bevat geen nieuwe wettelijke maatregelen en geeft daarmee geen aanleiding om gevolgen te verwachten op regeldruk en administratieve lasten, voor de overheid, bedrijfsleven of burgers.

De uiteindelijke regeldruk en administratieve lasten zijn afhankelijk van de specifieke invulling van de doelen in concrete beleidsmaatregelen. Het is niet uit te sluiten dat zowel de uitvoering van afzonderlijke beleidsmaatregelen als de uitvoering van de beleidsmaatregelen in onderling verband bezien aanleiding geven tot nieuwe regels of verhoging van de uitvoeringslasten. Bij de uitwerking van eventuele maatregelen zal het kabinet zich inspannen om onwenselijke gevolgen voor de regeldruk, administratieve lasten en andere uitvoeringslasten te voorkomen of te mitigeren. Daarbij dient ook rekening gehouden te worden met eventuele gevolgen voor lokale overheden.