Raad van de
Europese Unie

Brussel, 22 november 2019
(OR. en)

14297/19

LIMITE

COSI 239
ENFOPOL 508
ENFOCUSTOM 196
FRONT 333
DAPIX 346
CYBER 322
JAI 1217

NOTA

van:	het voorzitterschap
aan:	het Comité van permanente vertegenwoordigers/de Raad
Betreft:	Hoe het verder moet met de interne veiligheid van de EU - Resultaat besprekingen - Verslag van het voorzitterschap

De snel veranderende veiligheidsomgeving vereist een geïntegreerde aanpak van nieuwe bedreigingen en uitdagingen. Een totaalaanpak van de interne veiligheid is een haalbare manier om bedreigingen die complexer en diverser zijn dan voorheen, aan te pakken en een maatschappijbrede benadering van de tegenmaatregelen mogelijk te maken.

Bij de uitvoering van de strategische agenda 2019-2024 op het gebied van Justitie en Binnenlandse Zaken heeft het voorzitterschap een reeks thematische besprekingen gevoerd om dieper in te gaan op hoe het verder moet met de interne veiligheid van de EU. Het voorzitterschap heeft drie grondbeginselen geformuleerd als leidraad voor dat beraad: aanbieden van een ruimte van vrijheid, veiligheid en recht aan de burgers van de EU; bestrijden van sociale uitsluiting en discriminatie; en bevorderen van de waarden van de Unie.

De besprekingen gingen in juli 2019, tijdens de informele bijeenkomst van het Permanent Comité operationele samenwerking op het gebied van de binnenlandse veiligheid (COSI), ter voorbereiding van de informele zitting van de Raad Justitie en Binnenlandse Zaken (Raad JBZ), van start met het aan de orde stellen van een aantal belangrijke horizontale thema's[1]. In de desbetreffende groepen, zoals de Groep wetshandhaving, de Groep terrorisme en de Groep informatie-uitwisseling, werden ook thematische besprekingen gehouden, die in het COSI verder werden voorbereid met het oog op het ministeriële debat. Een aantal thema's werd in detail besproken, zoals een beter kader voor operationele samenwerking op het gebied van rechtshandhaving, de impact van nieuwe technologieën en hybride bedreigingen op de interne veiligheid, de rol van de JBZ-instanties van de EU, informatiebeheer en automatisering, en opleiding voor rechtshandhavingsinstanties. De details van deze besprekingen zijn opgenomen in de documenten die voor de verschillende vergaderingen zijn opgesteld en in de bijlage bij dit verslag worden opgesomd.

In dit verslag wordt aandacht besteed aan geselecteerde aspecten, die de visie van het voorzitterschap weergeven op de kernpunten die deze debatten hebben opgeleverd en die in de wetgevingscyclus 2019-2024 verder besproken moeten worden.

1. Proactieve benadering van nieuwe technologieën

Technologische ontwikkelingen hebben een grote impact op het leven van de EU-burgers en vervolgens op de rechtshandhaving. Al deze ontwikkelingen, zoals kunstmatige intelligentie, onbemande luchtvaartuigen, nieuwe communicatienetwerken en online-omgevingen, om er maar een paar te noemen, kunnen het werk van de autoriteiten ondersteunen, maar ook voor illegale doeleinden worden aangewend. Zo kunnen bijvoorbeeld rechtshandhavingsinstanties bij terrorismebestrijding en eerstehulpverleners na een terroristische aanslag gebruikmaken van drones. Het steeds hogere innovatietempo stelt de capaciteit van rechtshandhavingsinstanties om zich aan te passen aan de snelle ontwikkeling van de technologische wereld op de proef. In de context van digitalisering moet worden beoordeeld in hoeverre de juridische kaders waarbinnen rechtshandhavingsinstanties en betrokken EU-instanties werken, afgestemd zijn op de huidige behoeften[2]. Dergelijke ontwikkelingen moeten worden geschraagd door de bescherming en bevordering van de grondrechten. Daarbij moeten de strikte vereisten inzake rechtshandhavingsactiviteiten in acht worden genomen die voortvloeien uit het kader voor gegevensbescherming. De Unie heeft immers een voortrekkersrol inzake normering op dit gebied.

---

1 Nota van het voorzitterschap over hoe het verder moet met de interne veiligheid in de EU (doc. WK 13264/19).

2 Doc. 12496/19 en 12224/19, Nieuwe technologieën en interne veiligheid.

Doel is de rechtshandhaving in de EU proactiever te maken om profijt te kunnen trekken van nieuwe technologieën en tegelijk te anticiperen op de daaraan verbonden risico's en die risico's te beheersen. Er is in dit verband behoefte aan een geïntegreerde, alomvattende aanpak op EU-niveau. Dit doel wordt ondersteund met het opzetten van een gezamenlijk innovatielab bij Europol voor het benutten van technologische ontwikkelingen en trends, innovatie en onderzoek, en voor het beoordelen van de relevantie daarvan voor rechtshandhaving en dialoog met de sector en de academische wereld. Volledige exploitatie van nieuwe technologieën vereist voortdurend onderzoek en voortdurende opleiding. Als bepaalde activiteiten bij het innovatielab worden gecentraliseerd en alle resultaten van de werkzaamheden van de bestaande netwerken daar samengebracht worden, zou dat voordelen opleveren in termen van rationalisatie en kostenefficiëntie, vooral op die gebieden waar de lidstaten niet voldoende middelen hebben om alleen te handelen of waar gezamenlijk handelen en uitwisselen van beste praktijken meerwaarde biedt.

Aangezien technologisch onderzoek en technologische ontwikkeling vaak in handen is van universiteiten en de particuliere sector, worden de rechtshandhavingsinstanties daar in een relatief laat stadium bij betrokken. Om tegemoet te komen aan de bezorgdheid voor de toekomst van de rechtshandhavingsinstanties, moet volgens het voorzitterschap gepoogd worden om rechtshandhavingsinstanties van meet af aan proactief te betrekken bij de processen van technologische ontwikkeling, met name door rechtshandhavers meer en op een meer gecoördineerde manier te laten deelnemen aan door de EU gefinancierde programma's voor onderzoek en ontwikkeling op veiligheidsgebied.

Het voorzitterschap moedigt de proactieve betrokkenheid van rechtshandhavingsinstanties bij de ontwikkeling van nieuwe technologieën aan. Het innovatielab moet daarbij als ondersteuningsplatform fungeren. Het is belangrijk dat de behoeften van de rechtshandhavingsinstanties in een vroeg stadium bekend zijn en in acht worden genomen bij de ontwikkeling van nieuwe technologieën die van invloed zijn op hun werk of die nodig zijn voor een efficiëntere respons van de rechtshandhavingsinstanties. Bovendien moet in wetgeving over nieuwe technologieën meer rekening worden gehouden met interneveiligheids- en rechtshandhavingsbelangen om beperkingen in het juridisch kader te ondervangen, met name door er systematisch aandacht aan te besteden in dreigingsevaluaties.

2. Effectief informatiebeheer

Samenwerking inzake rechtshandhaving op EU-niveau zal in toenemende mate gebaseerd zijn op betere en efficiëntere technologische oplossingen en informatiesystemen en de interoperabiliteit daarvan[3]. In een tijdperk van grote hoeveelheden digitale gegevens hebben rechtshandhavings-instanties toegang tot meer gegevens en informatie dan ooit tevoren. De aangeboden technische oplossingen en capaciteit moeten navenant zijn. Tegelijkertijd ontbreken belangrijke statistische gegevens over verschillende criminaliteitsgebieden. Daarom is het van bijzonder belang erop toe te zien dat informatiesystemen van hoogwaardige en volledige gegevens worden voorzien en effectief worden gebruikt. Wij moeten ervoor zorgen dat de bevoegde nationale autoriteiten toegang hebben tot deze systemen en voldoende opgeleid zijn om ze ten volle te kunnen gebruiken.

Criminaliteitsanalyse blijft essentieel bij rechtshandhaving. Analyse geeft meerwaarde aan ruwe gegevens en maakt er actionable informatie van die nationaal en bij grensoverschrijdende operaties in de hele EU kan worden gebruikt. Een broodnodige duidelijke visie op EU-normen voor criminaliteitsanalyse ontbreekt echter. Analyse maakt in ieder geval een integrerend deel uit van alle informatieprocessen bij de rechtshandhaving. Voor het verwerken en analyseren van informatie zijn voldoende menselijke en financiële middelen vereist. Voor een succesvolle verbetering en standaardisering van de analyse is daarom een beter begrip van alle behoeften op het gebied van de rechtshandhaving nodig en met name van de verschillende daarmee verband houdende informatie-processen, waaronder die voor strafrechtelijk onderzoek en het vergaren van criminele inlichtingen.

De interoperabiliteitsverordeningen[4] zijn op 11 juni 2019 in werking getreden. Het is van cruciaal belang dat een efficiënte uitvoering van de verordeningen wordt gewaarborgd. Zowel op EU- als op lidstaatniveau zullen voor deze technologische revolutie van de IT-systemen van de EU veel middelen moeten worden uitgetrokken en moet het tijdpad worden gerespecteerd. Het is belangrijk dat, bij de opbouw van de interoperabiliteitsarchitectuur, in de technische oplossingen steeds rekening wordt gehouden met de behoeften van de eindgebruikers. Voorts is het van cruciaal belang om in passende en voortgezette opleiding voor eindgebruikers te voorzien zodat deze nieuwe informatiesystemen kunnen worden gebruikt en volledig interoperabel gemaakt. Het is duidelijk dat interoperabiliteit veel meer is dan het ontwikkelen van IT-systemen; er is ook een mentaliteits-verandering mee gemoeid. Een succesvolle implementatie vereist daarom tevens een verandering in onze operationele en bestuurscultuur.

---

3 Doc. 13510/19, EU Information management – automation, access to, exchange of, and analysis of information.

4 EU 2019/817 en EU 2019/818.

Op ruimere schaal is betere informatie-uitwisseling niet alleen een technische ontwikkeling. Om de beoogde voordelen te behalen, moet ervoor worden gezorgd dat competenties, middelen en eindgebruikersinterfaces op nationaal niveau doelmatig zijn. Informatie is geen absolute waarde; ze moet bruikbaar zijn en tot actie leiden. Zonder degelijke implementatie kunnen deze ontwikkelingen en de daaraan verbonden voordelen in het gedrang komen.

Naast effectief onderzoek moeten de werkzaamheden van de rechtshandhavingsinstanties evenzeer gericht zijn op het voorkomen en beëindigen van criminaliteit. Doeltreffende, hoogwaardige informatie op het juiste moment op de juiste plaats draagt bij aan dit doel. Wat informatiegestuurde rechtshandhaving betreft, zijn Europol en Frontex uitstekend geplaatst om dit werk te ondersteunen met hun analytische vermogens, onder meer doordat zij ruimere toegang tot het Schengeninformatiesysteem (SIS) hebben, zolang de lidstaten hun systematisch hoogwaardige ruwe gegevens verstrekken.

Het voorzitterschap vraagt om een integraal EU-kader voor informatiebeheer, om ervoor te zorgen dat alle noodzakelijke bestaande informatie snel en efficiënt toegankelijk is en wordt verwerkt en uitgewisseld, zodat informatiegestuurde actie mogelijk is.

3. Multidisciplinaire grensoverschrijdende samenwerking

Nauwere sectoroverschrijdende operationele samenwerking door het beperken van dubbel werk en doeltreffender coördinatie is van cruciaal belang voor een succesvol optreden. Door het steeds veranderende, horizontale karakter van diverse bedreigingen van de veiligheid, zoals CBRN-wapens en hybride activiteiten, is bij de genomen maatregelen in reactie op of ter voorkoming van deze activiteiteneen horizontale aanpak nodig, waarbij rekening moet worden gehouden met de bevoegdheid van de lidstaten op het gebied van de nationale veiligheid. Er moet een geïntegreerde en coherente aanpak komen om te zorgen voor multidisciplinaire operationele samenwerking, die verder gaat dan grensoverschrijdende samenwerking bij rechtshandhaving, zodat ook andere autoriteiten, zoals actoren op het gebied van civiele bescherming, erbij worden betrokken.

Verschillen in nationale besluitvormingsprocessen, wetgeving en werkmodellen zijn grote uitdagingen voor de operationele grensoverschrijdende samenwerking. Voorts staan inconsistenties in de nationale praktijken voor het verzamelen en verwerken van gegevens, voortvloeiend uit de verschillende administratieve systemen, technische oplossingen en functionele regelingen in de afzonderlijke lidstaten, grensoverschrijdende samenwerking in de weg. Een andere opgave is het vaststellen en wegnemen van de belemmeringen voor operationele samenwerking tussen rechtshandhavingsinstanties, zoals het aanpakken van incompatibele radiofrequenties in grensgebieden, taalbarrières en de noodzaak om de bestaande rechtsgronden aan te vullen met meer gedetailleerde bilaterale overeenkomsten. De kans bestaat dat nationale entiteiten in dringende situaties niet weten dat er vele operationele alternatieven – gefragmenteerd over verschillende EU-instrumenten – en beschikbare kanalen voor informatie-uitwisseling zijn.

De multidisciplinaire operationele samenwerking tussen rechtshandhavingsinstanties moet worden geïntensiveerd door de ontwikkeling en het gebruik van nieuwe methoden om samen te werken en informatie uit te wisselen, waarbij men ook zijn toevlucht neemt tot nieuwe technologische toepassingen en tools . Die toepassingen kunnen bijvoorbeeld onbemande autonome systemen, automatische nummerplaatherkenningstechnologie of geïntegreerde zoekinterfaces voor beschikbare databanken zijn. Er is een duidelijke dynamiek en een gunstige gelegenheid om hiermee door te gaan en hieraan verdere steun te verlenen.

Een leven lang leren en opleiding volgen is zelfs nog belangrijker om alle bestaande mogelijkheden te benutten en zich voor te bereiden op toekomstige uitdagingen. De door de EU-instanties verstrekte opleiding moet efficiënt worden aangewend. Tegelijkertijd moet ervoor worden gezorgd dat de activiteiten van de EU-instanties elkaar aanvullen en dat overlappingen worden weggewerkt.

Wij moeten rekening houden met regionale verschillen en nationale specifieke kenmerken, en tegelijkertijd streven naar een gemeenschappelijke rechtshandhavingscultuur bij de rechtshandhavingsinstanties van de EU. Het verbeteren van talenkennis, het ontdekken van elkaars cultuur en het uitwisselen van beste praktijken draagt bij tot een beter begrip van regionale en culturele verschillen en steunt het gemeenschappelijke doel.

Bilaterale en multilaterale regelingen blijven belangrijk voor lokale en regionale samenwerking, en er is flexibiliteit nodig om eerbiediging van de regionale diversiteit en de verschillende operationele belangen te garanderen. In toekomstige ontwikkelingen moet rekening worden gehouden met de verdeling van verantwoordelijkheden, rechtsmacht en soevereiniteit.

De JBZ-instanties van de EU blijven een belangrijke rol spelen bij het ondersteunen van de inspanningen van de lidstaten binnen hun respectieve mandaten. Het is algemeen aanvaard dat echte grensoverschrijdende samenwerking tussen de autoriteiten van de lidstaten, sterk gesteund door de bevoegde EU-instanties, de meest haalbare manier is om tot een Veiligheidsunie te komen en zowel bestaande als nieuwe bedreigingen in een steeds veranderende omgeving duurzaam aan te pakken[5].

Bij toekomstige ontwikkelingen op het gebied van de interne veiligheid moeten de instanties dus een actieve rol blijven spelen, met een verwachte toename van bestaande taken en nieuwe verantwoordelijkheden, welke voortkomen uit zowel politieke als operationele behoeften. Gezien de beperkte middelen moet worden besproken in welke context instanties het best meerwaarde kunnen creëren, bijvoorbeeld wanneer het nodig is dat de lidstaten toegang krijgen tot middelen of technische uitrusting door het bundelen van middelen, wanneer de gegevensanalysecapaciteit kan worden vergroot en wanneer sterkere operationele steun kan worden verstrekt. Er moeten transparante criteria worden vastgesteld om uit te maken op welke gebieden de lidstaten de meeste steun nodig hebben, rekening houdend met technologische ontwikkelingen en specifieke behoeften aan materiële of andere middelen. Bij het ontwikkelen van de rol van de instanties moet worden gestreefd naar een evenwichtige oplossing waarbij rekening wordt gehouden met de behoeften van de lidstaten. Het is van essentieel belang dat een gecoördineerde en holistische benadering wordt gevolgd om de kernexpertise en de sterke punten van elke instantie te verbeteren, en om op kosteneffectieve wijze en zonder overlappingen in taken en functies meerwaarde te creëren.

Er is behoefte aan meer informatie-uitwisseling en samenwerking door de instanties: de bestaande en nieuwe bedreigingen op het gebied van de interne veiligheid worden immers steeds complexer en zijn in toenemende mate grensoverschrijdend. Ook is er behoefte aan effectievere interactie met particuliere partijen waar het gaat om informatiedeling. In het bijzonder is evaluatie nodig van de rechtsgrond voor Europol om persoonsgegevens rechtstreeks van particuliere partijen te vragen en ontvangen[6].

---

5 De rol van de EU-instanties werd specifiek behandeld in de informele vergadering van het COSI en de informele zitting van de Raad in juli (doc. WK 13271/19 en WK 13266/19) en was een horizontaal thema in alle debatten.

6 Er zijn in de Groep wetshandhaving besprekingen gehouden over de samenwerking van Europol met particuliere partijen (doc. 10494/19, 11832/19, 12858/1/19).

Ter versterking van de multidisciplinaire benadering van rechtshandhaving door Europol op lange termijn moet de samenwerking tussen de douaneautoriteiten en Europol worden uitgebouwd door het aantal douaneverbindingsofficieren bij Europol te verhogen, het gebruik van Siena door de douane in alle lidstaten van de EU te bevorderen en de regelmatige en gestructureerde uitwisseling van informatie tussen de partijen, waaronder informatie met betrekking tot risicobeheer en inlichtingen, te verbeteren. Een kortetermijndoel moet zijn dat de douane meer bijdraagt aan en beter geïntegreerd wordt bij de uitvoering van de operationele actieplannen van Empact. Door deze acties zou de positieve ontwikkeling in de samenwerking tussen de douane en Europol van de afgelopen jaren doorgaan.

De uitdagingen bij de samenwerking tussen de Europese Unie en Interpol moeten worden aangegaan. Het is belangrijk dat gegevensbanken die als belangrijkste bron van informatie voor de samenwerking met derde landen op het gebied van rechtshandhaving fungeren, in de toekomst verder effectief worden gebruikt door de autoriteiten van de lidstaten van de EU. Tevens moet uiteraard de toepasselijke wetgeving inzake gegevensbescherming volledig worden nageleefd.

Het voorzitterschap onderstreept dat het juridisch kader voor grensoverschrijdende samenwerking op het gebied van rechtshandhaving en het mandaat van Europol moeten worden herzien en aangepast aan de huidige realiteit en de toekomstige uitdagingen. De ontwikkeling van een gemeenschappelijke rechtshandhavingscultuur onder de rechtshandhavingsinstanties van de EU moet verder worden ondersteund.

4. Totaalaanpak van veiligheid

In de nabije toekomst kan een aantal trends en ontwikkelingen worden verwacht die van invloed zullen zijn op het dreigingslandschap in de EU. Criminaliteit wordt nog steeds bepaald door de vraag en vindt plaats omdat er gelegenheid toe is. Voorts blijven veranderingen op veiligheids-gebied in de naburige regio's en de verschillende vormen van gewelddadige radicalisering in Europa een bedreiging vormen voor onze interne veiligheid. Een totaalaanpak van veiligheid met betere coördinatie, middelen en technologische capaciteiten vereist een beter situationeel bewustzijn en paraatheid voor uiteenlopende uitdagingen.

Rechtshandhavingsinstanties, de civiele bescherming en andere bevoegde instanties moeten doorgaan met hun inspanningen om beter voorbereid te zijn op de bestrijding van hybride bedreigingen. De samenwerking bij het voorkomen en bestrijden van hybride bedreigingen tussen bevoegde nationale autoriteiten, op basis van hun respectieve mandaten, en tussen instellingen, organen en instanties van de EU in de nexus interne-externe veiligheid, moet voortdurend worden verbeterd en steeds meer gemeengoed worden. Tegelijkertijd moet de synergie worden vergroot en moet dubbel werk worden voorkomen, onder meer door horizontale werkmethoden, meer uitwisseling van informatie, en sectoroverstijgende opleiding en oefeningen.

Benadrukt wordt dat de besprekingen over de interne dimensie van hybride bedreigingen moeten worden voortgezet, met name met betrekking tot de rol van de JBZ-instanties bij het vergroten van de vermogens van de EU en de lidstaten om hybride acties en de oorsprong daarvan te identificeren.

Voorts vereist de doeltreffende bestrijding van desinformatie een totaalaanpak. In dit verband moet de deelname van de rechtshandhavingsinstanties, ook aan bestaande EU-mechanismen, zoals het systeem voor vroegtijdige waarschuwing, worden overwogen. De rechtshandhavingsinstanties maken de EU en haar lidstaten weerbaarder, en de bestrijding van desinformatie moet in aanmerking worden genomen[7]. Het voorzitterschap beklemtoont de noodzaak van een beter gebruik van de bestaande instrumenten en van meer holistische coördinatie op EU-niveau. De steun van de JBZ-instanties voor de lidstaten moet in dit verband ook aan bod komen.

Het gebruik van technologie en van het internet bij het organiseren van criminele activiteiten zal blijven toenemen. Zo zal het gebruik van onlineplatforms op zowel het surface web als het darkweb voor de handel in een veelheid aan illegale goederen naar verwachting toenemen. Voorts kan de online-omgeving daadwerkelijk worden misbruikt om te radicaliseren, te werven en aan te zetten tot geweld. De verspreiding van terroristische content en content met kindermisbruik op het internet moet doeltreffend worden voorkomen, en die content moet snel van het internet worden verwijderd.

[7] Hybride bedreigingen en interne veiligheid: Strategische communicatie op het gebied van rechtshandhaving en bestrijding van desinformatie (doc. 11831/19)

Voorts wordt gewezen op de rol van het voorkomen van gewelddadige radicalisering als integrerend deel van een totaalaanpak van terrorismebestrijding. Samenwerken met en ondersteunen van eerstelijnswerkers blijft essentieel voor het voorkomen en aanpakken van gewelddadig extremisme. Politiek of ideologisch gemotiveerd gewelddadig extremisme moet in al zijn vormen worden aangepakt. Voortaan moet de focus op het voorkomen en bestrijden van gewelddadig extremisme en terrorisme gericht blijven, waarbij een brede aanpak wordt gehanteerd die ook oog heeft voor opkomende trends in het gewelddadig extremisme.

De dreiging die uitgaat van gewelddadig rechts-extremisme en terrorisme moet te lijf worden gegaan door middel van een beter situatieoverzicht, het voortdurend delen van goede praktijken, samenwerking met belangrijke derde landen en het tegengaan van de verspreiding van illegale rechts-extremistische inhoud, zowel on- als offline. De uitdaging in verband met terugkerende buitenlandse terroristische strijders moet worden aangegaan, onder meer door een efficiënter gebruik van het SIS.

Het voorzitterschap onderstreept de noodzaak van een integrale, maatschappijbrede benadering van veiligheid om verschillende bedreigingen voor de interne veiligheid aan te pakken. Onderstreept wordt hoe belangrijk het is dat in alle relevante beleidssectoren op een meer strategische, gecoördineerde en coherente wijze te werk wordt gegaan.

BIJLAGE

Subject	Meeting	Reference Number
Future Direction of internal security in the EU	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13264/19
Hybrid threats and internal security	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13265/19
Twenty Years of Europol - what next?	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13266/19
The future of EU Internal Security	Informal Council meeting on 18-19 July 2019, Helsinki	WK 13271/19
The future direction of EU internal security: new technologies and internal security	JHA Council on 2 October 2019	12496/19
Hybrid threats and Internal Security	JHA Council on 2 October 2019	12495/19
Right-wing violent extremism and terrorism	JHA Council on 2 October 2019	12494/19
EU Information Management - Automation, access to, sharing of, and analysis of information	COSI meeting on 19 November 2019	13510/19
The future of EU law enforcement: Training for law enforcement	COSI meeting on 19 November 2019	13973/19