Comité R | I
Toezicht op de inlichtingendiensten

ACTIVITEITENVERSLAG
2025

ACTIVITEITENVERSLAG

2025

Inhoud

Overeenstemmend artikel 35 van de Wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse legt het Comité R/I met voorliggend Activiteitenverslag 2025 verantwoording af over zijn activiteiten.

In dit verslag zet de Comité de belangrijkste activiteiten uiteen die in 2025 werden uitgevoerd, of het nu gaat om toezichtonderzoeken, uitgebrachte adviezen of het werk dat werd verricht door de leden en de griffie van het Beroepsorgaan. Er wordt ook bijzondere aandacht besteed aan de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens die in 2025 door de inlichtingendiensten werden ingezet, alsook aan de wijze waarop hierop toezicht wordt gehouden.

Brussel, 7 april 2026

Frédéric Givron
Griffier

Vanessa Samain
Voorzitster

Séverine Merckx
Franstalig lid

Filip Vanneste
Nederlandstalig lid

VOORWOORD

Eensgezindheid is vaak zeldzaam, maar over één iets lijkt iedereen het wel eens te zijn: het afgelopen jaar werd gekenmerkt door ingrijpende omwentelingen op zowel geopolitiek als maatschappelijk vlak. Sinds de Tweede Wereldoorlog heeft onze maatschappij zelden een dergelijke opeenstapeling van spanningen meegemaakt: gewapende conflicten, desinformatie, democratische achteruitgang... Al deze factoren stellen onze veiligheid duidelijk op de proef, maar daar blijft het niet bij; ze ondermijnen onze instellingen, onze sociale cohesie en het vertrouwen van de burgers in het handelen van de overheid.

Het voorbeeld van andere Europese landen laat zien hoe moeilijk het is om de institutionele onafhankelijkheid te herstellen als die gedurende lange tijd in het gedrang is gebracht. Hoewel het in België nog niet zo ver is gekomen, is ook ons land helaas niet immuun voor deze trend van de verzwakking van de rechtsstaat. Uit een rapport[1] van de Civil Liberties Union for Europe heeft België immers, samen met zes andere landen, de weinig benijdenswaardige status van "*land in verval*" ...

In deze woelige tijden staat of valt de democratische geloofwaardigheid van het werk van de inlichtingen- en veiligheidsdiensten met het bestaan van een sterk toezichthoudend orgaan dat bij machte is zijn rol als onafhankelijke toezichthouder waar te maken. We zijn des te vastberadener deze opdracht te vervullen omdat vertrouwen in de democratie niet zomaar kan worden uitgeroepen. Het moet stap voor stap worden verdiend, met geduld en toewijding, door rigoureus, veeleisend en constant te werk te gaan.

In 2025 ontbrak het zeker niet aan opdrachten. Het Comité R/I kon niet alleen meerdere toezichtonderzoeken afsluiten, maar heeft bovendien op eigen initiatief ook drie nieuwe onderzoeken geopend, waarmee het aantoont vast van plan te zijn om onder alle omstandigheden vooruitgang te boeken.

De analyse van de cijfers bij het toezicht op de bijzondere inlichtingenmethoden (BIM) laat zien dat de trend van de afgelopen jaren zich doorzet: het aantal methoden dat wordt gebruikt door de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) blijft stijgen. De drie uitzonderlijke methoden die door de ADIV het meest werden ingezet, blijven dezelfde als in voorgaande jaren: de militaire inlichtingendienst maakt voornamelijk gebruik van het afluisteren van telefoons, het binnendringen in informaticasystemen en van observaties in niet voor het publiek toegankelijke plaatsen. Voor de VSSE bestaat de overgrote meerderheid van de gebruikte specifieke methoden uit de kennisname van oproep- en lokalisatiegegevens. Alvast een weerkerende vaststelling kan onder de aandacht worden gebracht: de methode van infiltratie (in de reële of virtuele wereld) wordt door beide diensten zelden of nooit gebruikt.

Verder konden twee andere nieuwigheden worden opgetekend in 2025. Naast de uitvoering van zijn gewone opdrachten (toezichtonderzoeken, adviezen verlenen, BIM-controle...) werd het Comité R/I in het kader van een gerechtelijk dossier op verzoek van de Brusselse kamer van inbeschuldigingstelling verzocht om over te gaan tot een diepgaande controle wat betreft de wettelijkheid van de inzet van bijzondere inlichtingenmethoden. Voor het eerst in zijn geschiedenis heeft het Comité in dat kader begin 2025 een prejudicieel advies verleend. Daarnaast werd het Comité ook voor het eerst gevat in zijn hoedanigheid van extern meldingskanaal voor integriteitsschendingen binnen de VSSE en de ADIV. Het Comité was al vooruitgelopen op deze nieuwe wettelijke bevoegdheid met de oprichting van een specifieke cel die hiermee werd belast.

1 Civil Liberties Union for Europe, *Liberties Rule of Law Report 2026*, www.liberties.eu.

We kunnen ook niet voorbijgaan aan de verontrustende situatie van het Beroepsorgaan, waarvan het Comité R/I het voorzitterschap en de griffie waarneemt. In 2025 is het aantal beroepen, als gevolg van de uitbreiding van sectoren waarvoor een veiligheidsadvies of -machtiging vereist is, bijzonder sterk toegenomen. In zijn streven om de beroepsdossiers binnen een redelijke termijn te kunnen afhandelen, heeft het Comité R/I beslist om het aantal zittingen aanzienlijk te verhogen. Gelet echter op het geheel van opdrachten waarmee het Comité is belast en ondanks de goede wil van de vertegenwoordigers van de overige instanties die zetelen in het Beroepsorgaan, stuit deze toename vandaag op haar grenzen. De verdere digitalisering van de griffie, waarmee in 2024 is begonnen, blijft dan ook een prioriteit. Dankzij de blijvende inzet van alle medewerkers van de griffie van het Beroepsorgaan, hopen we dit project in 2026 af te kunnen ronden.

Niettemin, als deze tendens zich voortzet, is er een reëel risico op verzadiging en zal er een onmogelijke keuze moeten worden gemaakt tussen de inachtneming van de redelijke termijnen, de kwaliteit van de beslissingen en de vereisten op het vlak van nationale veiligheid. Bovenal vormt deze evolutie een bedreiging voor de belangrijkste en prioritaire opdracht van het Comité, te weten het toezicht op de inlichtingen- en veiligheidsdiensten.

Tot slot heeft het Comité de noodzakelijke hervormingen nodig om zijn interne werking te verbeteren, ter harte genomen en werden verschillende initiatieven ontplooid.

Het spreekt voor zich dat een ambitieus personeelsbeleid essentieel is als we kwaliteitsvol werk willen leveren om het hoofd te kunnen bieden aan de actuele uitdagingen. Dit jaar is het personeelsbestand van het Comité R/I verder uitgebreid, waardoor vrijwel alle afdelingen versterking kregen. Dankzij deze inspanningen kan het Comité verder op een moderne en professionele wijze werken, onder meer door een auditplan op te stellen dat in 2026 zal worden geïmplementeerd, alsook een strategisch meerjarenplan.

Ook is het na 35 jaar bestaan duidelijk geworden dat de visuele identiteit van het Comité een 'opfrisbeurt' nodig had. Meer dan een puur esthetische operatie, wilden we dat het nieuwe logo de zichtbare uitdrukking zou vormen van de grondige veranderingen en moderniseringen die intern worden doorgevoerd. We zijn dan ook bijzonder trots op het resultaat dat de vrucht is van een lange, collectieve denkoefening maar vooral de weergave van principes als wettelijkheid, integriteit, onafhankelijkheid en transparantie, dewelke richting geven aan het werk van het Comité.

Ter afronding wil ik hier, in wat meer is dan een gebruikelijke paragraaf, mijn oprechte dank uitspreken aan alle leden van het Comité voor hun voortdurende inzet ten dienste van het algemeen belang. Achter de steeds talrijkere en diverse opdrachten van het Comité staan mannen en vrouwen die vastbesloten zijn om bij te dragen aan een Staat die transparanter, rechtvaardiger en veiliger is.

2026 belooft een veeleisend jaar te worden, maar ik ben ervan overtuigd dat we dankzij de kracht van ons team, de helderheid van onze visie en de soliditeit van onze waarden, de uitdagingen die voor ons liggen, aankunnen. Door samen op koers te blijven, zullen we onze bestemming veilig bereiken.

Als enthousiaste voorzitster die trots is op het werk van alle leden van het Comité R/I, wens ik u veel leesgenot bij het lezen van ons Activiteitenverslag 2025.

Vanessa Samain
7 april 2026

TOEZICHTONDERZOEKEN

VINGER AAN DE POLS

1. AFGESLOTEN ONDERZOEKEN

1.1. Bedreigingen tegen in België aanwezige politieke opposanten

In juni 2023, enkele weken na de vrijlating van een Belgische hulpverlener (en nog drie andere Europeanen) die gedurende meer dan één jaar op willekeurige wijze werd(en) opgesloten in Iran, ontstond er controverse rond de toekenning van visa aan een Iraanse delegatie op bezoek in Brussel. België kende visa 'met territoriaal beperkte geldigheid' toe aan veertien Iraanse vertegenwoordigers, onder wie de burgemeester van Teheran, die uitgenodigd waren om deel te nemen aan de *Brussels Urban Summit*, een internationale bijeenkomst van de burgemeesters van grote steden. Onthullingen over de vermeende activiteiten van observatie en spionage ten aanzien van Iraanse opposanten door leden van de betrokken delegatie, wakkerde de politiek-mediatieke controverse verder aan. In deze context vroeg de Begeleidingscommissie van de Comités P en R/I naar de inschatting door het OCAD van de dreiging die de Iraanse delegatie kon vertegenwoordigen. Van dit onderzoek werd een eerste, gemeenschappelijk verslag van de Comités P en R/I opgesteld, waaruit de beperkte betrokkenheid van het OCAD bij dit dossier - enkel bestaand uit een dubbele evaluatie van de dreiging van het evenement en de burgemeester van Teheran - bleek.[1]

Naast dit specifieke voorval verzocht de Begeleidingscommissie om een tweede, ruimer toezichtonderzoek te openen naar de manier waarop het OCAD een evaluatie maakt van de dreiging ten aanzien van opposanten van autoritaire regimes die in ons land verblijven. In dit onderzoek kozen de Comités ervoor om in het bijzonder te kijken naar (1) het wettelijk en reglementair kader waarbinnen het OCAD handelt en de bevoegdheden waarover het (al dan niet) beschikt bij de analyse van 'autoritaire regimes' en hun activiteiten in België en (2) in voorkomend geval, op welke manier het OCAD overgaat tot de analyses en evaluaties van de potentiële dreigingen ten aanzien van opposanten van die regimes. Er werd ook onderzocht hoe relevant de begrippen 'autoritaire regimes' en 'opposanten' zijn, en hoe het OCAD deze begrippen in de praktijk toepast.

De analyse van het wettelijke kader bevestigde dat mogelijke terroristische of extremistische dreigingen tegen "*opposanten van autoritaire regimes die in België aanwezig zijn*" binnen het bevoegdheidsdomein van het Coördinatieorgaan vallen. Het OCAD kan dus punctuele evaluaties en/of strategische analyses uitvoeren over dit thema. In de praktijk bleken de begrippen 'autoritair regime' of 'politiek opposant' echter niet relevant te zijn voor het OCAD. Dit Coördinatieorgaan werkt immers op basis van hypothesen over het - reële of veronderstelde - bestaan van een terroristische en/of extremistische dreiging. Er is geen systematische opvolging (en dus ook geen definitie of operationalisering) van deze categorieën, al kunnen ze incidenteel wel opduiken in evaluaties. Het OCAD kon geen cijfers voorleggen over het aantal evaluatieverzoeken dat het ontvangt met betrekking tot mogelijke dreigingen die verband houden met (opposanten van) een zogenaamd autoritair regime. Volgens het Coördinatieorgaan zijn dergelijke vragen over het algemeen afkomstig van het Nationaal

1 Comité R/I, *Activiteitenverslag 2023*, p. 3 ("De dreigingsevaluatie van het OCAD over een Iraanse delegatie in Brussel"). Parallel daarmee, en ook hier op vraag van de Begeleidingscommissie, opende het Comité R/I een toezichtonderzoek naar de informatiepositie van de inlichtingendiensten (Comité R/I, *Toezichtonderzoek naar de informatiepositie van de inlichtingendiensten en de opvolging die werd verzekerd ter gelegenheid van het bezoek van een Iraanse delegatie aan Brussel van 12 tot 15 juni 2023 voor de Brussels Urban Summit, met inbegrip van de wijze waarop het screeningproces werd gevoerd met het oog op de afgifte van de visa aan de leden van deze delegatie*, www.comiteri.be).

Crisiscentrum en van de Centrale directie van operaties inzake gerechtelijke politie van de Federale Politie.

Naar het voorbeeld van de punctuele dreigingsevaluaties, worden de strategische analyses steeds opgestart op basis van informatie over (potentiële) extremistische en/of terroristische dreigingen in België of tegen Belgische belangen in het buitenland. Sinds 2020 heeft het OCAD verscheidene analyses gewijd aan de terroristische en extremistische dreigingen gelinkt aan het Iraanse regime en dit als gevolg van de poging tot aanslag tegen een bijeenkomst van opposanten van het regime in Teheran in Villepinte (Frankrijk) in 2018 en de aanhouding in België in dat verband van een Belgisch-Iraans koppel. Dergelijke dreigingen worden door het OCAD omschreven als vallend onder een "*aan het buitenland gelinkte context*" of een "*context van politieke oppositie in het buitenland of van interstatelijke dreiging*". Met deze termen omvat het Coördinatieorgaan "*alle actoren en dreigingen die verband houden met buitenlandse conflicten en/of politieke spanningen die een zekere impact hebben in ons land*".[2] De Comités P en R/I stelden echter vragen bij (de reikwijdte van) deze dreigingscategorie, waarvan de benaming varieert van document tot document.

Het onderzoek bevestigde dat de middelen van het OCAD in de allereerste plaats worden gewijd aan de opvolging van de dreigingen in België.

Het onderzoek van de Comités P en R/I vestigde ook de aandacht op de vaagheid die blijft bestaan omtrent de opdracht van het OCAD met betrekking tot een 'statelijke dreiging'. In maart 2022, na de invasie van Oekraïne door Rusland, gaf de Nationale Veiligheidsraad het OCAD de opdracht om dreigingen vanuit Rusland te onderzoeken, ongeacht hun aard ('*all-threat assessment*'). De Comités oordeelden dat een dergelijk mandaat een mogelijke uitbreiding van de bevoegdheden van het OCAD inhoudt, die verduidelijkt en, indien nodig, wettelijk verankerd moet worden.

Aanbevelingen

› De begrippen 'autoritair regime' en 'opposant' definiëren en de categorie 'aan het buitenland gelinkte context' verduidelijken

Hoewel er tijdens het onderzoek geen enkele disfunctie kon worden vastgesteld die in verband kon worden gebracht met het feit dat het OCAD de begrippen 'autoritair regime' of 'opposant' van deze regimes niet heeft gedefinieerd, moedigen de Comités P en R/I niettemin een overleg aan tussen de Belgische partners – bijvoorbeeld in het kader van de Strategie T.E.R. – teneinde deze begrippen nauwkeuriger te bepalen of zelfs te operationaliseren en dat met het oog op een doeltreffende communicatie tussen de diensten. Het gebruik van verschillende uitdrukkingen aangaande de dreigingen die gelinkt zijn aan een buitenlandse context ("*aan het buitenland gelinkte context*", "*context van politieke oppositie in het buitenland*", "*interstatelijke dreiging*") en de onduidelijkheid in de antwoorden van het OCAD over de in de gemeenschappelijke gegevensbank TER (GGB TER) opgenomen

2 OCAD, *Threat Trajectory 2023-2024*, ref. DOC OCAD/D/474035/139, p. 19.

entiteiten, zaaien verwarring over de draagwijdte van deze categorie en de bevoegdheden ter zake van het Coördinatieorgaan. Bijgevolg bevelen de Comités P en R/I aan het OCAD aan om deze analysecategorie te verduidelijken.

› **Werken aan statistische mogelijkheden wat betreft de dreigingen in verband met 'opposanten'**

Het OCAD kon geen statistieken voorleggen over het aantal evaluatieverzoeken dat het ontvangt met betrekking tot dreigingen gelinkt aan (opposanten van) een zogenaamd autoritair regime. De Comités P en R/I moedigen het OCAD aan om zijn inspanningen voort te zetten op het vlak van de verwerking van inkomende en uitgaande informatie met als doel meer nauwkeurige statistieken te kunnen opmaken over (onder andere) de vragen om evaluatie die het coördinatieorgaan ontvangt.

1.2. Kennis van en toezicht op het Cybercommando van de ADIV[3]

Halverwege oktober 2022 heeft het ministerie van Defensie het Cybercommando opgericht. Het werd ingebed in de Algemene Dienst Inlichting en Veiligheid van de Strijdkrachten (ADIV) en is bijgevolg onderworpen aan het toezicht van het Comité R/I. Met het oog op een efficiënte en effectieve uitoefening van dit toezicht, was het voor het Comité van primordiaal belang om dit nieuwe commando in al zijn facetten grondig te leren kennen. De doelstelling om het Cyber Command als onderdeel van ADIV te laten evolueren tot een volwaardige Cybercomponent/Cybermacht (Cyber Force) kan *prima facie* gevolgen hebben voor de uitoefening van de bevoegdheden van het Comité. Deze evolutie riep meerdere fundamentele vragen op, o.m. met betrekking tot de uitoefening van de opdrachten van de ADIV in cyberspace, en was voor het Comité een bijkomende aanleiding om een specifiek toezichtonderzoek naar het Cyber Command te openen.

Uit het onderzoek is gebleken dat de interne zeggenschapsstructuren en de beheerinstrumenten de wettelijke voorziene inbedding van het Cyber Command in de ADIV in de praktijk bevestigen.

De cybercapaciteit van het Cybercommando staat thans in voor de exploitatie van cyberspace ten voordele van de ADIV en van Defensie en biedt in bepaalde gevallen steun aan de Natie. Afhankelijk van haar opdracht, valt de cybercapaciteit onder een verschillend juridisch kader: de Wet houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V) - in dat geval berust de verantwoordelijkheid bij het Cybercommando van de ADIV - dan wel het koninklijk besluit Structuur Defensie en de Wet Aanwending en Paraatstelling Defensie en zijn uitvoeringsbesluit, en in dat geval berust de verantwoordelijkheid bij de Cybermacht. Hoewel vanuit juridisch oogpunt het Cybercommando en de Cybermacht twee afzonderlijke entiteiten zijn binnen de Krijgsmacht, is dit op organisatorisch vlak niet zo. De commandant van het Cybercommando is tevens de

3 Dit onderzoek, dat in december 2025 werd afgesloten, werd begin 2026 voorgesteld aan de Parlementaire Begeleidingscommissie van het Vast Comité van toezicht op de politiediensten en het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten.

commandant van de Cybermacht en er is één organisatie waarbinnen alle personeelsleden, desgevallend, ten dienste (moeten) staan van beide hoedanigheden. Waar de cybercommando opdrachten en -bevoegdheden wettelijk zijn vastgelegd in de W.I&V, is dit niet het geval voor de opdrachten van de Cybermacht. Anderzijds verschillen de gezagslijnen naargelang de cybereenheid optreedt als uitvoeringsorgaan van de ADIV (Chef ADIV) of als Cybermacht (Chef van Defensie). Deze dualiteit in juridische structuur, hoewel begrijpelijk en verantwoord, houdt het risico in op onduidelijkheid bij de uitvoering van de opdrachten en bij de aanwending van bevoegdheden, alsook op discussies omtrent de bevoegdheid van het Comité R/I als toezichtorgaan op de activiteiten van de cybereenheid.

Aanbevelingen

› De specifieke opdrachten van de Cybermacht opnemen in het KB van 30 juni 2025

Het Comité beveelt aan om, net zoals bij het Stafdepartement inlichtingen en veiligheid, de specifieke opdrachten van de Cybermacht, dus de cybereenheid handelend als strijdkracht, in het KB van 30 juni 2025 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en van de bevoegdheden van bepaalde autoriteiten, nader te omschrijven. Meer bepaald beveelt het Comité aan dat de regering, via koninklijk besluit, op concrete wijze de vormen van operationele inzet van de Cybermacht, en desgevallend de vormen van hulpverlening en militaire bijstand, vastlegt.

Het Comité herinnert eraan dat de Cybermacht geenszins belast kan worden, reglementair of operationeel, met het verrichten van inlichtingenactiviteiten zoals bedoeld in artikel 11 W.I&V noch met de uitvoering van de in deze bepaling en in de Classificatiewet omschreven veiligheidsopdrachten. Het Comité brengt hierbij ook onder de aandacht dat activiteiten die onder de wettelijke draagwijdte vallen van de handhaving van de militaire veiligheid (art. 11, §1, 2° W.I&V) of van de bescherming van het militaire geheim (art. 11, §1, 3° W.I&V) niet aan de Cybermacht toegewezen kunnen worden.

› De commandomeeting in de schoot van de ADIV juridisch bestendigen

Binnen de ADIV bestaat de gewoonte om een tweewekelijkse commandomeeting te organiseren tussen de Chef ADIV, de adjunct-chef, de hoofdcommissaris en adjunct hoofdcommissaris, de Cybercommandant alsook de directeurs van alle directies. Deze commandomeeting doet *de facto* dienst als het directiecomité van de ADIV. Het Comité beveelt aan om deze meeting juridisch, in een koninklijk of ministerieel besluit, te bestendigen.[4] Een dergelijke, reglementair ingerichte commandomeeting zou een goede gewoonte juridisch bevestigen en bestendigen. Daarnaast zou het tevens een verplichting creëren in hoofde van de Chef ADIV en de Cybercommandant om formeel overleg te plegen en om zodoende het Cybercommando verder in te kapselen binnen de ADIV.

› Geleverde diensten en producten evalueren

Het Nationaal Strategisch Inlichtingenplan (NSIP) van 2022 voorziet in een versterkte samenwerking op cybervlak tussen de VSSE en de ADIV. Deze stelt dat in het licht van de toename van de voorziene middelen de ADIV ondersteuning biedt aan zijn nationale partners, die zich onder meer vertaalt in het gebruik van vergarings- en analysecapaciteiten van de ADIV ten gunste van de VSSE.

4 Ter vergelijking, het directiecomité van de VSSE en diens samenstelling werd bij koninklijk besluit vastgelegd (art. 4 KB van 5 december 2006 betreffende het algemeen bestuur van de Veiligheid van de Staat).

Tijdens zijn toezichtonderzoek heeft het Comité elementen ontvangen die erop wijzen dat de VSSE vooralsnog weinig gebruik zou maken van de cybercapaciteiten van de ADIV. Het Comité benadrukt dat ze dit niet verder heeft onderzocht, en dus betrokken informatie kan bevestigen noch ontkrachten. Desondanks is het Comité van oordeel dat de ADIV een kwantitatieve en kwalitatieve evaluatie moet maken van de door de eenheid geleverde diensten en producten aan andere instanties, en dit zowel klanten die behoren tot Defensie alsook extern eraan. Gelet op de verwachting van de regering zoals blijkt uit het Nationaal Strategisch Inlichtingenplan dient een verhoogde aandacht te geschieden wat betreft de geleverde diensten en producten aan de VSSE.

› Afdoende budgettaire middelen voorzien voor de Cybereenheid

De actuele geopolitieke situatie noodzaakt tot een verhoogde aandacht voor de militaire cybercapaciteit van België. De beheersmatige en juridische inrichting van het Cybercommando en de Cybermacht vormen hierbij een noodzakelijke eerste stap. Het Comité beveelt aan dat de regering en Defensie afdoende aandacht besteden aan de noodzakelijke middelen van de cybercapaciteit om te kunnen voldoen aan de vele verwachtingen van de politieke en militaire overheden ten aanzien van deze eenheid. Het Comité adviseert hierbij om het budget van vergelijkbare cybereenheden in de lidstaten van de NATO als referentie te hanteren.

› De 'tegenaanval'-bevoegdheid behouden bij ADIV

Tijdens het toezichtonderzoek deelde de ADIV mee dat het een studie ging uitvoeren om na te gaan of de Inlichtingenwet gewijzigd moet worden voor wat betreft de specifieke cyberopdrachten van de ADIV en, in het bijzonder, de zogenaamde 'tegenaanval'- bevoegdheid. Er dient in hoofde van de ADIV en de Cybereenheid te worden bestudeerd of deze bevoegdheid niet dient te worden geschrapt als bevoegdheid van de ADIV (Cybercommando) en deze te laten overhevelen naar de Cybermacht? Het Comité is van oordeel dat, hoewel *prima facie* dit logisch lijkt, dit geenszins het geval is. De bevoegdheid om een tegenaanval uit te voeren na een cyberaanval, is onlosmakelijk verbonden met de inlichtingen- en veiligheidsopdrachten van de ADIV. Daarenboven zou een dergelijke wettelijke overheveling naar de Cybermacht maar mogelijk zijn wanneer Cybermacht als entiteit bij wet wordt ingericht. Het Comité ziet geen reden waarom de Cybermacht bij wet zou worden georganiseerd wanneer de andere strijdkrachten, zoals grondwettelijk voorzien voor wat betreft de organisatie van de Krijgsmacht, bij koninklijk besluit worden ingericht.

Overigens herinnert het Comité eraan dat door de regering de keuze werd genomen om deze bevoegdheid te verbinden met het Cybercommando (zie het verslag aan de Koning bij het KB Structuur Defensie van 30 juni 2025).

› Toewijzing van personeel voor de Cybermacht

Het Comité stelt vast dat de regering heeft besloten om de Cybermacht als aparte strijdkracht in te richten. Tegelijkertijd dient het vast te stellen dat elk militair personeelslid, voor diverse redenen, verbonden wordt met een bepaalde macht en de oprichting van de Cybermacht zich hierin niet vertaalt. Elke militair behoort, voor de toepassing van deze regeling, tot de Landmacht, de Luchtmacht, de Marine, de Medische dienst of tot het burgerpersoneel. Het Comité beveelt aan na te gaan of en zo ja in welke mate er een categorie Cybermacht toegevoegd kan worden voor de werking van vernoemde regelingen.

› De Kamercommissie Opvolging Militaire Missies bevoegd maken om het Comité R/I met toezichtonderzoeken te belasten

Het Comité is bevoegd om ambtshalve een toezichtonderzoek te openen naar de Cybereenheid handelend als Cybermacht. In het verlengde hiervan beveelt het Comité aan om de Kamercommissie Opvolging Militaire Missies, die belast is met het parlementair toezicht op de operationele aspecten van de Krijgsmacht en dus ook op de activiteiten van de militaire cybercapaciteit binnen een militaire operatie, wettelijk bevoegd te maken om het Comité R/I te belasten met een toezichtonderzoek naar de cybercapaciteit handelend als Cybermacht. Binnen het federaal parlement beschikken nu reeds de Begeleidingscommissie en een parlementaire onderzoekscommissie over de bevoegdheid om het Comité R/I met een toezichtonderzoek te belasten.

1.3. Een (betwist) Frans rapport over de Moslimbroeders[5]

In 2021 voerde het Comité R/I op verzoek van de Begeleidingscommissie een toezichtonderzoek naar de opvolging door de inlichtingendiensten van de Moslimbroeders en de eventuele bedreiging die zij in België vormen. De publicatie in mei 2025 van het rapport *"Frères musulmans et islamisme politique en France"*[6] wakkerde het debat over de dreiging van de beweging opnieuw aan. Dit voor België zeer kritische rapport gaf aanleiding tot debatten in de Kamer. De Begeleidingscommissie verzocht daarop het Comité R/I zijn toezichtonderzoek van 2021 te actualiseren en te beoordelen welke vorderingen er werden gemaakt met de aanbevelingen.[7]

Het Comité kon vaststellen dat de VSSE en de ADIV sinds 2024 gezamenlijk toezicht houden op de Moslimbroeders en dit binnen het gemeenschappelijk platform *Counter Extremism & Counter Terrorism* (PFCECT). Het Comité zag dit als een passend antwoord op zijn aanbeveling om de samenwerking tussen de twee diensten op dit gebied te versterken. Het Comité looft ook de gemeenschappelijke definitie van het fenomeen waarover de VSSE, de ADIV en hun veiligheidspartners het eens zijn geworden. Bovendien wordt het fenomeen voortaan structureel gevolgd binnen de Strategie T.E.R., met name in het kader van de Werkgroep Islamitisch Extremisme. Wat betreft de aanbeveling om de autoriteiten, administraties en het publiek meer te sensibiliseren voor deze dreiging, nam het Comité nota van de initiatieven van de VSSE en, in mindere mate de ADIV, om het overleg met de partners te verbeteren via de verspreiding van nota's, de organisatie van veiligheidsbriefings en het houden van coördinatievergaderingen. De VSSE heeft bovendien van meerdere van zijn activiteitenverslagen gebruik gemaakt om het grote publiek te sensibiliseren voor de problematiek van de Moslimbroeders. Het Comité beschikte evenwel niet over informatie betreffende de voortgang van de aanbeveling met betrekking tot de voorafgaande controle van integriteit, loyauteit en discretie bij de toekenning van bepaalde gevoelige functies.

Wat betreft het dreigingsbeeld, schat het PFCECT het aantal individuen die actief deelnemen aan de verspreiding van de ideologie van de Moslimbroeders op een honderdtal en identificeert het enkele tientallen organisaties die nauw aansluiten bij de Moslimbroeders in België. Onder de vastgestelde

5 Dit onderzoek werd in december 2025 afgerond en werd begin 2026 voorgesteld aan de Begeleidingscommissie.

6 Ministère de l'Intérieur, *Frères Musulmans et Islamisme Politique en France* (Moslimbroeders en politiek islamisme in Frankrijk), beschikbaar op de website www.interieur.fgouv.fr.

7 Comité R/I, *Activiteitenverslag 2021*, pp. 63-69 ("Een vernieuwde aandacht voor de Moslimbroederschap").

evoluties wijst het PFCECT op de vermindering van financiering voor de Broederschap, de opkomst van nieuwe, *online* religieuze onderwijsinitiatieven en de terugtrekking van bepaalde actoren naar België als gevolg van de veiligheidsdruk vanwege de Franse autoriteiten.

De inlichtingendiensten oordelen dat de Moslimbroeders tot op heden geen rechtstreekse bedreiging vormen op het vlak van gewelddadige actie in België of tegen Belgische belangen. De diensten zijn echter van mening dat hun ideologie aanzet tot de ontwikkeling van een klimaat van polarisatie. In dit opzicht wordt deze ideologie beschouwd als een mogelijke vector van radicalisering voor bepaalde profielen. De bedreiging die de aanhangers van deze ideologie vormen, moet daarom geval per geval worden beoordeeld. Het PFCECT verwacht dat de bedreiging stabiel zal blijven tijdens de komende vijf jaar. De Moslimbroeders zullen hun ideologie waarschijnlijk blijven verspreiden, zij het op beperkte wijze daar hun financiële inkomsten zijn gedaald.

Het OCAD heeft een andere perceptie van het fenomeen dan het PFCECT dewelke sinds 2021 niet is veranderd: het Coördinatieorgaan identificeert geen directe bedreiging die op korte of lange termijn kan leiden tot een toename van het dreigingsniveau.

Wat betreft de conclusies van het Franse rapport over de aanwezigheid van de Moslimbroederschap in België, komt de analyse van het PFCECT niet helemaal overeen met deze in het Franse rapport: het PFCECT ziet geen aanwijzingen dat islamisten controle zouden uitoefenen in België en acht de invloed van de Moslimbroeders beperkter dan het Franse rapport laat uitschijnen.

2. LOPENDE TOEZICHTONDERZOEKEN

2.1. De analysemethodologie van de VSSE en de ADIV

De VSSE en de ADIV maken dagelijks individuele analyses van de dreiging in het kader waarvan ze kwalificaties toekennen aan individuen. In verschillende stadia van een inlichtingenonderzoek, en om verschillende redenen, kunnen deze analyses het voorwerp uitmaken van externe communicatie met partners en overheidsinstanties. Dergelijke communicatie kan zeer concrete, negatieve gevolgen hebben voor de rechten en vrijheden van burgers, aangezien ze kan leiden tot administratieve beslissingen die een significante weerslag op hen hebben (bijv. de weigering of intrekking van een veiligheidsmachtiging, de weigering van afgifte of intrekking van een verblijfsvergunning, de weigering om de Belgische nationaliteit toe te kennen, de bevriezing van tegoeden, enz.). De analyse van de inlichtingendiensten en de gebruikte kwalificaties worden echter soms betwist door de betrokkenen – met name via klachten die bij het Comité R/I worden ingediend.

Om licht te werpen op wat zich afspeelt achter de schermen van de individuele dreigingsanalyses en op de wijze waarop de resultaten van deze analyses aan derden worden gecommuniceerd, heeft het Comité R/I in 2023 een toezichtonderzoek geopend in verband met de analysemethodologie die de inlichtingen- en veiligheidsdiensten gebruiken om personen te kwalificeren.

Na een onderbreking van meerdere maanden, onder andere als gevolg van de verwerking en afronding van prioritaire dossiers van het Comité, werd het onderzoek in 2025 opnieuw hernomen. Er

werden aanvullende vragen gesteld aan de ADIV en de VSSE en het Comité R/I heeft de diensten ontmoet om bepaalde aspecten van hun methodologie te laten verduidelijken. Er werden ook controles uitgevoerd op het intranet van de VSSE. Via deze onderzoeksdaden heeft het Comité meer bepaald onderzocht over welke instrumenten de medewerkers van de ADIV en de VSSE beschikken om hen te helpen bij de redactie van de analyses alsook welke interne processen voor kwaliteitscontrole er bestaan.[8]

2.2. De analysemethodologie van het OCAD

Parallel met zijn toezichtonderzoek naar de analysemethodologie van de VSSE en de ADIV, startte het Comité R/I een gemeenschappelijk onderzoek met het Comité P om de methodologie te onderzoeken die het OCAD hanteert om de dreigingen te analyseren.

Ook dit onderzoek werd opgeschort omdat andere dossiers voorrang moesten krijgen en werd uiteindelijk opnieuw opgenomen in 2025. Er werden aanvullende vragen gesteld aan het OCAD, dat schriftelijk en tijdens gesprekken heeft geantwoord. De interne documentatie van het OCAD, meer bepaald zijn instrument voor dreigingsevaluatie, werd grondig bestudeerd. In het kader van dit onderzoek hebben de Comités P en R/I bijzondere aandacht besteed aan de risico-indicatoren die het OCAD gebruikt in zijn dreigingsanalyses, aan de inspanningen van het Coördinatieorgaan om zijn personeel vertrouwd te maken met dit instrument alsook aan de intern georganiseerde kwaliteitscontrole.[9]

2.3. (Pogingen tot) synergieën tussen de twee inlichtingendiensten

Onder de tekortkomingen die in de Belgische veiligheidsketen werden vastgesteld door de parlementaire onderzoekscommissie belast met het onderzoek naar de terroristische aanslagen van 22 maart 2016, werden het gebrek aan samenwerking tussen de veiligheidsdiensten en "*het ontbreken van een cultuur van informatiedeling*" met de vinger gewezen. In zijn aanbevelingen besteedde de onderzoekscommissie bijzondere aandacht aan de versterking van de samenwerking tussen beide inlichtingendiensten. Ook het Comité R/I heeft in het kader van zijn toezichtonderzoeken meermaals opgeroepen tot een betere coördinatie tussen de VSSE en de ADIV.

In antwoord op deze vaststellingen en aanbevelingen hebben de ADIV en de VSSE in 2018 een Nationaal Strategisch Inlichtingenplan (NSIP) opgesteld. Het plan werd goedgekeurd door de Nationale Veiligheidsraad (NVR) en een herziene versie werd gepubliceerd in 2022. Het opzet van het Inlichtingenplan is om via nauwere samenwerking de diensten te ondersteunen bij de uitvoering van hun respectieve opdrachten, hun informatiepositie te versterken en de middelen te rationaliseren. Het document organiseert de samenwerking tussen beide diensten in meerdere domeinen, zoals bijvoorbeeld op het vlak van terrorismebestrijding, contraspionage of meer specifiek op het gebied van IT en de organisatie van opleidingen. Naast het NSIP zijn nog andere instrumenten of protocolakkoorden die voorzien in toenadering, of zelfs coördinatie, tussen de VSSE en de ADIV rond specifieke projecten.

8 Een gedeclassificeerde versie van het onderzoeksrapport werd in 2026 aan de Begeleidingscommissie worden voorgesteld.

9 Ook van dit onderzoeksrapport werd in 2026 een gedeclassificeerde synthese aan de Begeleidingscommissie voorgelegd.

In deze context heeft het Comité ervoor geopteerd een toezichtonderzoek te openen om de bestaande en geplande synergieën tussen de twee inlichtingendiensten in kaart te brengen en te beoordelen. Synergieën worden er gedefinieerd als duurzame vormen van samenwerking, *in casu* uitsluitend tussen de VSSE en de ADIV, met als kenmerk het bundelen van middelen (bijv. menselijke, financiële, informatieve of materiële middelen) om de doeltreffendheid vanuit het oogpunt van operaties of ondersteunende functies te verbeteren. Het onderzoek heeft als doel na te gaan in hoeverre de synergieën die in de actieplannen en beleidsdocumenten zijn uiteengezet, daadwerkelijk worden geïmplementeerd en hoe effectief ze zijn.

2.4. Aanval op een politieke opposant in Tienen

Eind augustus 2025 richtte de burgemeester van Tienen een schrijven aan het Comité R/I aangaande de aanval op een Congolese politieke tegenstander van het huidige Congolese regime in zijn gemeente. Zeer snel na de feiten bleek uit een eerste onderzoek in open bronnen dat de betrokkene het voorwerp uitmaakte van een opsporingsbericht vanwege de Congolese autoriteiten. De burgemeester klaagde erover dat hij, in zijn hoedanigheid van bestuurlijke politieautoriteit, door de inlichtingen- en veiligheidsdiensten niet op de hoogte was gesteld van het bestaan van een dreiging tegen een inwoner van zijn gemeente.

Dit individuele dossier sluit aan bij bekende uitdagingen die al in eerdere onderzoeken van het Comité werden onderzocht, meer bepaald in verband met de activiteiten van buitenlandse inlichtingendiensten ten aanzien van hun diaspora in België of deze in verband met de doorgifte van inlichtingen aan derde instanties. Het leek dan ook aangewezen om zich te buigen over een mogelijk disfunctioneren van de inlichtingendiensten alsook het beheer van dit dossier door de VSSE en de ADIV te onderzoeken in het licht van de eerder gedane aanbevelingen.

Het onderzoek van het Comité R/I heeft betrekking op de informatiepositie van de diensten ten aanzien van de dreiging tegen de betrokkene, i.e. de informatie die de VSSE en de ADIV hebben verzameld en de middelen die ze inzetten om dit vergaren van gegevens te versterken. In het onderzoek wordt ook gekeken naar de informatie-uitwisseling tussen de twee inlichtingendiensten en met andere partners.

3. OVERIGE CONTROLEACTIVITEITEN

In april 2025 bracht het Comité een bezoek aan het buitenland om de Belgische bijdrage aan een multinationale informatie-uitwisselingsoperatie inzake terrorismebestrijding te onderzoeken. In april 2025 vonden er ook controlebezoeken plaats met betrekking tot operaties van de ADIV in het Midden-Oosten.

Om redenen van classificatie kunnen de resultaten van deze controles niet worden gedeeld via externe verslaglegging.

INLICHTINGENMETHODEN, ONDERSTEUNINGSMAATREGELEN EN GEGEVENSVERZAMELING IN HET BUITENLAND

DE WETTELIJKE KRIJTLIJNEN VAN GEGEVENSVERZAMELING

De volgende delen zijn gewijd aan het toezicht op de inlichtingenmethoden waaraan het Comité bijzondere aandacht besteedt en waarbij het, wat de bijzondere inlichtingenmethoden (BIM) betreft, optreedt als jurisdictioneel orgaan. Ook wordt gerapporteerd over de ondersteuningsmaatregelen die de inlichtingendiensten kunnen aanwenden ter ondersteuning van hun operaties. Tot slot wordt in een laatste deel ingegaan op buitenlandse intercepties, beeldopnames en IT-intrusies die de ADIV mag uitvoeren.

1. INLICHTINGENMETHODEN

Vooraleer verslag uit te brengen over het aantal (bijzondere) inlichtingenmethoden die de inlichtingendiensten in 2025 hebben ingezet en het toezicht van het Comité R/I op deze methoden, wordt deze manier van verzamelen van inlichtingen kort toegelicht.

1.1. Wat is een inlichtingenmethode?

Om gegevens te verzamelen, kunnen de Belgische inlichtingendiensten drie soorten methoden gebruiken, de zgn. gewone, specifieke en uitzonderlijke methoden. Dit onderscheid, door de wetgever in 2010 ingevoerd, heeft tot doel de methoden in te delen naargelang hun graad van inmenging in het privéleven van burgers: hoe indringender de methode, hoe strenger de procedures en controles op het gebruik ervan.

1.1.1. Gewone methoden

Gewone methoden zijn methoden voor het verzamelen van gegevens waarvoor de wetgever oorspronkelijk geen bijzonder voorafgaand extern toezicht had opgelegd, omdat de inmenging in het privéleven minder ingrijpend werd geacht. Alle methoden die tot deze categorie behoren, vallen dus uitsluitend onder het gewone toezicht van het Comité R/I.

> Het observeren en doorzoeken van publiek toegankelijke plaatsen zonder technische hulpmiddelen (bijv. iemand op straat volgen zonder de betrokkene te filmen) en het werken met menselijke bronnen (informanten) vallen onder deze categorie.

Sinds 2016 werden enkele nieuwe gewone methoden, de zogenaamde gewone methoden ‘plus’, ingevoerd, waarvoor het Comité met een specifiek toezicht belast is en/of waarvoor de betrokken

inlichtingendienst een bijkomende verplichting heeft om informatie aan het Comité te verstrekken. De toezicht- of informatieplicht is voor elk van deze methoden anders geregeld.[10]

Tot deze categorie behoren onder meer:
- Het gebruiken van beelden die zijn opgenomen door de camera's van de politiediensten;
- Het identificeren van de abonnee van een dienst of een telecommunicatiemiddel (bijv. een gsm-nummer of een IP-adres) zonder gebruik te maken van een technisch hulpmiddel, maar via een vordering bij een operator/provider;
- De identificatie van financiële producten of diensten die een bepaalde persoon of onderneming gebruikt, of omgekeerd (bijv. verificatie van de identiteit gekoppeld aan een bekend bankrekeningnummer).

1.1.2. Specifieke en uitzonderlijke methoden

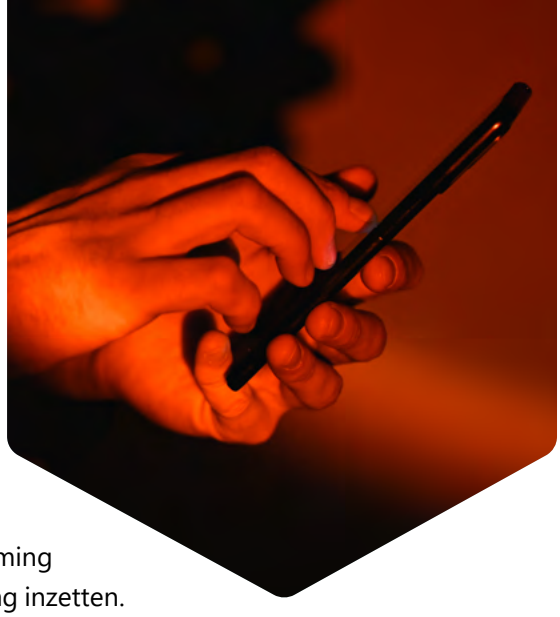
De inlichtingendiensten mogen ook gebruik maken van bijzondere inlichtingenmethoden. Deze methoden omvatten de specifieke en de uitzonderlijke inlichtingenmethoden. Het gebruik van deze methoden moet in overeenstemming zijn met de beginselen van wettelijkheid, proportionaliteit en subsidiariteit. De inlichtingendienst moet aantonen dat de informatie die hij zoekt in het kader van zijn opdrachten, redelijkerwijs niet kan worden verzameld met behulp van een minder indringende methode (zoals een gewone methode). De omvang van de ingezette middelen moet ook in verhouding staan tot het door de dienst ingeschatte dreigingsniveau.

Voorbeelden van specifieke methoden zijn:
- Kennisname van oproep- en lokalisatiegegevens van elektronische communicatie;
- Observeren en doorzoeken van voor het publiek toegankelijke plaatsen met behulp van technische hulpmiddelen (bijv. iemand op straat volgen waarbij foto's of video-opnames worden gemaakt).

Voorbeelden van uitzonderlijke methoden zijn:
- Binnendringen in een informaticasysteem;
- Afluisteren, kennisnemen en opnemen van privécommunicatie;
- Informatie verkrijgen over de transacties, rekeningen en activa van een welbepaalde persoon en de transacties van de betrokkene onder toezicht plaatsen (real-time monitoring).

Gezien hun meer indringende aard zijn bijzondere inlichtingenmethoden onderworpen aan een **dubbel extern toezicht** dat verschilt naargelang het om een specifieke dan wel uitzonderlijke methode gaat.

10 Zie Comité R/I, *Activiteitenverslag 2022*, pp. 84-88.



De bestuurlijke commissie die toezicht houdt op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens (BIM-Commissie), voert een ***a priori* controle** uit op de wettigheid en op de naleving van de beginselen van proportionaliteit en subsidiariteit van elke bijzondere inlichtingenmethode. Zij moet van elke beslissing in verband met de toepassing van een specifieke methode op de hoogte worden gebracht en moet haar uitdrukkelijke toestemming geven voordat een dienst een uitzonderlijke methode mag inzetten.

Het Comité R/I staat vervolgens in voor de ***a posteriori* controle** van deze methoden. Het controleert de wettigheid van beslissingen in verband met deze specifieke en uitzonderlijke methoden én de naleving van de beginselen van proportionaliteit en subsidiariteit.

Het Comité treedt hier op als jurisdictioneel orgaan. Zijn voorafgaand akkoord is niet nodig om een BIM toe te passen, maar wanneer het een onwettig gebruik vaststelt of merkt dat de beginselen van proportionaliteit of subsidiariteit niet werden nageleefd, zet het Comité de betrokken methode stop als die op dat moment nog wordt toegepast. Als gegevensbeschermingsautoriteit gelast het bovendien het verbod op de exploitatie en de vernietiging van de via die methode verkregen gegevens.

1.1.3. Illustratie: van een gewone observatie naar een uitzonderlijke observatie

In onderstaand fictief voorbeeld gebruikt de inlichtingendienst eerst een gewone methode, alvorens over te gaan naar een specifieke en vervolgens een uitzonderlijke methode om de gezochte informatie te verzamelen. In deze casus wordt de aandacht gevestigd op de beginselen van wettigheid, proportionaliteit en subsidiariteit alsook op de versterking van de controle- en traceerbaarheidsmechanismen voor de meer indringende methoden.

Een individu wordt geseind wegens herhaalde contacten met een extremistisch milieu dat een bedreiging kan vormen voor de nationale veiligheid. In het huidige stadium is er geen concreet element dat toelaat het bewijs te leveren van het bestaan van een specifieke dreiging. De dienst zet een **gewone observatiemethode (art. 16/1 W.I&V)** in: discreet toezicht op voor het publiek toegankelijke plaatsen, volgen van verplaatsingen, identificatie van de personen met wie de betrokkene contact heeft. De observatie is beperkt tot wat zichtbaar is in de openbare ruimte en er wordt geen gebruik gemaakt van indringende technische middelen. Concreet betekent dit dat de persoon gevolgd wordt door een of meerdere leden van de dienst en van op afstand wordt geobserveerd. De dienst mag deze methode toepassen zonder de BIM-Commissie of het Comité R/I hiervan op de hoogte te moeten brengen.

Uit de observaties blijkt dat er regelmatig potentieel problematische ontmoetingen plaatsvinden in een bepaald gebouw en dat er sprake is van een ongewoon komen en gaan, vooral ‘s nachts. De dienst wenst deze elementen beter te objectiveren. Als de potentiële

dreiging als voldoende gekenmerkt is en de gewone methoden voor gegevensverzameling ontoereikend worden geacht, maakt de dienst gebruik van een **specifieke observatiemethode (art. 18/4 W.I&V)**. Concreet kan het gaan om de installatie van een camera op straat, gericht op de ingang van het gebouw, om alle komen en gaan op gestructureerde wijze te documenteren. De observatie blijft zich buiten afspelen en is uitsluitend gericht op wat zichtbaar is vanaf de openbare weg, maar is nu gebaseerd op een technisch middel waarmee continu opnames kunnen worden gemaakt. Deze specifieke methode moet worden aangemeld bij de BIM-Commissie voordat ze kan worden uitgevoerd. De Commissie brengt het Comité R/I op de hoogte. Beide toezichthoudende organen kunnen de toepassing van de methode te allen tijde beëindigen als zij van mening zijn dat niet langer aan de voorwaarden van wettigheid, proportionaliteit of subsidiariteit wordt voldaan.

Tot slot blijkt uit de verzamelde informatie dat er in het gebouw zelf mogelijk concrete voorbereidingen aan de gang zijn en dat een gewelddadige actie wordt overwogen. De hierboven beschreven methoden laten niet toe om de precieze aard vast te stellen van de activiteiten die achter gesloten deuren plaatsvinden, en ook andere specifieke methoden zouden dat niet mogelijk maken. Een **uitzonderlijke observatiemethode (art. 18/11 W.I&V)** kan dan worden toegestaan, zoals bijv. de discrete plaatsing van een camera binnen een gebouw dat niet toegankelijk is voor het publiek, en dit met als doel te observeren wat daar gaande is. Deze maatregel impliceert een bijzonder grote inmenging in het privéleven en wordt alleen toegepast als er sprake is van een ernstige potentiële dreiging voor de nationale veiligheid en wordt ingezet binnen een strikt wettelijk kader. Alvorens deze methode kan worden ingezet, is de toelating nodig vanwege de BIM-Commissie. Het Comité voert vervolgens ook een *a posteriori* toezicht uit.

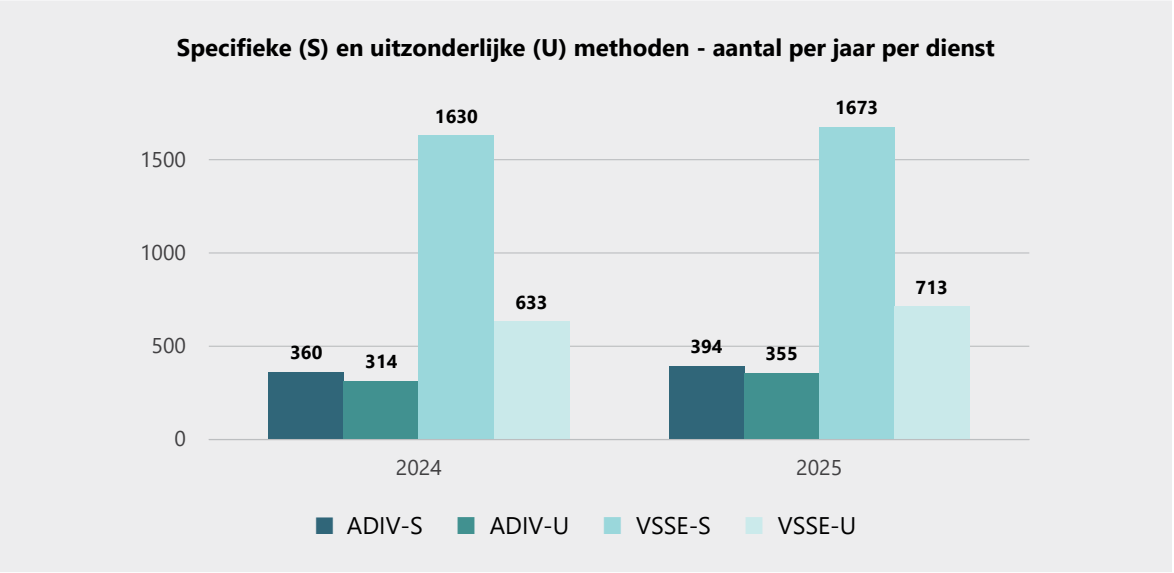
1.2. Cijfers met betrekking tot de bijzondere methoden en bepaalde gewone methoden

1.2.1. Algemene tendensen

Tussen 1 januari en 31 december 2025 werden **3.135 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden** door beide inlichtingendiensten samen: 749 methoden door de ADIV en 2.386 methoden door de VSSE. Dit komt overeen met een **toename van 6,7% tegenover 2024** (toen er 2.937 bijzondere methoden werden aangewend).[11]

11 Om te beschikken over een globaal kwantitatief overzicht telt het Comité het werkelijke aantal methoden waarvan de diensten gebruik hebben gemaakt. Op te merken valt dat de inlichtingendiensten het aantal toegepaste methoden niet op dezelfde wijze berekenen. Er is sprake van BIM-dossiers en een dossier bestaat gewoonlijk uit de toepassing van meerdere methoden (2,25 methoden per dossier in 2025, tegenover 2,19 in 2024). Dit valt meer bepaald te verklaren door het feit dat sommige methoden niet van andere kunnen worden losgemaakt. Afluisteren van telefoongesprekken bijvoorbeeld, wat een uitzonderlijke methode is (art. 18/17 W.I&V), kan niet worden uitgevoerd zonder kennis te nemen van de metadata van de oproepen, wat een specifieke methode is (art. 18/8, §1, 1° W.I&V). Tussen 1 januari en 31 december 2025 werden door de twee inlichtingendiensten samen 1.389 BIM-dossiers opgesteld voor het gebruik van bijzondere inlichtingenmethoden: 1.152 BIM-dossiers door de VSSE (735 dossiers met betrekking tot specifieke methoden en 417 met betrekking tot uitzonderlijke methoden) en 237 BIM-dossiers voor de ADIV (112 dossiers met betrekking tot specifieke methoden en 125 met betrekking tot uitzonderlijke methoden).

Onderstaande grafiek toont de evolutie van het aantal specifieke en uitzonderlijke methoden per dienst van 2024 tot 2025.



Er tekent zich voor beide diensten een afwijkend beeld af. Het aantal BIM's dat de VSSE heeft toegepast is immers aanzienlijk hoger dan dat het geval is voor de ADIV. Deze tendens wordt al vele jaren vastgesteld. In 2024 en 2025 vertegenwoordigde het aandeel BIM's van de VSSE telkens meer dan driekwart van het totaal.

Aangezien de ADIV een groot deel van zijn bevoegdheden uitoefent in een op het buitenland gerichte context en zijn opdrachten op het nationale grondgebied voornamelijk gericht zijn op militaire uitdagingen, is het logisch dat het aantal BIM's waarvan deze dienst gebruik maakt, lager is dan dit het geval is voor de VSSE; deze dienst oefent zijn bevoegdheden voornamelijk in een bredere binnenlandse context uit. In het buitenland kan de ADIV bovendien ook gebruik maken van artikel 44 W.I&V dat betrekking heeft op intercepties, beeldopnamen en IT-intrusies.[12]

Het aantal specifieke en uitzonderlijke methoden dat door de militaire inlichtingendienst werd gebruikt, kende tussen 2024 en 2025 evenwel een toename met circa 10% en dit voor beide types methoden. De ADIV maakt meer gebruik van specifieke dan van uitzonderlijke methoden, maar wel in veel mindere mate dan de VSSE. Deze vaststelling geldt voor zowel 2024 als 2025.

Voor de VSSE laat de groeicurve voor het aantal specifieke methoden die in 2024 en 2025 werden ingezet, een lichte stijging zien (+3%), terwijl de toename voor de uitzonderlijke methoden meer uitgesproken is (+13%). Zoals vermeld (*supra*), blijft het aantal specifieke methoden in 2025 beduidend hoger dan het aantal uitzonderlijke methoden: zo vertegenwoordigen de specifieke methoden doorgaans meer dan 70% van de door de VSSE ingezette BIM's. Ook deze vaststelling werd al gedaan in 2024 en bevestigt de tendens die al meerdere jaren wordt waargenomen.

12 Zie in dit verband *"3. Buitenlandse intercepties, beeldopnamen en IT-intrusies"*.

1.2.2. Door de ADIV gebruikte methoden

Tussen 1 januari en 31 december 2025 werden **749 bijzondere inlichtingenmethoden ingezet door de ADIV**, waarvan 394 specifieke en 355 uitzonderlijke methoden.[13]

Onderstaande tabellen, grafieken en toelichtingen geven een gedetailleerd overzicht van de methoden die de ADIV in de loop van 2025 heeft toegepast en geven een beknopte analyse van hun evolutie ten opzichte van het voorgaande jaar.

Specifieke methoden (ADIV)

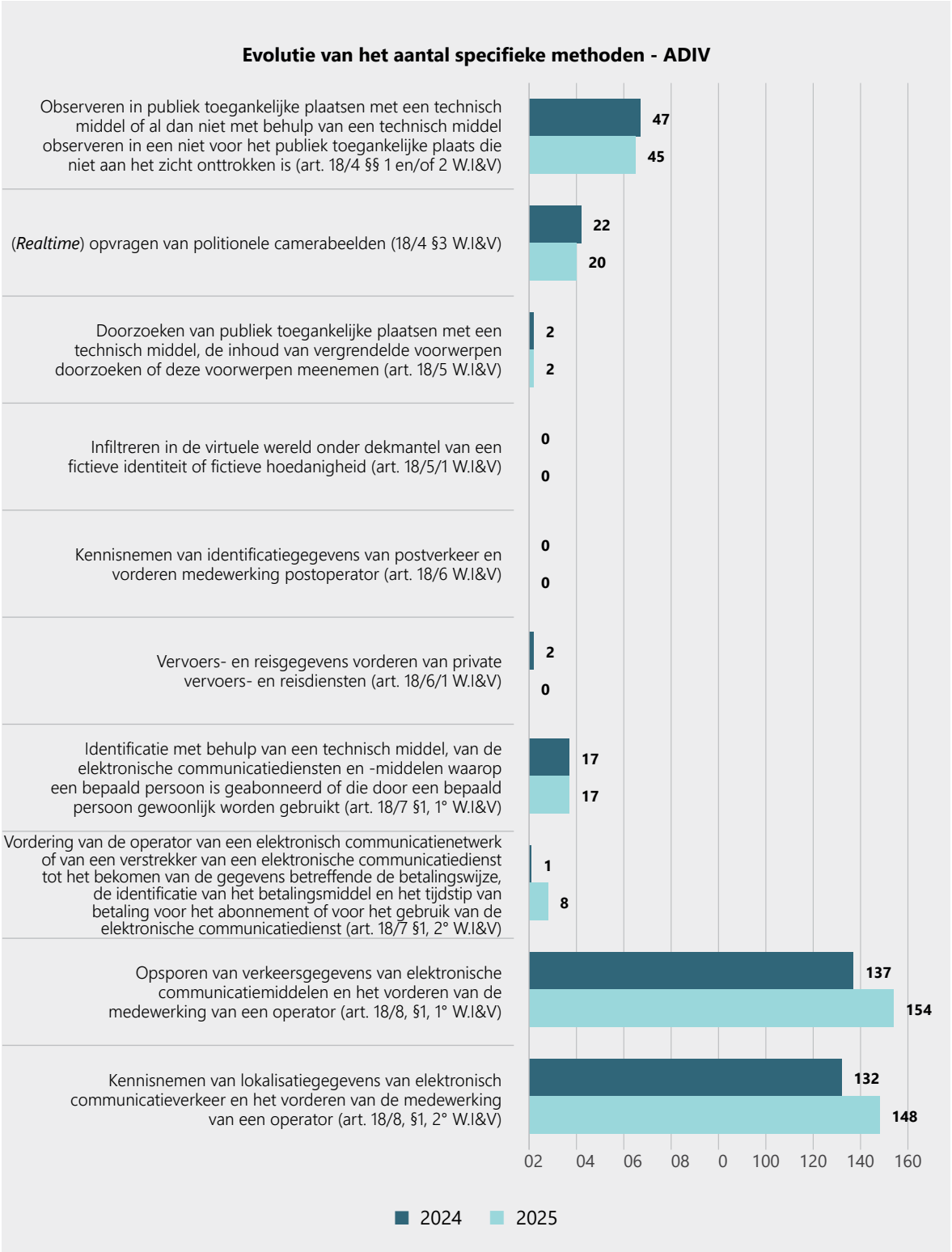
Specifieke methoden (ADIV)	2025
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 §§ 1 en/of 2 W.I&V)	45
Realtime opvragen van politionele camerabeelden (publiek toegankelijke plaatsen) (18/4 §3 W.I&V)	20
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	2
Infiltreren in de virtuele wereld onder dekmantel van een fictieve identiteit of fictieve hoedanigheid (art. 18/5/1 W.I&V)	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	0
Identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt (art. 18/7 §1, 1° W.I&V)	17
Vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 §1, 2° W.I&V)	8
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	154
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator (art. 18/8, §1, 2° W.I&V)	148
TOTAAL	**394**

Het opsporen van verkeersgegevens van elektronische communicatiemiddelen alsook het lokaliseren van de oorsprong of de bestemming van elektronische communicaties (art. 18/8, §1, 1° en 2° W.I&V) blijven de twee meest gebruikte specifieke methoden door de ADIV. Deze methoden worden gewoonlijk samen gebruikt, wat verklaart waarom hun aantallen bijna identiek zijn. Observatie met technische middelen of op een plaats die niet toegankelijk is voor het publiek (art. 18/4 §§1 en/of 2 W.I&V) blijft de derde meest gebruikte methode door de militaire dienst.

Als we deze cijfers vergelijken met die voor 2024, zien we dat het aantal specifieke methoden dat door de militaire inlichtingendienst wordt gebruikt tussen 2024 en 2025 met 9% toeneemt.

13 Voor 237 BIM-dossiers, met gemiddeld 3,2 methoden per dossier.

Onderstaande grafiek illustreert de evolutie van het gebruik van specifieke methoden door de ADIV van 2024 tot 2025. Wanneer hierop dieper wordt ingegaan, blijkt dat de tendensen enigszins verschillend zijn. Uit deze vergelijking blijkt immers dat, hoewel er een toename is van het totale aantal specifieke methoden, het gebruik van bepaalde methoden lichtjes is afgenomen. Dit is meer bepaald het geval voor observaties alsook voor de *realtime* toegang tot politionele camerabeelden. Anderzijds is de toename het grootst voor de twee specifieke methoden die het meest worden gebruikt (kennisname van verkeersgegevens van elektronische communicatiemiddelen en van lokalisatiegegevens (art. 18/8, §1, 1° en 2° W.I&V).



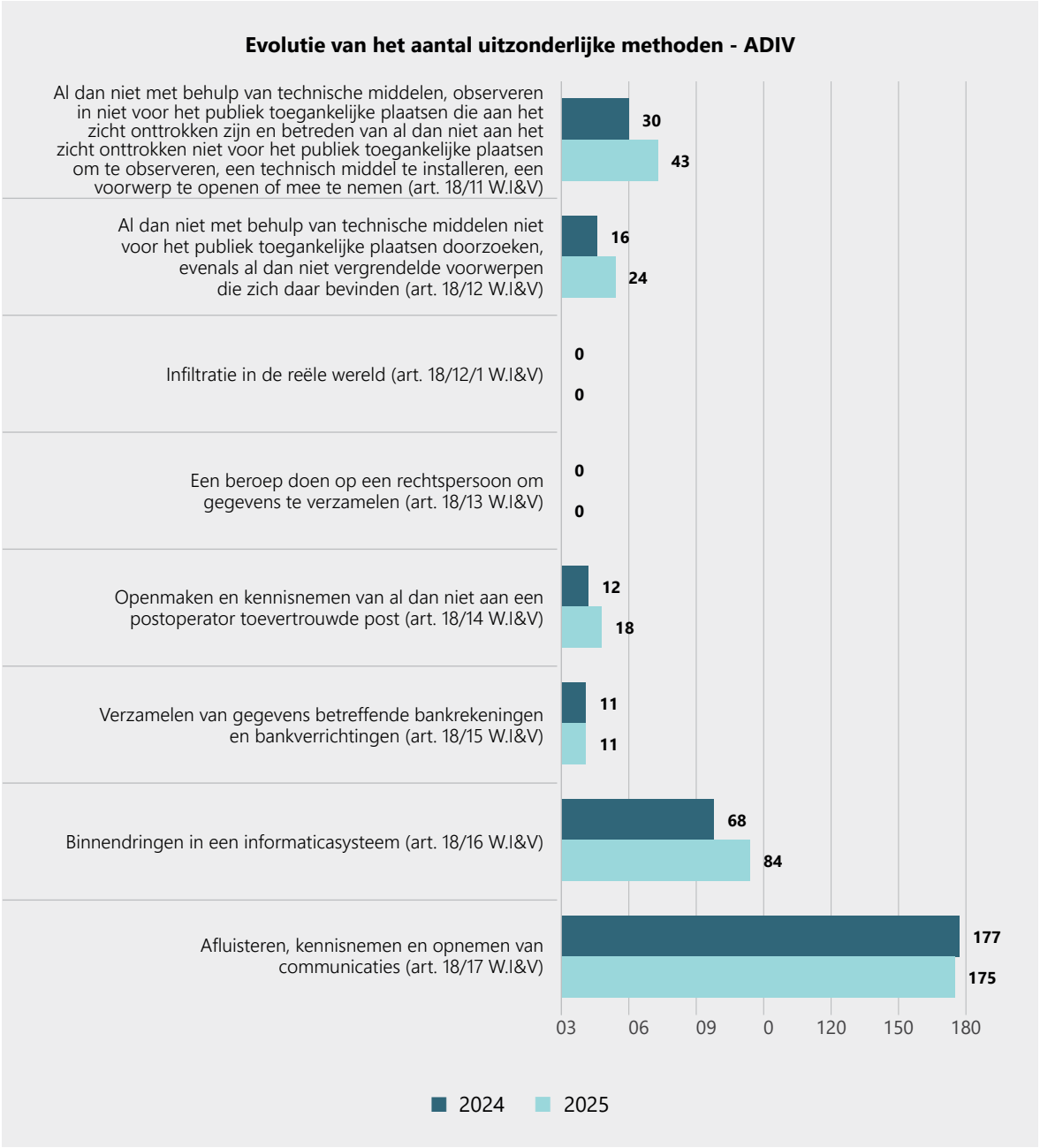
Uitzonderlijke methoden (ADIV)

Uitzonderlijke methoden (ADIV)	2025
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)	43
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	24
Infiltratie in de reële wereld (art. 18/12/1 W.I&V)	0
Een beroep doen op een rechtspersoon om gegevens te verzamelen (art. 18/13 W.I&V)	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	18
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	11
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	84
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	175
TOTAAL	**355**

Afluisteren van communicaties (art. 18/17 W.I&V) was de uitzonderlijke methode die de militaire inlichtingendienst in 2025 het meest heeft gebruikt; deze methode was goed voor bijna de helft van het totale aantal uitzonderlijke methoden. Binnendringen in een informaticasysteem (art. 18/16 W.I&V) en observaties op plaatsen die niet toegankelijk zijn voor het publiek (art. 18/11 W.I&V) staan respectievelijk op de tweede en derde plaats. De vaststellingen hieromtrent sluiten aan bij de algemene tendens van de afgelopen jaren, aangezien deze methoden ook al in 2022, 2023 en 2024 de drie meest gebruikte uitzonderlijke methoden waren die door de militaire dienst werden ingezet.

Onderstaande grafiek illustreert de evolutie van het gebruik van uitzonderlijke methoden door de ADIV van 2024 tot 2025. Uit de vergelijking met de cijfers voor 2024, blijkt dat het aantal uitzonderlijke methoden dat daadwerkelijk door de ADIV werd ingezet in 2025 over het algemeen hoger ligt dan in het voorgaande jaar. Per type methode schommelt de tendens tussen toename en stagnatie. Er is een zeer lichte daling voor het afluisteren van communicaties (art. 18/17 W.I&V). Binnendringingen in informaticasystemen (art. 18/16 W.I&V) laten dan weer de grootste toename in netto cijfers optekenen voor 2025 in vergelijking met 2024.

In 2024 en 2025 maakte de ADIV geen gebruik van infiltratie in de reële wereld noch van infiltratie in de virtuele wereld (dit laatste is een specifieke methode). De dienst heeft ook geen beroep gedaan op een rechtspersoon om gegevens te verzamelen. Dezelfde opmerkingen gelden ook voor de VSSE.



Bedreigingen waarvoor specifieke en uitzonderlijke maatregelen worden ingezet (ADIV)

Net als vorig jaar bleef spionage de dreiging waarvoor de ADIV in 2025 de meeste BIM's heeft ingezet.[14] Er is een toename van BIM's die worden ingezet in het kader van de strijd tegen inmenging. Voor BIM's in verband met de georganiseerde misdaad, die weliswaar minder talrijk zijn, blijkt toch een duidelijke stijging vast te stellen. Het aantal BIM's met betrekking tot extremisme en terrorisme blijft laag. Dit is niet noodzakelijk een verrassing, aangezien de ADIV zich in deze zaken richt op de situatie in het buitenland en gebruik kan maken van artikel 44 W.I&V.[15]

14 Een methode kan voor meerdere bedreigingen worden gebruikt.

15 Zie in dit verband "*3. Buitenlandse intercepties, beeldopnamen en IT-intrusies*".

Gewone methoden 'plus' (ADIV)

De W.I&V voorziet eveneens in gewone methoden waarvoor het Comité R/I met een specifiek toezicht belast is en/of waarvoor de betrokken inlichtingendienst een bijkomende verplichting heeft om informatie aan het Comité te verstrekken (de zogenaamde gewone methoden 'plus').[16] De verplichting inzake toezicht of informatieverstrekking is verschillend gereglementeerd voor elk van deze methoden, ondanks het herhaalde pleidooi van het Comité om deze verplichting te standaardiseren.

De vergelijking met de cijfers voor 2024 toont een toename in het gebruik van deze methoden in 2025.

Gewone methoden 'plus' (ADIV)	2025	2025
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie (art. 16/2 W.I&V)	432	571
Gerichte opzoekingen PNR-gegevens (art. 16/3/1 W.I&V)	7	21
Gebruik politionele camerabeelden (niet in *realtime*) (art. 16/4, §2 W.I&V)	18	22
Vorderen van bepaalde financiële gegevens (art. 16/6 W.I&V)	23	27

Er is een globale toename met ca. 25% voor het gebruik van de identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie (art. 16/2 W.I&V), het gebruik van politionele camerabeelden (niet in *realtime*) (art. 16/4, §2 W.I&V) en het vorderen van bepaalde financiële gegevens (art. 16/6 W.I&V).

Het gebruik van de methode van gerichte opzoekingen van PNR-gegevens (art. 16/3/1 W.I&V) is dan weer verdrievoudigd in 2025. De stijging van de cijfers voor deze laatste methode kan worden verklaard door het gegeven dat er in 2024 een daling van het aantal gerichte opzoekingen van PNR-gegevens werd geregistreerd, en dit volgend op een arrest van het Grondwettelijk Hof van 12 oktober 2023 waarbij artikel 16/3 W.I&V werd vernietigd.[17] Dit arrest verhinderde de VSSE en de ADIV om opzoekingen te doen in de PNR-gegevensbank. Een herstelwet, aangenomen door de wetgever en van kracht geworden op 15 juli 2024, maakte het voor de inlichtingendiensten opnieuw mogelijk om de PNR-gegevensbank te bevragen; dit verklaart dat dit type methode vanaf medio 2024 opnieuw werd gebruikt.

1.2.3. Methoden ingezet door de VSSE

Tussen 1 januari en 31 december 2025 werden **2.386 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden door de VSSE**, waarvan 1.673 specifieke en 713 uitzonderlijke methoden.[18]

16 Zie in dit verband "*1.1. Wat is een inlichtingenmethode?*".

17 In zijn arrest (131/2023) meende het Grondwettelijk Hof dat het toepassingsgebied voor de inlichtingendiensten veel ruimer was dan oorspronkelijk bepaald in de Europese regelgeving en dat het ontbreken van een voorafgaande onafhankelijke controle van de aanvragen vanwege de inlichtingendiensten een schending van de burgerrechten vormde. Om die reden werden verschillende artikelen van de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens geschrapt, evenals artikel 16/3 W.I&V dat dit verzoek om toegang regelde. Tot aan de inwerkingtreding van de herstelwet konden de inlichtingendiensten de PNR-gegevensbank niet meer raadplegen.

18 Voor 1.152 BIM-dossiers, met gemiddeld twee methoden per dossier.

Onderstaande tabellen, grafieken en toelichtingen geven een gedetailleerd overzicht van de methoden die de VSSE in de loop van 2025 heeft toegepast evenals een beknopte analyse van hun evolutie ten opzichte van het voorgaande jaar.

Specifieke methoden (VSSE)

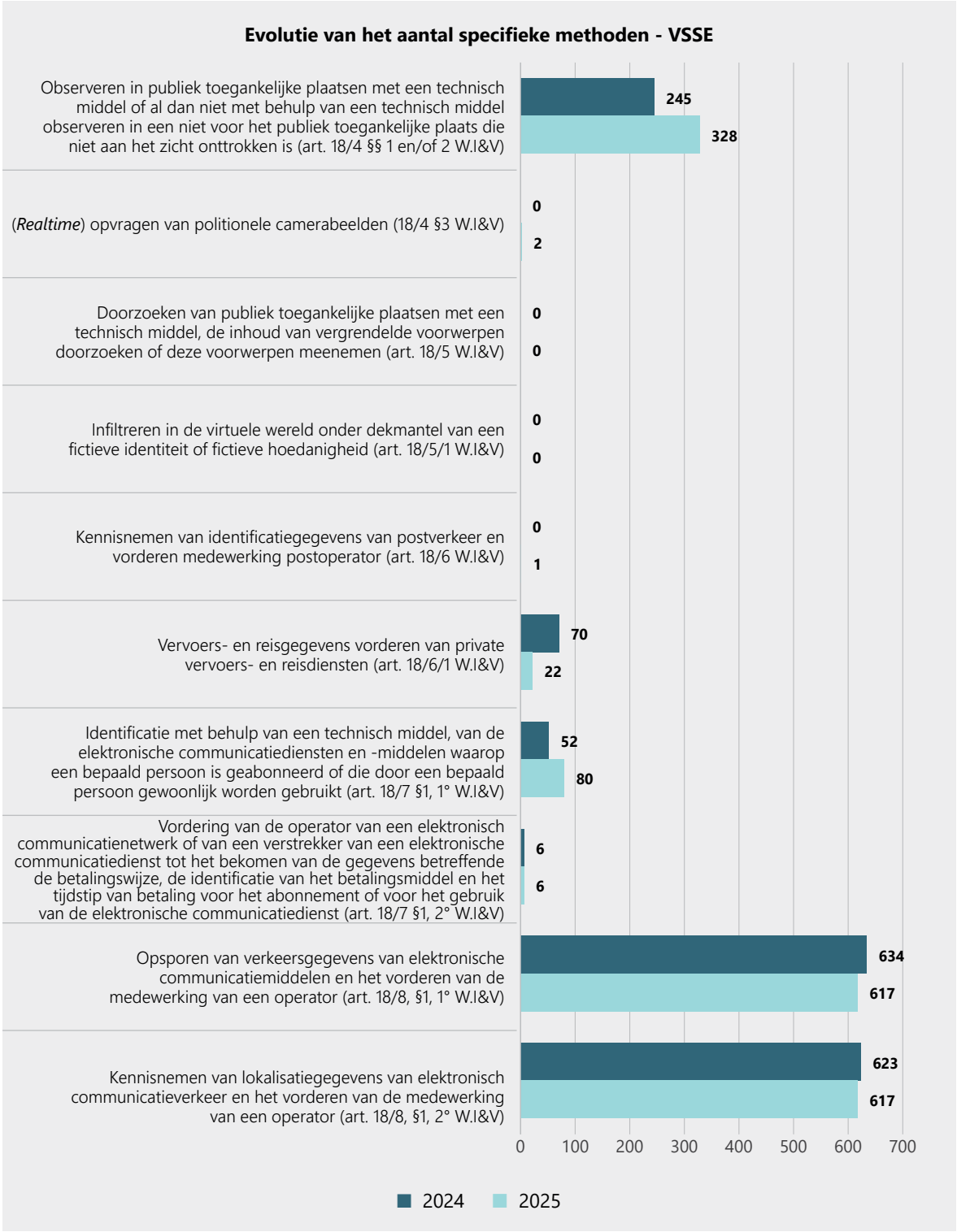
Specifieke methoden (VSSE)	2025
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 §§ 1 en/of 2 W.I&V)	328
Realtime opvragen van politionele camerabeelden (publiek toegankelijke plaatsen) (18/4 §3 W.I&V)	2
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0
Infiltreren in de virtuele wereld onder dekmantel van een fictieve identiteit of fictieve hoedanigheid (art. 18/5/1 W.I&V)	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	1
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	22
Identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt (art. 18/7 §1, 1° W.I&V)	80
Vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 §1, 2° W.I&V)	6
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	617
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator (art. 18/8, §1, 2° W.I&V)	617
TOTAAL	**1.673**

Wat betreft de specifieke methoden die in 2025 het meest werden ingezet, zijn de kennisname van verkeersgegevens van elektronische communicatiemiddelen alsook van de lokalisatiegegevens (art. 18/8, §1, 1° en 2° W.I&V) de twee door de VSSE meest gebruikte specifieke methoden. Samen zijn ze goed voor iets minder dan driekwart van de specifieke methoden die in 2025 door de VSSE werden ingezet. Deze methoden worden gewoonlijk samen gebruikt, wat verklaart waarom hun aantallen identiek zijn. Observatie met technische middelen op plaatsen die toegankelijk zijn voor het publiek (art. 18/4 §§1 en/of 2 W.I&V) blijft de derde meest gebruikte methode door de burgerlijke inlichtingendienst. Deze drie methoden worden ook door de ADIV het meest gebruikt (*cf. supra*).

Als de cijfers worden vergeleken met deze voor 2024, kan worden opgemerkt dat het aantal specifieke methoden dat door de VSSE wordt gebruikt, tussen 2024 en 2025 slechts een lichte stijging kent (+ 43 eenheden, i.e. een toename met iets minder dan 3%). De verdeling per methode weerspiegelt een eerder ongelijke tendens. Het aantal van de twee specifieke methoden die het meest worden gebruikt blijkt in geringe mate te zijn gedaald ten opzichte van 2024. Anderzijds is er een toename merkbaar van het aantal observaties met technische middelen of op een niet voor het publiek toegankelijke plaats

(art. 18/4 §§1 en/of 2 W.I&V), dat in één jaar met 33% is gestegen. Er is dan weer een duidelijke afname voor wat betreft het vorderen van vervoers- en reisgegevens (art. 18/7 §1, 2° W.I&V).

Tot slot valt op te merken dat de VSSE in 2024 noch in 2025 (en ook niet daarvoor) gebruik heeft gemaakt van artikel 18/5 W.I&V, dat voorziet in de mogelijkheid om in geval van een potentiële dreiging die onder de bevoegdheid van de dienst valt, met technische middelen voor het publiek toegankelijke plaatsen te doorzoeken en de inhoud van daar aangetroffen vergrendelde voorwerpen te inspecteren of mee te nemen. De dienst maakte ook geen gebruik van infiltratie in de virtuele wereld (art. 18/5/1 W.I&V). Deze opmerking geldt ook voor de ADIV.



Uitzonderlijke methoden (VSSE)

Uitzonderlijke methoden (VSSE)	2025
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)	22
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	18
Infiltratie in de reële wereld (art. 18/12/1 W.I&V)	0
Een beroep doen op een rechtspersoon om gegevens te verzamelen (art. 18/13 W.I&V)	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	17
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	82
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	101
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	473
TOTAAL	**713**

De meest gebruikte uitzonderlijke methode bestaat erin telefoongesprekken af te luisteren (art. 18/17 W.I&V). Deze methode alleen al is goed voor meer dan de helft van het totale aantal uitzonderlijke methoden die de dienst in 2025 heeft ingezet. Een soortgelijke tendens werd vastgesteld voor de ADIV (*cf. supra*). Daarna volgt binnendringen in een informaticasysteem (art. 18/16 W.I&V), wat ook de tweede meest gebruikte methode is door de militaire inlichtingendienst. Anderzijds blijkt het verzamelen van gegevens over bankrekeningen en -transacties (art. 18/15 W.I&V) een methode die weinig werd gebruikt door de ADIV - ca. tienmaal per jaar - terwijl het de op twee na meest gebruikte methode is door de VSSE in 2025.

Tot slot valt op te merken dat de VSSE, in vergelijking met de ADIV, minder gebruik maakt van observatie- en doorzoekingsmethoden voor plaatsen die niet toegankelijk zijn voor het publiek (artt. 18/11 en 18/12 W.I&V). De uitzonderlijke methode van observatie werd door de VSSE 22 keer ingezet, tegenover 43 keer voor de ADIV. De uitzonderlijke methode van doorzoeken werd in 2025 18 keer gebruikt door de VSSE, terwijl de ADIV deze methode 24 keer hanteerde.

Uit een vergelijking met het aantal uitzonderlijke methoden dat in 2024 door de VSSE werd ingezet, blijkt dat hun aantal tussen 2024 en 2025 met 13% is gestegen (een netto toename van 80 methoden). Onderstaande grafiek toont de evolutie in het gebruik van elke uitzonderlijke methode. Daaruit blijkt dat voor twee van de drie uitzonderlijke methoden die in 2025 het meest werden gebruikt door de dienst, een duidelijke toename valt op te merken tegenover het jaar. Het gaat om het afluisteren van communicatie (art. 18/17 W.I&V) evenals het verzamelen van gegevens betreffende bankrekeningen en -verrichtingen (art. 18/15 W.I&V). Deze twee methoden kennen een aanzienlijke toename tussen 2024 en 2025 (respectievelijk van 380 naar 473 en van 59 naar 82 methoden). Deze tendens werd niet waargenomen bij de ADIV, waar het gebruik van beide methoden stabiel is gebleven (*cf. supra*). Tot slot, terwijl binnendringing in informaticasystemen (art. 18/16 W.I&V) de grootste toename in netto cijfers laat zien voor 2025 in vergelijking met 2024 onder de uitzonderlijke methoden voor de ADIV, is het gebruik van deze methode bij de VSSE licht gedaald tegenover 2024.

Van 2023 tot en met 2025 maakte de VSSE geen gebruik van infiltratie in de reële wereld noch van infiltratie in de virtuele wereld (dit laatste is een specifieke methode). De dienst heeft ook geen beroep gedaan op een rechtspersoon om gegevens te verzamelen. Deze bevindingen werden tevens vastgesteld bij de ADIV.

FOCUS: valse namen en fictieve identiteiten, valse en fictieve hoedanigheden

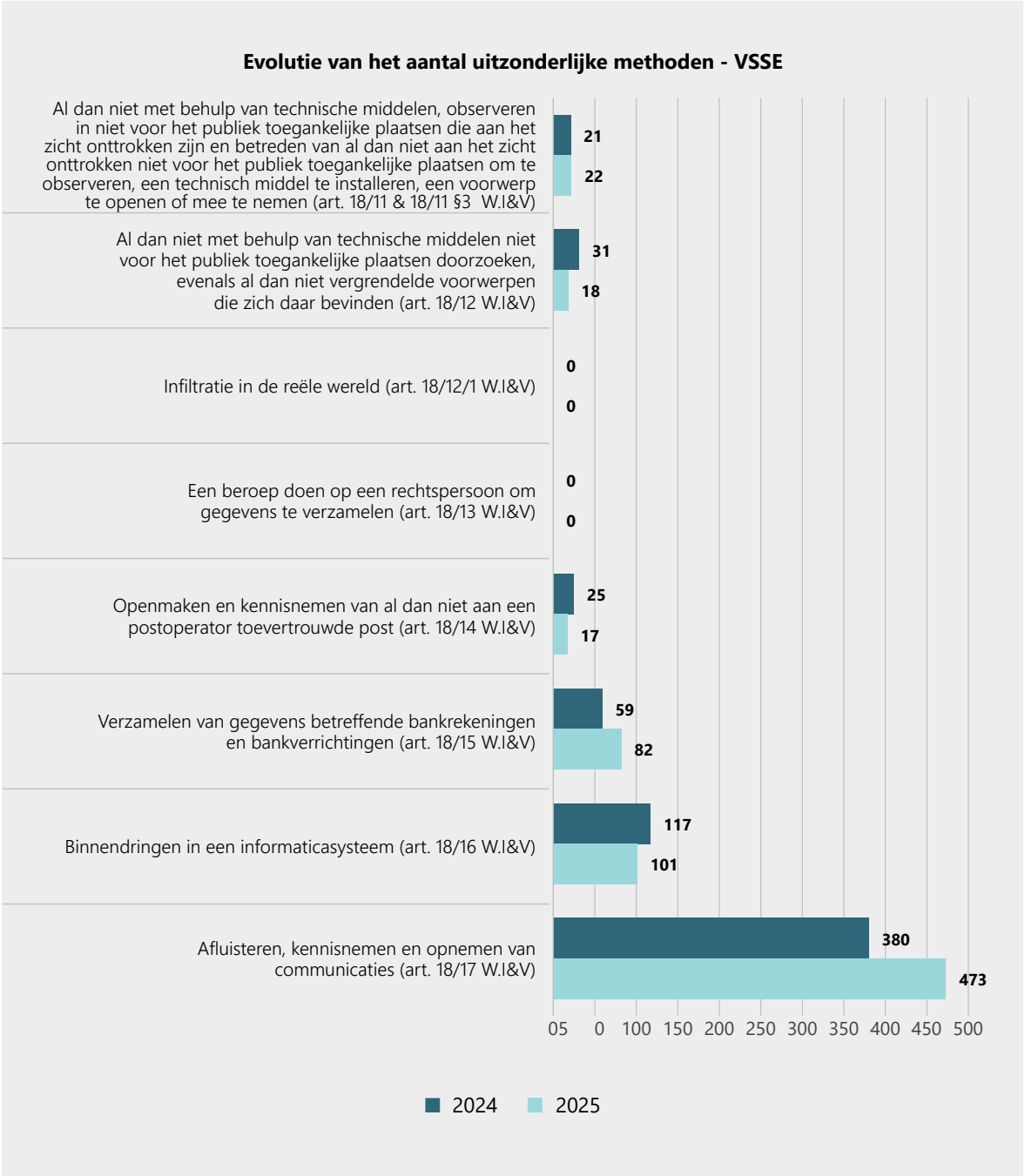
De W.I&V maakt een onderscheid tussen valse namen en fictieve identiteiten. In beide gevallen gaat het erom dat een lid van de inlichtingen- en veiligheidsdienst een naam gebruikt die niet de zijne is.

Het belangrijkste verschil betreft het bewijs van deze naam: een **valse naam** wordt niet ondersteund door de creatie van officiële identiteitspapieren, terwijl een **fictieve identiteit** wordt gestaafd door een identiteitskaart, paspoort, vreemdelingenkaart of verblijfsdocument. De valse naam kan worden ondersteund door documenten (bijv. visitekaartjes, een cv, enz.) die de inlichtingendienst creëert, zolang het niet gaat om officiële documenten die voorkomen op de lijst voor de fictieve identiteit.

Het tweede verschil ligt in het feit dat de valse naam beperkt is tot wat hij is, i.e. een valse naam en voornaam, terwijl de fictieve identiteit een breder concept is dat alle informatie kan omvatten die is opgenomen in de documenten die de bewuste identiteit staven (rijksregisternummer, geboortedatum, nationaliteit, enz.).

De verschillen tussen de valse naam en de fictieve identiteit komen dus overeen met een gradatie in zowel de betrokken informatie, de geloofwaardigheid van de valse informatie als de statelijke middelen die worden gebruikt ter ondersteuning van die geloofwaardigheid.

De W.I&V maakt het voor een lid van een inlichtingendienst ook mogelijk zich te beroepen op hoedanigheden die niet de zijne zijn, zoals een beroep (bijv. diplomaat, hoogleraar, elektricien...), een status (bijv. eigenaar, politiek vluchteling), een titel of een functie. Ook hier is er sprake van een gradatie: indien er rechtsgevolgen voortvloeien uit de hoedanigheid waarop het lid van de inlichtingendiensten zich beroept, gaat het om een **fictieve hoedanigheid**. Als er geen bijzondere rechtsgevolgen voortvloeien uit de hoedanigheid waarop de agent zich beroept, gaat het om een **valse hoedanigheid**.



Bedreigingen waarvoor specifieke en uitzonderlijke maatregelen worden ingezet (VSSE)

Onder de bedreigingen die de civiele inlichtingendienst opvolgt, vormen terrorisme en spionage net als in 2024 het leeuwendeel wat betreft de inzet van bijzondere inlichtingenmethoden. Daarna zijn, in aantallen ingezette BIM's, de bedreigingen van inmenging en extremisme aan de orde. In mindere mate maakt (doch steeds frequenter) maakt de VSSE gebruik van methoden in het kader van de strijd tegen de georganiseerde misdaad.

Gewone methoden 'plus' (VSSE)

Met uitzondering van het gebruik van politionele camerabeelden (niet in *realtime*) dat afneemt, is het gebruik van deze methoden door de VSSE in 2025 aanzienlijk toegenomen. De identificatie van de 'abonnee of gewoonlijke gebruiker' van telecommunicatie (i.e. de identiteit van de persoon die aan de simkaart is gekoppeld) stijgt van 5.543 naar 6.439, verzoeken om bepaalde financiële gegevens blijft stabiel (van 229 naar 330) en gerichte zoekopdrachten naar PNR-gegevens kent een opmerkelijke stijging (van 74 in 2024 naar 207 in 2025). Deze drastische stijging, die eveneens wordt vastgesteld bij de ADIV, is ook hier te verklaren door het feit dat er in 2024 een daling van het aantal gerichte opzoekingen van PNR-gegevens werd geregistreerd volgend op een arrest van het Grondwettelijk Hof van 12 oktober 2023 waarbij artikel 16/3 W.I&V werd vernietigd.[19] Een herstelwet maakte het voor de inlichtingendiensten opnieuw mogelijk om de PNR-gegevensbank te bevragen.

Gewone methoden 'plus' (VSSE)	2025	2025
Identificatie van de "abonnee of de gewoonlijke gebruiker" van telecommunicatie (art. 16/2 W.I&V)	**5.543**	**6.439**
Gerichte opzoekingen PNR-gegevens (art. 16/3/1 W.I&V)	**74**	**207**
Gebruik politionele camerabeelden (niet in *realtime*) (art. 16/4, §2 W.I&V)	**76**	**53**
Vorderen van bepaalde financiële gegevens (art. 16/6 W.I&V)	**229**	**330**

1.3. Toezicht uitgeoefend door het Comité R/I

Voorliggend onderdeel heeft betrekking op het toezicht dat het Comité R/I uitoefent op de bijzondere inlichtingenmethoden (BIM). Alvorens het te hebben over het aantal en de aard van de beslissingen die het Comité R/I in 2025 heeft genomen, wordt de wijze waarop het toezicht op de BIM's wordt uitgeoefend nader beschreven. Daarbij is er in het bijzonder aandacht voor de beschermde beroepen alsook voor het eerste prejudiciële advies dat het Comité in januari 2025 heeft uitgebracht.

1.3.1. Aard van het toezicht

Het toezicht door het Comité is van jurisdictionele aard en heeft betrekking op de wettelijkheid, de proportionaliteit en de subsidiariteit van de specifieke en uitzonderlijke inlichtingenmethoden.

Het Comité moet niet akkoord gaan alvorens er gebruik wordt gemaakt van een BIM, maar kan wel bevelen om een methode niet langer te gebruiken, kan een verbod opleggen om de met behulp van een methode verzamelde gegevens te exploiteren en kan bevelen om deze gegevens te vernietigen indien het onwettigheden of de niet-naleving van het proportionaliteits- of subsidiariteitsbeginsel vaststelt.

Om dit toezicht *a posteriori* uit te oefenen, neemt het Comité kennis van *alle* toelatingen voor inzet van BIM (art. 43/3 W.I&V). Indien tijdens het gevoerde **onderzoek *prima facie*** vermoedens van onregelmatigheden naar voren komen, trekt het Comité het dossier naar zich toe voor een grondigere controle (art. 43/2 W.I&V).

19 Zie hierboven.

Buiten deze vatting op eigen initiatief, kan het Comité op vier andere manieren worden gevat (art. 43/4 W.I&V):

- Op verzoek van de Gegevensbeschermingsautoriteit (GBA);
- Op klacht van een burger;
- Van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
- Van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10, § 3 W.I&V.

Eens het is gevat, kan het Comité meerdere types van beslissingen nemen.[20]

1. Een einde stellen aan de betrokken methode indien ze nog steeds wordt gebruikt of indien ze is geschorst door de BIM-Commissie, en de exploitatie van de via deze methode verzamelde gegevens verbieden en hun vernietiging bevelen (art. 43/6, §1, lid 1, W.I&S);
2. Een gedeeltelijk einde maken aan het gebruik van een toegelaten methode;
3. De door de BIM-Commissie opgelegde schorsing en verbod volledig of gedeeltelijk opheffen (art. 43/6, §1, lid 1, W.I&V). Dit houdt in dat de methode waarvoor de leidinggevende van de dienst toelating heeft verleend, (gedeeltelijk) wordt beschouwd als wettig, proportioneel en subsidiair door het Comité;
4. De onbevoegdheid van het Comité R/I vaststellen;
5. Verklaren dat de aanhangige zaak ongegrond is en het verdere gebruik van de methode toestaan.

Daarnaast kan het Comité ook worden gevat in zijn hoedanigheid van prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* van het Wetboek van Strafvordering (Sv.)). In dat geval brengt het Comité een advies uit over de al dan niet rechtmatigheid van de specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité dan niet op als jurisdictioneel orgaan.

1.3.2. Daling van het aantal vattingen

In 2025 werd het Comité **twaalf keer** gevat. Dit aantal, dat duidelijk is gedaald tegenover 2024 (23 vattingen), is vergelijkbaar met 2023 (13 vattingen).

Alle vattingen zijn het resultaat van een door de BIM-Commissie bevolen schorsing. Dit betekent dat bij de *prima facie* controle van alle toelatingen tot uitvoering van bijzondere methoden, het Comité geen elementen heeft geïdentificeerd die een vatting op eigen initiatief vereisten.

20 Het betreft hier enkel de definitieve beslissingen. Er kunnen meerdere tussentijdse beslissingen worden genomen in het kader van de behandeling van een dossier (bijv. horen van de leden van de BIM-Commissie, aan de inlichtingendienst vragen om bijkomende inlichtingen te verstrekken).

Type vatting	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
1. Op eigen initiatief	16	3	1	1	4	2	1	5	0	0	0
2. Gegevensbeschermings-autoriteit	0	0	0	0	0	0	0	0	0	0	0
3. Klacht	0	1	0	0	0	0	0	0	0	2	0
4. Exploitatieverbod door BIM-commissie	11	19	15	10	12	9	8	9	13	20	12
5. Toelating minister	0	0	0	0	0	0	0	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0	0	0	0	1	0
TOTAAL	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**	**13**	**23**	**12**

Van deze twaalf vattingen hebben er vier betrekking op de ADIV en acht op de VSSE. Meerdere toelatingen hadden betrekking op methoden ten aanzien van dezelfde perso(o)n(en) van belang.

1.3.3. Verboden op exploitatie van illegaal verzamelde gegevens en bevel om ze te vernietigen

Voor alle vattingen in 2025 werd er bevolen om een einde te stellen aan de methode en om de op illegale wijze verzamelde gegevens te vernietigen.

De genomen beslissingen kunnen inhoudelijk worden onderverdeeld in vier categorieën, afhankelijk van het type probleem dat werd vastgesteld:

Toegang tot meer gegevens dan die waarop de methode betrekking heeft

Drie exploitatieverboden waren het gevolg van fouten die leidden tot de verstrekking van te veel gegevens over de beoogde persoon. In twee gevallen was de fout toe te schrijven aan de derde dienst die door de inlichtingendienst werd gevorderd:

- Een inlichtingendienst wilde via een uitzonderlijke methode te weten komen welke applicaties twee doelwitten gebruikten en wat de inhoud was van de uitwisselingen via deze applicaties (*datatap*). De aanvraag had betrekking op drie telefoonnummers. Na het verkrijgen van een eensluidend advies van de BIM-Commissie, werd de methode uitgevoerd via een Belgische externe dienst. De inlichtingendienst stelde echter vast klassieke telefoongesprekken te hebben ontvangen op de drie betrokken telefoonnummers. Die waren echter niet gevorderd; de aanvraag had volgens de operationele keuzes van de betrokken dienst enkel betrekking op de uitwisselingen van *data*. Toen het diensthoofd deze fout ontdekte, bracht hij de BIM-Commissie hiervan op de hoogte. Deze laatste zag zich genoodzaakt een exploitatieverbod uit te spreken wat betreft deze informatie en maakte het dossier aanhangig bij het Comité. Het Comité verklaarde dat de opname van de klassieke telefoongesprekken illegaal was. Het beval dat deze onwettig verkregen informatie niet mocht worden gebruikt alsook om ze te vernietigen.
- Enkele maanden later deed zich een soortgelijk geval voor. Het had betrekking op dezelfde inlichtingendienst die een soortgelijke operatie (*datatap*) wenste uit te voeren op een mobiel telefoonnummer.

› Een inlichtingendienst wilde een uitzonderlijke methode gebruiken om informatie te verkrijgen over bankverrichtingen die gedurende een periode van enkele maanden op een bankrekening waren uitgevoerd. Alleen bepaalde banktransacties waren het doelwit, i.e. transacties die in hun mededeling verwezen naar een welbepaald element. Na een eensluidend advies van de BIM-Commissie te hebben gekregen, deed de dienst een beroep op een operator om de methode uit te voeren. Bij vergissing werd in het aan deze operator gerichte verzoek niet vermeld dat de verrichtingen op basis van de mededeling moesten worden gesorteerd. Hoewel de inlichtingendienst deze fout heeft rechtgezet door een nieuw verzoek toe te sturen, had de dienst ondertussen alle verrichtingen ontvangen die tijdens de beoogde periode op deze bankrekening waren gedaan. Nadat het hoofd van de inlichtingendienst de BIM-Commissie daarvan op de hoogte had gebracht, stelde deze laatste vast dat gegevens op illegale wijze waren verzameld en verbood ze de exploitatie ervan. Het Comité R/I werd gevat door de BIM-Commissie en bevestigde de illegaliteit, verbood de exploitatie van de betrokken gegevens en beval hun vernietiging.

Informatie verzamelen over een persoon die geen doelwit is

Drie andere beslissingen van exploitatieverbod en vernietiging van illegale gegevens houden verband met het feit dat de verzamelde gegevens betrekking hadden op personen die niet het doelwit waren van de inlichtingendienst:

› Een inlichtingendienst wilde specifieke en uitzonderlijke methoden gebruiken om kennis te krijgen van gespreks- en lokalisatiegegevens en van de inhoud van communicatie met betrekking tot een telefoonnummer van een doelwit gedurende een welbepaalde periode. Meerdere maanden nadat deze methoden waren uitgevoerd, stelde de inlichtingendienst vast dat het telefoonnummer waarop de methoden waren uitgevoerd niet het doelwit betrof, maar een andere persoon met dezelfde voor- en achternaam die zich in dezelfde omgeving als het doelwit begaf en bovendien veel gemeenschappelijke kennissen had. Het diensthoofd bracht de BIM-Commissie daarvan op de hoogte en deze laatste kwam tot het besluit dat de informatie die met deze methode was verzameld, illegaal was en niet kon worden gebruikt. Het Comité R/I bevestigde de illegale aard van de gegevens evenals het verbod om ze te exploiteren en beval om ze te vernietigen.

› Een inlichtingendienst had een specifieke methode gelanceerd om gespreks- en lokalisatiegegevens van een mobiel telefoonnummer te verkrijgen. Om de methode uit te voeren, was de medewerking van een telefoonoperator vereist. Nadat er met de uitvoering van de methode was begonnen, gaf de dienst er zich rekenschap van dat de operator een fout had gemaakt en aan de dienst de gevraagde gegevens van een verkeerd telefoonnummer had toegestuurd. De inlichtingendienst bracht de BIM-Commissie op de hoogte van deze fout. Deze verklaarde de verzamelde informatie onwettig, verbood de exploitatie ervan en vatte het Comité R/I. Dit laatste bevestigde dat de verzamelde informatie onwettig was, verbood de exploitatie ervan en beval om ze te vernietigen.

Informatie verzamelen buiten een periode die het voorwerp uitmaakt van een toelating

Vijf beslissingen werden genomen nadat er gegevens betreffende het doelwit waren verzameld buiten de periode waarvoor toelating was verleend:

- Een inlichtingendienst had de intentie om de handelingen van een doelwit te blijven observeren, meer bepaald met behulp van technische middelen. Na het doelwit te hebben geobserveerd met behulp van een specifieke methode, motiveerde de dienst meermaals een verlenging van deze observatie. De opeenvolgende specifieke methoden lieten de dienst echter niet toe om het doelwit gedurende een ononderbroken periode te observeren met technische middelen. Er lagen immers telkens enkele dagen tussen twee observatieperiodes en die dagen werden niet gedekt door een methode. Gedurende drie korte periodes waarvoor geen toelating was verleend, heeft de dienst echter gegevens verzameld met technische middelen. Meerdere maanden na uitvoering van deze observatie heeft de dienst dit incident gemeld aan de BIM-Commissie. Deze laatste stelde de illegale aard vast van de gegevens die werden verzameld tijdens periodes waarvoor geen toelating was gegeven en vaardigde een verbod uit op exploitatie ervan. Het Comité R/I heeft drie beslissingen genomen die deze lezing bevestigen en beval om de betrokken gegevens te vernietigen.
- In het kader van een ander dossier waarbij gebruik werd gemaakt van hetzelfde type observatiemateriaal, werd een soortgelijke fout gemaakt die de betrokken dienst eveneens aan de BIM-Commissie heeft gemeld. Volgend op de beslissing van de BIM-Commissie om een exploitatieverbod uit te vaardigen, verklaarde ook het Comité R/I dat de gegevens die buiten de toegelaten periode waren verzameld illegaal waren, dat ze niet mochten worden geëxploiteerd en moesten worden vernietigd.
- Een inlichtingendienst had een specifieke methode gelanceerd om gespreks- en lokalisatiegegevens van een mobiel telefoonnummer te verkrijgen voor een in de tijd beperkte periode. De operator verstrekte aan de inlichtingendienst echter gegevens voor een langere periode dan de periode zoals vermeld in de toelating. Na hiervan op de hoogte te zijn gebracht door de betrokken inlichtingendienst, nam de BIM-Commissie een beslissing van exploitatieverbod van de gegevens die waren verzameld buiten de periode waarop de toelating betrekking had. Nadat het Comité R/I op zijn beurt was gevat door de BIM-Commissie, bevestigde het de illegale aard van de betrokken gegevens, verbood het de exploitatie ervan en beval het om ze te vernietigen.

Een onevenredige maatregel

- Een inlichtingendienst wilde een observatiemethode ten aanzien van een voertuig verlengen. Op basis van de inlichtingen die de dienst eerder had verzameld, bleek echter dat het voertuig niet langer werd gebruikt door de persoon tegen wie de maatregel was gericht. Bijgevolg concludeerde de BIM-Commissie dat de beslissing van het diensthoofd niet toeliet de noodzaak van de specifieke methode te rechtvaardigen; ze meende dat zowel de feitelijke omstandigheden als de motivering in termen van subsidiariteit en proportionaliteit ontoereikend waren. De BIM-Commissie beval de schorsing van de betrokken methode en verbood de exploitatie van de verzamelde gegevens. Nadat het Comité R/I op zijn beurt was gevat, bevestigde het de onwettige aard van de maatregel, verbood het de exploitatie van de via deze maatregel verzamelde gegevens en beval het om deze gegevens te vernietigen.

1.3.4. Specifieke aandacht van het Comité voor bepaalde profielen

Beschermde beroepen

De W.I&V bepaalt dat wanneer een BIM gericht is tegen een advocaat, een arts of een journalist, ze alleen mag worden toegestaan indien ze strikt noodzakelijk is om de wettelijke opdrachten van de diensten te vervullen en geen enkele minder indringende maatregel mogelijk is. De toelating is onderworpen aan een strengere procedure en specifiek toezicht. Bovendien mag informatie die onder het beroepsgeheim of de bronbescherming valt, alleen worden geëxploiteerd voor zover dit strikt relevant is voor de betrokken dreiging, teneinde de gevolgen voor de grondrechten te beperken.

In 2025 werden slechts in een zeer beperkt aantal gevallen BIM's ingezet tegen beroepen die bijzondere bescherming genieten. In het kader van zijn controleopdracht heeft het Comité de nodige verificaties verricht en vastgesteld dat er was voldaan aan de garanties en voorwaarden waarin de wet voorziet.

Andere hoedanigheden: politieke mandatarissen en diplomaten

De W.I&V voorziet voor politieke mandatarissen noch voor diplomaten in een specifieke beschermingsregeling die vergelijkbaar is met de regeling die bestaat voor advocaten, artsen of journalisten. Gelet echter op de specifieke aard van hun functies en hun maatschappelijke rol, is het noodzakelijk om bijzondere aandacht te hebben voor hun eventuele betrokkenheid wanneer BIM's worden ingezet, teneinde de draagwijdte en gevolgen ervan met de nodige omzichtigheid te beoordelen.

In 2025 werden slechts in een beperkt aantal gevallen BIM's ingezet tegen politieke mandatarissen en diplomaten. Het Comité heeft zijn klassieke controleopdracht uitgevoerd en vastgesteld dat er was voldaan aan de garanties en voorwaarden waarin de wet voorziet.

1.3.5. Een eerste prejudicieel advies verleend in januari 2025

In 2024 werd het Comité R/I voor het eerst in zijn bestaan gevat met een verzoek om een prejudicieel advies uit te brengen betreffende de legaliteit van specifieke en uitzonderlijke methoden waarvan de verzamelde gegevens werden gebruikt in het kader van een strafzaak.[21] Het Comité bracht zijn advies uit in januari 2025. Het verloop van het onderzoek evenals een beschouwing over een aantal vragen die tijdens de controle zijn gerezen, worden hierna samengevat.

21 Los van de verschillende manieren waarop het Comité kan worden gevat om een controle *a posteriori* te voeren met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden (zie in dit verband punt "*1.3.1 Aard van het toezicht*"), kan het Comité ook worden gevat in zijn hoedanigheid van "prejudicieel adviesverlener" (artt. 131*bis*, 189*quater* en 279*bis* Sv.). Desgevallend brengt het Comité een advies uit over de legaliteit van de specifieke of uitzonderlijke methoden waarvan de verzamelde gegevens worden gebruikt in het kader van een strafrechtelijke zaak. Adviesaanvragen worden ingediend door de onderzoeksgerechten of de strafrechters.

Onderzoek van het dossier en advies van het Comité

Het verzoek werd geformuleerd voor de Kamer van Inbeschuldigingstelling van het hof van beroep van Brussel door een inverdenkinggestelde die een controle *a priori* wenste van de regelmatigheid van de tegen hem ingestelde procedure.

Overwegende dat een gecombineerde lezing van de artikelen 235*bis* en 131*bis* van het Wetboek van Strafvordering (Sv.) toelaat om aan het Comité te vragen advies uit te brengen bij de controle van de regelmatigheid van de procedure, en dit nog vóór de fase van de regeling van de rechtspleging, vroeg de Kamer van Inbeschuldigingstelling in zijn arrest van 24 september 2024 aan het Comité R/I om zich uit te spreken over de door de VSSE toegepaste specifieke en uitzonderlijke methoden.

In de bewuste zaak had de VSSE een significant aantal specifieke methoden van gegevensverzameling ingezet vooraleer de BIM-Commissie op de hoogte te brengen van het bestaan van strafbare feiten die vervolgens het voorwerp hebben uitgemaakt van een gedeclassificeerd proces-verbaal op basis van artikel 19/1 W.I&V.

Na onderzoek van het dossier kwam het Comité tot het besluit dat de betrokken bijzondere inlichtingenmethoden waren beslist en uitgevoerd in overeenstemming met de wet.[22]

Dit dossier heeft het Comité R/I ook de kans geboden zich uit te spreken over een aantal vragen (hierna samengevat) met betrekking tot de draagwijdte van zijn vatting evenals de samenloop tussen een strafrechtelijk en een inlichtingenonderzoek.

Draagwijdte van de vatting van het Comité

Tijdens het onderzoek stelde het Comité vast dat de draagwijdte van zijn vatting verschillend is naargelang het wordt gevat met een controle *a posteriori* op basis van de artikelen 43/2 en volgende W.I&V (bijv. ter gelegenheid van een klacht) dan wel met een prejudicieel advies op basis van het Wetboek van Strafvordering (Sv).

Op basis van artikel 43/2 W.I&V en volgende, heeft deze controle van het Comité R/I betrekking op de wettigheid, de proportionaliteit en de subsidiariteit van de specifieke en uitzonderlijke methoden van gegevensverzameling waarvan de inlichtingen- en veiligheidsdiensten gebruik maken tegen een persoon die een persoonlijk belang aantoont. In dit geval onderzoekt het Comité de bijzondere methoden die beide diensten hebben gebruikt en specifiek op de betrokkene waren gericht of die, zonder dat de methoden gericht waren tegen deze laatste, het mogelijk hebben gemaakt om persoonsgegevens over de betrokkene rechtstreeks te verzamelen. Met 'rechtstreeks verza-

22 Tijdens het onderzoek van het dossier heeft de VSSE geantwoord op alle vragen van het Comité en werden alle noodzakelijke documenten overgemaakt.

melen' wordt elke situatie bedoeld waarin de betrokkene zelf aan de oorsprong ligt van de gegevens die in verband met deze persoon worden verzameld bij de toepassing van de methode. Met andere woorden, 'rechtstreeks verzamelen' is het verzamelen waarbij de betrokkene zelf rechtstreeks informatie verstrekt, openbaar maakt of meedeelt en die door de inlichtingendienst wordt verzameld. Het gaat dus niet om situaties waarin gegevens over de betrokkene worden verzameld bij een derde.

Bij de prejudiciële evaluatie is de draagwijdte van de vatting algemener aangezien het gaat om alle bijzondere methoden van gegevensverzameling die werden toegepast en hebben geleid tot de mededeling van een gedeclassificeerd proces-verbaal van de BIM-Commissie op basis van artikel 19/1 W.I&V.

Dit verschil heeft als gevolg dat voor eenzelfde inlichtingenonderzoek de draagwijdte van de controle door het Comité niet noodzakelijk dezelfde is naargelang het wordt gevat door een klacht of een verzoek om een prejudicieel advies uit te brengen.

Samenloop van een strafrechtelijk en een inlichtingenonderzoek

Het Comité bevestigde dat de inlichtingen- en veiligheidsdiensten een inlichtingenonderzoek parallel mogen voeren met een strafrechtelijk onderzoek uitgevoerd door de gerechtelijke overheden.

Hoewel de inlichtingen- en veiligheidsdiensten verplicht zijn om aan de BIM-Commissie te rapporteren wanneer ze kennis krijgen van bepaalde aanwijzingen van strafbare feiten, blijft het doel van een onderzoek door een inlichtingendienst het verzamelen van informatie dat verband houdt met de wettelijke opdrachten van de inlichtingen- en veiligheidsdiensten.

De artikelen 13/5 en 19/1 W.I&V bevatten bepalingen over de interactie tussen een inlichtingenonderzoek en een strafrechtelijk onderzoek. Artikel 13/5 W.I&V kan niet aldus worden geïnterpreteerd dat een strafrechtelijk onderzoek voorrang heeft op een inlichtingenonderzoek of dat het gelijktijdig verrichten van deze twee soorten onderzoek verboden is. Integendeel, dit artikel laat talrijke hypothesen toe waarin een inlichtingenonderzoek parallel met een strafrechtelijk onderzoek wordt voortgezet.

Artikel 19/1 W.I&V biedt ook een kader voor de gevolgen van een aangifte van bepaalde aanwijzingen of feiten door de inlichtingen- en veiligheidsdiensten bij de BIM-Commissie. De gevolgen met betrekking tot de bewijskracht van een gedeclassificeerd proces-verbaal moeten worden beoordeeld door de strafrechter en niet door het Comité.

Het Comité kan nagaan of de inlichtingen- en veiligheidsdiensten deze twee artikelen wel degelijk in acht hebben genomen. Het Comité is echter niet bevoegd om toezicht te houden op het werk van de BIM-Commissie, waarvan de onafhankelijkheid bij wet is gegarandeerd.

Tot slot is het Comité R/I van mening dat eventuele tekortkomingen in het overleg en/of de communicatie tussen een inlichtingen- en veiligheidsdienst en de BIM-Commissie enerzijds en de gerechtelijke overheden anderzijds, geen invloed hebben op de wettelijkheid van de methoden.

2. ONDERSTEUNINGSMAATREGELEN

Sinds de wetswijziging van 2022 bestaat de mogelijkheid om ondersteuningsmaatregelen aan te vragen. De artikelen 13/1 tot en met 13/3 W.I&V voorzien in het plegen van strafbare feiten, het gebruik van valse namen en het oprichten van rechtspersonen met als louter doel het verbeteren van de informatiepositie van de dienst via een agent of een bron. Het zijn zgn. 'ondersteuningsmaatregelen' en geen inlichtingenmethoden, want ze mogen niet worden aangewend om informatie in te winnen. Wel moeten ze in verhouding staan met het beoogde doel en mag de fysieke integriteit van personen nooit in het gedrang komen bij de uitvoering van deze maatregelen. De diensten zetten ondersteuningsmaatregelen in om hun informatiepositie te beschermen of te verbeteren, denk daarbij aan een bron die strafbare uitlatingen doet op internet om zijn trouw te tonen aan een extremistische groepering.

Ook ondersteuningsmaatregelen zijn gebonden aan strikte regels. Bij het plegen van strafbare feiten moet de aanvragende dienst deze steeds aan de BIM-Commissie voorleggen zodat deze een beslissing kan nemen over de proportionaliteit ervan. Voor het gebruik van fictieve identiteiten volstaat dan weer het overmaken van een maandelijkse lijst.[23]

In 2025 werden 17 verzoeken om toestemming voor het plegen van strafbare feiten door agenten of menselijke bronnen goedgekeurd door de BIM-Commissie. Ze werden allen ingediend door de VSSE.

3. BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES

Artikel 44 W.I&V biedt de ADIV de mogelijkheid om elke vorm van communicatie uitgezonden of ontvangen in het buitenland op te sporen, te onderscheppen, af te luisteren en er kennis van te nemen alsook op te nemen.

In dat kader heeft de ADIV als opdracht om elk jaar een interceptieplan, een intrusieplan en een beeldplan op te stellen waarin deze dienst "*een lijst opstelt met organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties, intrusies in hun informaticasystemen of opnames van vaste of bewegende beelden tijdens het komende jaar. Deze lijsten verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie, intrusie of opname van vaste of bewegende beelden in verband met de opdrachten bedoeld in artikel 11, §1, 1° tot 3° en 5°, en vermelden de voorziene duur*" (art. 44/3 W.I&V).

Deze bevoegdheden zijn onderworpen aan een drievoudige controle door het Comité, vóór, tijdens en na de uitvoering van de intercepties, intrusies of beeldopnamen. De controle *a priori* wordt verricht op basis van de lijsten die de ADIV elk jaar opstelt en ter goedkeuring voorlegt aan de minister van Defensie. De controle *tijdens* de interceptie, intrusie of de beeldopnamen wordt verricht "*op elk*

23 Over de opdrachten die in dit verband aan het Comité R/I zijn toegewezen, zie Comité R/I, *Activiteitenverslag 2022*, pp. 89.

ogenblik door middel van bezoeken aan de installaties waar de Algemene Dienst Inlichting en Veiligheid deze intercepties, intrusies en opnames van vaste of bewegende beelden uitvoert". Het toezicht *na* de uitvoering vindt plaats op basis van maandelijkse lijsten van landen of organisaties of instellingen die effectief het voorwerp hebben uitgemaakt van een operatie van afluisteren, intrusie of het maken van beeldopnamen alsook op basis van de controle van logboeken die permanent worden bijgehouden op de plaats van interceptie, intrusie of beeldopname.

Het Comité R/I heeft de drie plannen voor het jaar 2025 in december 2024 ontvangen, nadat ze waren goedgekeurd door de minister van Defensie, zoals bepaald in de W.I&V.

In 2025 heeft het Comité een reeks bezoeken ter plaatse afgelegd en verschillende ontmoetingen gehad met de ADIV, waardoor het aanvullende informatie kon verzamelen over de manier waarop de ADIV zich kwijt van deze opdracht.

In 2025 bracht het Comité ook een advies uit over een ontwerp van koninklijk besluit tot vaststelling van bepaalde regels met betrekking tot de uitoefening van deze bevoegdheid.

KLACHTEN, AANGIFTEN EN VERZOEKEN

IDENTIFICEREN, BEGRIJPEN EN VERBETEREN VAN DISFUNCTIES

Het Comité R/I onderzoekt op grond van artikel 34 W.Toezicht klachten, aangiften en individuele verzoeken van burgers. Deze worden onderverdeeld in drie categorieën:

- **klachten inzake de werking**, het optreden, het handelen of het nalaten te handelen van de inlichtingendiensten, het OCAD en zijn ondersteunende diensten en hun personeelsleden;
- **klachten over de toepassing van bijzondere inlichtingenmethoden** (BIM) door de VSSE of de ADIV;
- **individuele verzoeken met betrekking tot de verwerkingen van persoonsgegevens** door de hogervermelde diensten, hun personeelsleden en hun verwerkers. Het Comité R/I treedt in deze op als de gegevensbeschermingsautoriteit waartoe de verzoeker zich kan wenden om na te gaan of de toepasselijke gegevensbeschermingsregels werden nageleefd en om zijn gegevens te laten verbeteren of te verwijderen (de zgn. DPA[24]-klachten).

1. OVERZICHT IN CIJFERS

In 2025 ontving het Comité R/I in totaal **63 klachten, aangiften en verzoeken**.

De kolommen in onderstaande tabel verdelen de klachten naargelang het Comité R/I exclusief bevoegd is, dan wel samen met het Comité P of het Controleorgaan op de politionele informatie (COC).[25]

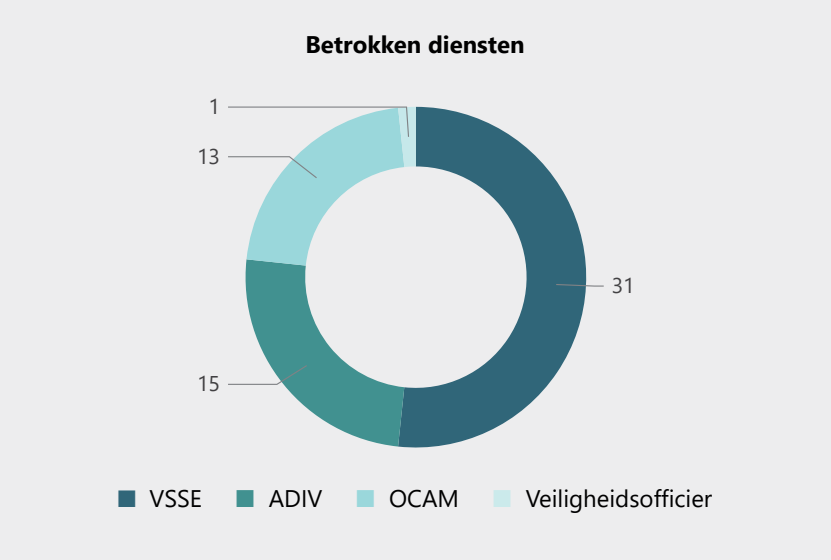
2025	COMITÉ R/I	COMITÉ R/I en COMITÉ P	COMITÉ R/I en COC	TOTAAL
Klachten ingediend	58	3	2	63
Onontvankelijke klachten	20	1	0	21
Ontvankelijke klachten	38	2	2	42
Hangende dossiers	0	0	0	0
Lopende dossiers	3	0	0	3
Ontvankelijke afgesloten dossiers	35	2	2	39
Corrigerende maatregelen	4	1	0	5

24 DPA staat voor *Data Protection Authority*.

25 Let wel, één en dezelfde klacht kan het voorwerp uitmaken van verschillende 'dossiers', en dit naargelang de betrokken diensten: een klacht tegen het OCAD én de VSSE wordt bijvoorbeeld zowel opgenomen in de door de Comités R/I en P gemeenschappelijk behandelde dossiers voor wat betreft het OCAD-luik, als bij de dossiers die uitsluitend door het Comité R/I worden behandeld voor wat betreft onderzoeksdaden met betrekking tot de VSSE.

61 klachten konden worden afgesloten in 2025. Slechts een beperkt aantal klachten waren begin 2026 nog in behandeling. Na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 21 klachten en aangiften af omdat ze kennelijk onontvankelijk waren of omdat het Comité R/I onbevoegd was om de opgeworpen vraag te behandelen. Ten opzichte van voorgaande jaren werd **een lichte stijging van het aantal bij het Comité R/I ingediende ontvankelijke klachten** vastgesteld.

Om ontvankelijk te zijn, moet de klacht of aangifte betrekking hebben op één of meerdere van de diensten waarop toezicht wordt gehouden (VSSE, ADIV of OCAD). Als de klachten inhoudelijk gaan over politionele tussenkomsten of de werking van het gerecht worden de klagers, indien mogelijk, doorverwezen naar de bevoegde instanties (bijv. de Hoge Raad van Justitie, het Openbaar Ministerie, het COC of het Comité P). Indien de aangiften enkel handelen over nuttige informatie die de inlichtingendiensten in eerste lijn zouden kunnen interesseren, wordt dit hen overgemaakt. Het Comité is niet bevoegd om klachten over de werking van buitenlandse inlichtingendiensten op Belgisch grondgebied te onderzoeken. Ook klachten met betrekking tot de werking en/of de beslissingen van de *Local Task Forces* (LTF's) en de Lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC-R's) zijn onontvankelijk, behoudens als deze handelen over de bijdragen van de inlichtingen- en veiligheidsdiensten in deze fora. Daarenboven is een klacht of aangifte pas ontvankelijk als de klager of aangever binnen de dertig dagen een identiteitsbewijs voorlegt. Anonieme klachten worden niet behandeld, doch de identiteit kan worden afgeschermd indien gewenst (behoudens bij DPA-klachten waarbij de identiteit doorslaggevend is voor het nazicht bij de inlichtingendiensten).



Uit het overzicht van de diensten die betrokken zijn bij de in 2025 ingediende klachten, blijkt de VSSE zeer sterk vertegenwoordigd.

2. AARD VAN DE ONTVANKELIJKE KLACHTEN

Van de 42 ontvankelijke klachten hadden er 24 betrekking op disfuncties bij de dienst(en) en werden 18 verzoeken met betrekking tot de verwerkingen van persoonsgegevens (DPA-klachten) behandeld. Er werden geen klachten over de inzet van bijzondere inlichtingenmethoden ingediend in 2025.

2025	COMITÉ R/I	COMITÉ R/I en COMITÉ P	COMITÉ R/I en COC	TOTAAL
Klachten over disfuncties	23	1	0	24
BIM klachten	0	0	0	0
DPA-klachten	15	1	2	18

2.1. Klachten over disfuncties bij de diensten

24 klachten en aangiften betroffen de werking, het optreden, het handelen of het nalaten te handelen van de inlichtingendiensten, het OCAD en zijn ondersteunende diensten en hun personeelsleden. **Slechts drie daarvan werden als gegrond beschouwd**.

In deze drie dossiers werden er **concrete maatregelen** genomen door de diensten **om het onderliggende functioneringsprobleem te remediëren**. Twee daarvan betroffen dossiers waarin een beroep tegen de weigering van een veiligheidsmachtiging werd ingediend bij het Beroepsorgaan en waarbij de hervorming van de beslissing niet werd uitgevoerd. Een ander dossier handelde over een batig gerangschikte kandidaat bij een inlichtingendienst die door een materiële vergissing nooit werd opgeroepen om zijn functie op te nemen.

De 21 overige ongegronde klachten waren sterk uiteenlopend. Er werd vastgesteld dat er in bepaalde dossiers een achterliggend burgerrechtelijk, tuchtrechtelijk of strafrechtelijk verhaal zat dat de bevoegdheid van het Comité te buiten ging. In twee dossiers waarbij de klagers in verdenking werden gesteld in een gerechtelijk dossier, beweerden zij – ten onrechte - dat zij jarenlang hadden gewerkt als 'informant' van een inlichtingendienst en in die hoedanigheid recht hadden op een vorm van strafrechtelijke immuniteit. Talrijke personen meenden het voorwerp uit te maken van doorlopende *surveillance* door de inlichtingendiensten, hetzij door vermeende fysieke agenten in hun omgeving (observatie), hetzij door cognitieve beïnvloeding. Geen enkel van deze klachten kon, na onderzoek, gegrond worden verklaard.

2.2. DPA-klachten

18 van de 42 in 2025 ingediende ontvankelijke klachten werden behandeld als DPA-klachten. Het Comité diende verschillende verzoeken te behandelen die waren ingediend in het raam van de **aanvraag tot verkrijging van de nationaliteit of een verblijfstitel**. Geconfronteerd met een negatief besluit op basis van door de VSSE, de ADIV en/of het OCAD verstrekte informatie, wenden verzoekers zich (onder meer) tot het Comité R/I voor een controle van de verwerking van hun persoons-

gegevens. De wijze waarop deze gegevens werden en worden gedeeld met buitenlandse partners, is een blijvend aandachtspunt voor het Comité dat wordt gevat door verzoekers die problemen ondervinden bij grenscontroles. Niet zelden gaat het hier over personen die ooit gekend waren in het raam van terrorisme, extremisme of radicalisme, maar waarover thans geen actuele informatie meer circuleert en deze personen ook niet meer worden opgevolgd. Door een wereldwijde proliferatie van namenlijsten na de aanslagen, blijkt dat personen op buitenlandse lijsten staan en hierdoor hinder ondervinden. Het Comité heeft echter geen enkele bevoegdheid ten aanzien van buitenlandse inlichtingendiensten en kan alleen de VSSE en de ADIV verzoeken om hiervan kennis te geven aan hun buitenlandse partnerdiensten. Het is met andere woorden afhankelijk van de welwillendheid van deze diensten, met dien verstande dat de samenwerking met deze soms beperkt of totaal niet aanwezig is.

Voor de eerste maal behandelde het Comité R/I in 2025 een **DPA-klacht tegen een veiligheidsofficier van een onafhankelijke federale toezichthouder** die evenwel geen enkele betrekking had op de inlichtingen- en veiligheidsdiensten. Echter, door een recente wetswijziging werd het Comité R/I residuair bevoegd voor alle DPA-klachten tegen veiligheidsofficieren en dit zowel in de publieke als in de private sector.

Het Comité legde als toezichthoudende autoriteit **in twee dossiers corrigerende maatregelen** op (art. 51/3 W.Toezicht). Het Comité R/I kan zich daarbij niet in de plaats stellen van de diensten in de zin dat het zelf een inlichtingenanalyse kan maken, maar kan wel dwingende beslissingen opstellen in geval dat het een verwerking van persoonsgegevens als onwettig heeft beoordeeld. Afhankelijk van het dossier, kan dit onder meer inhouden dat wordt verzocht om rectificatie of schrapping van de persoonsgegevens, dat de beslissing van het Comité R/I ter kennis moet worden gebracht van de partners en/of autoriteiten, of dat de beslissing binnen de betrokken dienst dient te worden verspreid.

ADVIEZEN

EEN UITEENLOPEND MAAR COHERENT GEHEEL AAN JURIDISCHE STANDPUNTEN

Enkel op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister mag het Comité R/I advies uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd (art. 33 W.Toezicht). Daarnaast dient het Comité ook advies te verlenen als Bevoegde Toezichthoudende Autoriteit (BTA) in het kader van de verwerking van persoonsgegevens (artt. 73 en 95 GBW). Soms worden adviezen geformuleerd vanuit deze dubbele hoedanigheid.

In 2025 werd **het Comité viermaal om advies verzocht**: tweemaal door de minister van Binnenlandse Zaken, eenmaal door de minister van Defensie en ook eenmaal door de Kamer van volksvertegenwoordigers. De gemiddelde termijn om een advies uit te brengen bedraagt ongeveer twee maanden.

Hierna volgt een samenvatting van de verleende adviezen, waarin de belangrijkste aangevoerde argumenten kort worden aangehaald. Om een duidelijk en volledig beeld te krijgen van hun reikwijdte en coherentie, is het aangewezen om de volledige adviezen te raadplegen.[26]

1. OVERLEG GEORGANISEERD OP BASIS VAN ARTIKEL 458*TER* VAN HET STRAFWETBOEK

Artikel 458*ter* van het Strafwetboek luidt als volgt:

"§ 1. Er is geen misdrijf wanneer iemand die uit hoofde van zijn staat of beroep houder is van geheimen, deze meedeelt in het kader van een overleg dat wordt georganiseerd, hetzij bij of krachtens een wet, decreet of ordonnantie, hetzij bij een met redenen omklede toestemming van de procureur des Konings. Dit overleg kan uitsluitend worden georganiseerd, hetzij met het oog op de bescherming van de fysieke en psychische integriteit van de persoon of van derden, hetzij ter voorkoming van de misdrijven bedoeld in Titel Iter van Boek II of van de misdrijven gepleegd in het raam van een criminele organisatie, zoals bepaald in artikel 324*bis*. De in het eerste lid bedoelde wet, decreet of ordonnantie, of de met redenen omklede toestemming van de procureur des Konings bepalen ten minste wie aan het overleg kan deelnemen, met welke finaliteit en volgens welke modaliteiten het overleg zal plaatsvinden.

26 Alle adviezen zijn terug te vinden op de website van het Comité (www.comiteri.be).

§ 2. De deelnemers zijn tot geheimhouding verplicht wat betreft de tijdens het overleg meegedeelde geheimen. Eenieder die dit geheim schendt, wordt gestraft met de straffen bepaald in artikel 458. De geheimen die tijdens dit overleg worden meegedeeld, kunnen slechts aanleiding geven tot de strafrechtelijke vervolging van de misdrijven waarvoor het overleg werd georganiseerd."

Deze bepaling, ingevoegd door de Wet van 6 juli 2017 of kortweg de Potpourri-wet V[27], maakt het mogelijk (beschermde) informatie te verstrekken in het kader van vertrouwelijk overleg met de politiediensten of op verzoek van de procureur des Konings, wanneer het erom gaat de fysieke of mentale integriteit van een persoon of derden te beschermen dan wel om de openbare veiligheid te beschermen. Deze bepaling is met name van toepassing op overleg dat plaatsvindt in het kader van de Lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC). Aangezien er in het kader van dergelijk overleg persoonsgegevens worden verwerkt, was er nood aan een specifieke rechtsgrondslag om een kader voor die verwerkingen te creëren.

Op 12 november 2024 werd een **wetsvoorstel** betreffende de verwerking van persoonsgegevens bij deelname aan een overleg georganiseerd op grond van artikel 458*ter* van het Strafwetboek ingediend in de Kamer van volksvertegenwoordigers. Via de Gegevensbeschermingsautoriteit (GBA) werd aan het Comité gevraagd om een advies uit te brengen over de tekst van het wetsvoorstel.

In zijn advies, verleend op **25 februari 2025**, merkte het Comité op dat het voorstel duidelijkheid miste wat betreft de overheden die precies werden bedoeld. Bij gebreke van een bepaling die formeel de overheden aanwees van Titel 3 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (GBW)[28], oordeelde het Comité R/I dat de tekst niet van toepassing was op de overheden ten aanzien van dewelke het de bevoegde toezichthoudende autoriteit is inzake gegevensbescherming en dat het bijgevolg niet bevoegd was om een advies uit te brengen. Het voegde echter toe dat, in de veronderstelling dat de opstellers de intentie hadden bepaalde overheden van Titel 3 GBW aan te wijzen, de regeling van het voorstel uitdrukkelijk in die zin moest worden aangevuld en dat de essentiële elementen van de verwerkingen moesten worden geregeld. Bij gebreke daarvan, en bij ontstentenis van de bewuste elementen, bracht het wetsvoorstel het wettelijkheidsbeginsel in gevaar.

Op 18 juni 2025 diende de opsteller een nieuwe versie van de tekst bij de Kamer in, waarin een aantal punten werd verduidelijkt.[29] Het voorstel werd goedgekeurd tijdens de plenaire vergadering van 8 januari 2026.

27 Wet van 6 juli 2017 houdende vereenvoudiging, harmonisering, informatisering en modernisering van bepalingen van burgerlijk recht en van burgerlijk procesrecht alsook van het notariaat, en houdende diverse bepalingen inzake justitie, *B.S.* 24 juli 2017.

28 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *B.S.* 5 september 2018.

29 Wetsvoorstel betreffende de verwerking van persoonsgegevens, bij deelname aan een overleg georganiseerd op grond van artikel 458*ter* van het Strafwetboek, *Parl. St.*, Kamer van volksvertegenwoordigers, 2024-2025, Doc 56 0935/001, 18 juni 2025.

2. INTERCEPTIE VAN COMMUNICATIE IN HET BUITENLAND DOOR DE ADIV

Met het oog op de uitvoering van zijn opdrachten kan de ADIV elke vorm van in het buitenland uitgezonden of ontvangen communicatie opsporen, onderscheppen, afluisteren, er kennis van nemen en opnemen. De artikelen 44 tot 44/5 van de Wet houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V) bevatten de bijzondere bepalingen voor de uitoefening van deze bevoegdheid evenals de modaliteiten betreffende het toezicht dat het Comité R/I ter zake uitoefent.

Op 28 juli 2025 vroeg de **minister van Defensie** aan het Comité om een advies uit te brengen over een ontwerp van koninklijk besluit tot vaststelling van de regels voor vernietiging van de illegaal verzamelde gegevens zoals bedoeld in artikel 44/4 W.I&V en tot vaststelling van de regels inzake medewerking zoals bedoeld in artikel 44/5 W.I&V.

Het voor advies overgelegde ontwerp van koninklijk besluit had als doel, zoals zijn titel aangeeft, bepaalde modaliteiten voor uitvoering en toezicht nader vast te stellen, te weten:

- de regels voor vernietiging van onwettig verzamelde gegevens bij dit type intercepties (artikel 44/4 W.I&S) ;
- de regels die van toepassing zijn in gevallen waarin de medewerking van een operator van een netwerk of dienstverstrekker vereist is om een interceptie mogelijk te maken (artikel 44/5 W.I&V). Het ontwerp had als doel om door middel van beperkingen en garanties een kader te bieden voor de stromen van gegevens en metadata die aldus worden onderschept.

In zijn advies van **11 september 2025** formuleerde het Comité een aantal opmerkingen, met name over de vernietiging van illegaal verzamelde gegevens. In dit verband loofde het de centrale rol die aan de functionaris voor gegevensbescherming (DPO) wordt toegekend in de vernietigingsprocedure en nodigde het de wetgever uit om aan de DPO een soortgelijke rol toe te kennen in de procedure voor vernietiging van gegevens die onrechtmatig worden verzameld met behulp van een bijzondere inlichtingenmethode. Opdat het Comité zijn toezicht ten volle zou kunnen uitoefenen, pleitte het voor de toevoeging van een bepaling die de ADIV verplicht om binnen een termijn van twee weken elk proces-verbaal van vernietiging van illegaal verzamelde gegevens toe te sturen. Wat betreft de regels die van toepassing zijn op intercepties die de medewerking van dienstverstrekkers of operatoren van netwerken vereisen, vroeg het Comité om bepaalde gebruikte begrippen (bijv. 'automatische transmissie van stromen van gegevens en metadata' en 'operationeel directeur') beter te definiëren alsook om bepaalde procedurele termijnen nader vast te stellen. Bovendien wees het Comité erop dat elk systeem of elke uitrusting dat/die een inlichtingendienst gebruikt voor de geautomatiseerde verwerking van persoonsgegevens, technisch gezien moet voldoen aan de vereiste van uitlegbaarheid (beginsel van *explainability*).[30]

30 Informatie vergaren door middel van een geautomatiseerde stroom van (meta)gegevens vereist dat er zowel stroomop- als stroomafwaarts kan worden uitgelegd hoe het systeem tot een welbepaald resultaat is gekomen.

3. ADMINISTRATIEF VERBOD VAN BEPAALDE ORGANISATIES

Bij brief van 31 juli 2025 ontving het Comité R/I een verzoek van de **minister van Binnenlandse Zaken** om een advies uit te brengen over een voorontwerp van wet betreffende het administratief verbod voor rechtspersonen, vennootschappen zonder rechtspersoonlijkheid, verenigingen of feitelijke groeperingen die een ernstige en actuele bedreiging vormen voor de nationale veiligheid of het voortbestaan van de democratische en grondwettelijke orde.

Het voorontwerp van wet had als doel een mechanisme van administratief verbod te creëren ten aanzien van organisaties die door hun concrete, gecoördineerde en aanhoudende activiteiten een ernstige en actuele bedreiging vormen voor de nationale veiligheid of voor de grondslagen van de rechtsstaat. Het ontwerp voorzag erin dat een dergelijk verbod twee vormen kon aannemen: de administratieve ontbinding van de organisatie of een verbod op haar activiteiten.

In zijn advies van **9 oktober 2025** heeft het Comité R/I zich ertoe beperkt elementen te bespreken betreffende de activiteiten en verplichtingen van de inlichtingendiensten.[31]

Wat betreft de redenen die tot een administratief verbod kunnen leiden, merkte het Comité meer bepaald op dat het wetsontwerp zich beperkte tot drie bedreigingen ten aanzien van de nationale veiligheid, i.e. terrorisme, gewelddadig extremisme en gewelddadig radicalisme, terwijl de W.I&V meerdere expliciete bedreigingen voor de nationale veiligheid vermeldt.[32] Het Comité stelde zich vragen bij de gemaakte keuze om het toepassingsgebied te beperken tot deze drie bedreigingen en nodigde de opsteller uit om de redenen nader te vermelden. Het Comité nodigde de opsteller ook uit om de betekenis van deze drie begrippen, die in het ontwerp niet worden gedefinieerd, nader te bepalen. Tevens vestigde het de aandacht op het inhoudelijke verschil tussen het begrip 'radicalisme' enerzijds en de begrippen 'radicaliseringsproces' en 'radicalisering' anderzijds. Het eerste is een toestand; de andere twee zijn een proces, een traject.

Aangaande de procedure wees het Comité op de overheersende rol die was toegewezen aan het Coördinatiecomité voor Inlichting en Veiligheid (CCIV), dat werd belast met de nieuwe opdracht om een analyse te maken die als basis kon dienen voor een eventueel administratief verbod. Het Comité had meerdere vragen bij de toewijzing van deze nieuwe formele opdracht. Meer bepaald de vraag te weten in welke mate de bestaande werkingsregels van het CCIV zullen moeten worden aangepast om deze nieuwe opdracht uit te voeren, maar ook of het CCIV beschikt over voldoende bevoegdheden om deze opdracht naar behoren uit te voeren en of zijn wettelijk kader zou moeten worden aangepast. Het Comité beval aan om in het wetsontwerp de regels vast te leggen betreffende het quorum en de vereiste meerderheid om een formele beslissing als college te nemen wanneer een analyse of een verslag wordt uitgebracht in het kader van de betrokken procedure. Het Comité wees er ook op dat het ontwerp niets vermeldde over de werkzaamheden voorafgaand aan de opmaak van een

31 Voor een meer algemeen overzicht, zie meer bepaald de adviezen van de Raad van State (januari 2026) en het Federaal Instituut voor de Bescherming en de Bevordering van de Rechten van de Mens (FIRM) (september 2025).

32 Het gaat om spionage, terrorisme, extremisme, terrorisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties en inmenging (artikel 8, 1°, lid 2 W.I&V).

analyse door het CCIV. Met voorafgaande werkzaamheden worden het verkrijgen van de vereiste informatie bij de bevoegde operationele diensten (bv. VSSE of ADIV) en de gezamenlijke analyse van die informatie door de leden van het CCIV bedoeld teneinde te kunnen overgaan tot de opmaak en goedkeuring van een analyse. Het Comité wees echter op vele punten die in dit verband dienden te worden verduidelijkt, zoals de identiteit van de dienst die werkelijk is belast met de analyse of de te volgen procedure indien het CCIV meent niet over voldoende informatie te beschikken om een beslissing te nemen.

Tot slot, wat betreft de beroepsmogelijkheid, voorzag het ontwerp in de jurisdictionele controle door de mogelijkheid om voor de Raad van State beroep in te stellen tegen eender welk administratief verbod. In dit verband wees het Comité op de vaste rechtspraak van het Europees Hof voor de Rechten van de Mens met betrekking tot de vereisten die van toepassing zijn wanneer overheden gebruik maken van geclassificeerde/geheime informatie in een individuele bestuursbeslissing: het Hof erkent dat, om redenen van nationale veiligheid, de toegang van een persoon tot zijn dossier mag worden beperkt, maar dat een rechter of een andere onafhankelijke autoriteit toegang moet krijgen tot het volledige dossier, met inbegrip van alle geclassificeerde of geheime stukken, opdat een jurisdictionele beroepsprocedure zou voldoen aan het recht op een eerlijk proces (art. 6 EVRM) alsook aan het recht op een effectief rechtsmiddel (art. 13 EVRM). De essentiële vraag die volgens het Comité aan bod zou kunnen komen in het kader van het jurisdictioneel beroep waarin het ontwerp voorziet, heeft betrekking op de toegang van het gevatte rechtscollege tot de geclassificeerde stukken die aan de basis liggen van het advies van het CCIV en bijgevolg van de aangevochten beslissing. Het Comité merkte op dat de in het ontwerp beschreven beroepsprocedure voor de Raad van State mogelijk niet zou kunnen voldoen aan de vereisten zoals bepaald door het Europees Hof in de gevallen waarin de analyse van het CCIV is gebaseerd op geclassificeerde informatie. Indien de analyse van het CCIV is gebaseerd op geclassificeerde informatie die afkomstig is van een inlichtingendienst, en zelfs indien deze laatste ervoor heeft gekozen een niet-geclassificeerde nota aan het CCIV te verstrekken, blijft het onderliggende dossier geclassificeerd. De beslissing van het CCIV zal dus gebaseerd zijn op geclassificeerde informatie waartoe het rechtscollege dat een uitspraak moet doen, toegang zou moeten krijgen opdat er zou worden voldaan aan de vereisten van het Europees Hof. Het wetsontwerp bevat geen dergelijke compenserende maatregelen. Om aan deze fundamentele tekortkoming tegemoet te komen, moet er voorrang worden gegeven aan de optie om deze opdracht toe te vertrouwen aan het Comité, en dit gelet op de prerogatieven die de wet aan het Comité toevertrouwt en op zijn expertisedomein.

Begin 2026 kondigde de minister van Binnenlandse Zaken aan dat het ontwerp zou worden herzien op basis van de verschillende verleende adviezen.

4. PNR- EN ETIAS-LIJSTEN

Op 15 september 2025 verzocht de **minister van Binnenlandse Zaken** het Comité om een advies te verlenen over twee ontwerpen van koninklijk besluit tot vaststelling van, enerzijds, een referentiekader voor de doeleinden van de verwerking van passagiersgegevens (*Passenger name record*, PNR) en, anderzijds, een referentiekader voor de raadpleging van de gegevens *European Travel Information and Authorisation System* (ETIAS) voor repressieve doeleinden.

De ontwerpen hadden als doel, ter uitvoering van wetsbepalingen, lijsten van strafbare feiten volgens nationaal recht op te stellen die overeenstemmen met de misdrijven zoals bedoeld door de Europese wetgever. Wat betreft de verwerking van passagiersgegevens gaat het om terroristische misdrijven en ernstige vormen van criminaliteit zoals gedefinieerd in artikel 3, punten 8 en 9, van de PNR-richtlijn.[33] Voor de ETIAS-gegevens gaat het dan weer om terroristische misdrijven en ernstige strafrechtelijke misdrijven zoals gedefinieerd in artikel 3, punten 15 en 16, van de ETIAS-verordening.[34] Het doel van beide lijsten bestond erin om aan de bevoegde overheden en operationele diensten een referentiekader te bieden teneinde de naleving van repressieve doeleinden van gegevensverwerking te waarborgen.

In zijn advies van 18 november 2025 herinnerde het Comité R/I aan de algemene beperking die de Europese wetgever had vastgesteld: om een strafrechtelijk misdrijf te kunnen opnemen in de PNR- of ETIAS-lijst, moet de betrokken inbreuk worden bestraft met een vrijheidsberovende straf of maatregel met een maximumstraf van minimum drie jaar. Voor het overige merkte het Comité op dat de Europese wetgever weinig (of geen) inhoudelijke beperkingen had opgelegd wat betreft de aan bepaalde begrippen te geven interpretatie. Bijgevolg stelde het Comité vast dat de opsteller bepaalde begrippen op restrictieve wijze had omschreven (meer bepaald het begrip 'deelname aan een criminele organisatie') en dat een aantal strafrechtelijke inbreuken bijgevolg kon worden toegevoegd aan beide lijsten. Bovendien merkte het Comité op, met betrekking tot de definitie van het begrip 'sabotage', dat de opzettelijke aard van de handeling van de dader ervan moest worden toegevoegd.

33 Richtlijn 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit.

34 Verordening 2018/1240 van het Europees Parlement en de Raad van 12 september 2018 tot oprichting van een Europees reisinformatie- en -autorisatiesysteem.

DE CEL INTEGRITEIT

EXTERN MELDINGSKANAAL VOOR INTEGRITEITSSCHENDINGEN

1. DE 'KLOKKENLUIDERSWET'

Van misstanden of frauduleuze praktijken binnen een professioneel kader - zogenaamde integriteitsschendingen - kan melding worden gemaakt. De melders, ook wel 'klokkenluiders' genoemd, vervullen een belangrijke rol door fraude en onregelmatigheden die worden vastgesteld bij openbare instellingen (of private ondernemingen) aan te kaarten. Echter, de vrees voor vergeldingsmaatregelen kan klokkenluiders ervan weerhouden om de stap te zetten melding te doen. De melders verdienen dan ook een passende erkenning, ondersteuning en bescherming aangezien ze mogelijks grote professionele en persoonlijke risico's lopen.[35]

Een Europese richtlijn[36] biedt bescherming aan zij die dergelijke inbreuken op de wetgeving of vermoedelijke integriteitsschendingen melden of openbaar maken. Deze richtlijn werd omgezet in nationaal recht via de Wet van 8 december 2022 betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie (Klokkenluiderswet).[37] De wet trad op 2 januari 2023 in werking. Optreden als klokkenluider werd bijgevolg een recht en melders kunnen terugvallen op enkele minimumnormen die werden voorzien ter bescherming wanneer zij vrezen dat hun melding nefaste gevolgen kan hebben voor hun (werk)situatie.

De wet verplicht overheidsinstanties te voorzien in een meldingssysteem voor klokkenluiders op verschillende niveaus: een melder moet de mogelijkheid hebben om intern, binnen de eigen organisatie dan wel extern een melding te doen, of de melder kan er meteen voor kiezen om de misstanden openbaar te maken.[38] Deze drie niveaus staan niet hiërarchisch ten opzichte van elkaar; welk niveau de melder kiest, is niet onderhevig aan het subsidiariteitsbeginsel. De melder heeft naar eigen goeddunken de vrije keuze.

De bescherming en ondersteuning die wordt geboden, is van toepassing bij de diverse meldingswijzen en impliceert een variatie aan maatregelen.[39] Daarenboven zijn represaillemaatregelen verboden en kan een klokkenluider rekenen op informatie en (zowel technisch als juridisch) advies, psychologische ondersteuning en rechtsbijstand. In de wet wordt een procedure uitgetekend die het verloop schetst van een interne dan wel externe melding.

In het kader van potentiële meldingen van integriteitsschendingen die binnen de ADIV of de VSSE werden begaan, werd het Comité R/I belast met de opdracht om op te treden als extern meldingskanaal.[40]

35 Federaal Instituut voor de Bescherming en de Bevordering van de Rechten de van Mens (FIRM) *Gids voor Klokkenluiders*, december 2024, https://federaalinstituutmensenrechten.be/nl/publicaties/gids-voor-klokkenluiders, geraadpleegd op 3 maart 2026.

36 Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden, *Publicatieblad van de Europese Unie*, 26 november 2019, L305/17.

37 *BS*, 23 december 2022.

38 Art. 7, §1, 2° Klokkenluiderswet.

39 Art. 28 en 29 Klokkenluiderswet.

40 Art. 14 §1, 3e lid Klokkenluiderswet.

2. DE CEL INTEGRITEIT BIJ HET COMITÉ R/I

In het kader van de uitvoering van zijn opdracht als extern meldingskanaal voor integriteitsschendingen begaan bij de ADIV en de VSSE, werd binnen het Comité R/I de Cel Integriteit opgericht. Deze werd samengesteld met respect voor de taalpariteit alsook een gelijke vertegenwoordiging van mannen en vrouwen. De cel bestaat uit vier medewerkers van het Comité R/I: twee commissaris-auditoren (Dienst Enquêtes) en twee juristen (Legal Section).

Medewerkers of leden van de ADIV of VSSE kunnen voortaan bij het Comité R/I terecht om een melding te doen van een (vermeende) integriteitsschending. De Cel Integriteit zal deze onderzoeken teneinde na te gaan of de melding ontvankelijk en gegrond is en wat er kan/moet gebeuren opdat er een einde aan de schending wordt gesteld of dat deze in de toekomst niet meer opnieuw wordt begaan.

Daartoe beschikt de Cel over een zeer brede waaier aan bevoegdheden en mogelijke onderzoekdaden: betrokkenen kunnen uitgenodigd worden hun medewerking te verlenen, nuttige stukken kunnen worden opgevraagd, betrokkenen kunnen worden gehoord… Deze opdracht als extern meldingskanaal brengt niet alleen heel wat bevoegdheden inzake het onderzoek naar de potentiele integriteitsschending met zich mee, maar ook een verantwoordelijkheid met betrekking tot de bescherming tegen represailles van de melder en zij die aan het onderzoek meewerken. [41] De leden van de Cel Integriteit volgden eind 2024-begin 2025 een specifieke opleiding met het oog op de behandeling en het onderzoek van de meldingen.[42]

Eind 2025 nam het Centrum Integriteit van de Federale Ombudsman het initiatief om een informeel netwerk op te richten dat de verschillende externe meldkanalen van de publieke sector samenbrengt, waaraan ook de leden van de Cel Integriteit deelnemen. Het gaat om een uitwisselingsplatform – lees intervisiegroep - dat tot doel heeft experts van de betrokken meldkanalen samen te brengen om te overleggen over de gemeenschappelijke uitdagingen en vraagstukken waarmee hun diensten worden geconfronteerd. Een eerste startvergadering vond plaats in januari 2026. Het netwerk zou drie tot vier keer per jaar samenkomen. Het netwerk heeft onder meer tot doel de banden tussen de externe meldkanalen te versterken, kennis en goede praktijken te delen, hun zichtbaarheid te verbeteren en hun strategische rol in de bescherming van klokkenluiders binnen de publieke sector te bevestigen.

41 Art. 14, §1, 6° Klokkenluiderswet.

42 Art. 14, §2 Klokkenluiderswet. Het betrof de opleiding '*Masterclass Fraud Auditing*' bij het *Institute of Fraud Auditors* (IFA), een post-master executive opleiding voor professionals die zich specialiseren in fraudebestrijding, -onderzoek en -preventie. Ze beoogt mensen te vormen tot effectieve fraude auditors door hen diepgaande kennis en praktische vaardigheden bij te brengen rond *fraud risk management*, fraudepreventie en -onderzoek, interviewtechnieken, cybercrime, leren analyseren van fraude scenario's en aanleren van *best practices* binnen de publieke en private sector. De opleiding werd in 2025 door eenieder van de Cel Integriteit met succes afgerond.

3. TOEPASSINGSGEBIED MET ZIJN BEPERKINGEN

3.1. Een extra uitdaging : de 'nationale veiligheid'

Als extern meldingskanaal voor de ADIV en de VSSE, onderzoekt het Comité R/I eventuele meldingen van misbruik, onregelmatigheden en fraude binnen deze twee inlichtingendiensten. Dat brengt een extra uitdaging met zich mee: de specifieke werking van de inlichtingendiensten is geënt op de 'nationale veiligheid'[43] en de Klokkenluiderswet sluit het domein van de nationale veiligheid specifiek uit van het toepassingsgebied. Immers, artikel 4 van deze wet stelt:

> *"§1. Deze wet is niet van toepassing op:*
> *1° geclassificeerde informatie*
> *...*
> *§2. Deze wet is niet van toepassing op nationale veiligheid, behalve met betrekking tot meldingen van inbreuken op regels betreffende overheidsopdrachten op het gebied van defensie en veiligheid bedoeld in art. 3, §4, eerste lid."*

De beoogde diensten (ADIV en VSSE) zijn diensten die belast zijn met de 'nationale veiligheid'.[44] De expliciete uitsluiting van bovenvermelde schendingen maakt het moeilijk – lees *quasi* onmogelijk - om de Klokkenluiderswet in de praktijk van de inlichtingendiensten toe te passen en zijn beschermingsdoel waar te maken. De memorie van toelichting bij de Klokkenluiderswet gaf destijds in verband met de uitsluiting van schendingen begaan tijdens activiteiten die vallen onder de nationale veiligheid dan ook al aan:

> *"[...] Voor deze schendingen zal in een afzonderlijke wet een specifiek meldingssysteem (intern en extern) gecreëerd worden. In deze afzonderlijke wet zullen er voldoende waarborgen ingebouwd worden opdat het heimelijk karakter van de werking van de inlichtingen- en veiligheidsdiensten gegarandeerd blijft [...]".*[45]

43 Conform de memorie van toelichting wordt 'nationale veiligheid' hier gedefinieerd als "*het geheel van de activiteiten van inlichtingen- en veiligheidsdiensten zoals bedoeld in artikelen 7 en 11 van de wet van 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten*".

44 Artt. 7 en art. 11 W.I&V.

45 Wetsontwerp betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie, 3 november 2022, Memorie van toelichting, p.170.

Het Comité R/I waarschuwde op zijn beurt in zijn advies[46] op het wetsontwerp voor de Klokkenluidersregeling in de publieke sector voor een moeilijk te hanteren onderscheid:

> *"[…] Voor wat betreft integriteitsschendingen tegenover inlichtingendiensten is het Comité evenwel van oordeel dat het in de praktijk onmogelijk zal zijn om een duidelijk onderscheid te maken tussen integriteitsschendingen begaan buiten de uitoefening van de opdrachten van deze diensten en integriteitsschendingen begaan binnen de uitoefening ervan […]"*

Begin 2026 dient te worden vastgesteld dat er nog geen volwaardig alternatief is voor de bescherming van melders van integriteitsschendingen begaan in de domeinen die in artikel 4 van de Klokkenluiderswet werden uitgesloten. Een wetsontwerp dat het klokkenluidersstatuut regelt voor wat betreft de integriteitsschendingen die in de eerste wet werden uitgesloten, wordt voorbereid.

3.2. Toch meldingen mogelijk…

De afwezigheid van een beschermingsstatuut voor melders van integriteitsschendingen begaan in de context van nationale veiligheid neemt evenwel niet weg dat dergelijke meldingen toch kunnen worden gedaan.

Het Comité R/I kan immers op verschillende manieren gevat worden om een onderzoek te doen, weliswaar buiten het kader van de Klokkenluiderswet. Zonder een specifieke wet ontbreekt het vooralsnog aan de extra bescherming die in dergelijke situaties net een meerwaarde biedt en mensen zou kunnen aanzetten de melding ook effectief te doen.

In de praktijk brengen de uitsluitingen vervat in artikel 4 Klokkenluiderswet met zich mee dat het op heden erg moeilijk is voor het Comité om de taak van extern meldingskanaal ten volle te vervullen. Van zodra een melding wordt gedaan van een schending begaan binnen ADIV of de VSSE, wordt geraakt aan diensten die hun bestaansreden hebben omwille van opdrachten in het kader van de nationale veiligheid. Vanuit het Comité R/I wordt dan ook het belang van een aanvullend wetgevend kader benadrukt zodat ook melders van integriteitsschendingen begaan binnen ADIV of VSSE, hetzelfde recht op bescherming en ondersteuning kunnen genieten zoals door de richtlijn bedoeld werd (*infra)*, en dit zonder mogelijk andere belangen te schenden die door hun specificiteit tevens - en terecht - niet uit het oog mogen verloren worden.

46 Comité R/I, Advies nr. 005/VCI/2022 van 30 augustus 2022 op het wetsontwerp voor de Klokkenluidersregeling in de publieke sector (de huidige Klokkenluiderswet) (www.comiteri.be).

3.3. De beschermings- en ondersteuningsmaatregelen

Wanneer een melder een ontvankelijke melding gedaan heeft, kan hij of zij rekenen op de door de wet voorziene beschermingsmaatregelen.[47] In hoofdorde betreft dit de bescherming tegen represaillemaatregelen. Wanneer men meent slachtoffer te zijn van dergelijke maatregel, dan kan een klacht worden ingediend bij het bevoegde externe meldingskanaal.

Onder represaillemaatregelen vallen een brede waaier aan mogelijke verschijningsvormen: schorsing, degradatie, negatieve prestatiebeoordeling, discriminatie, dwang, intimidatie… De bewijslast dat de maatregel in kwestie niet als represaille voor de melding geldt, ligt bij de betrokken overheidsinstantie. Ook personen die de melder bijstaan en/of medewerking verleend hebben aan het onderzoek kunnen op de voorziene beschermings- en ondersteuningsmaatregelen rekenen, als daar zijn het verlenen van informatie en advies, rechtsbijstand, psychologische bijstand, media gerelateerde en sociale ondersteuning…

Een melding van een integriteitsschending is geen individuele klacht
Een melder van een integriteitsschending neemt een fundamenteel andere positie in dan iemand die een klacht formuleert over het functioneren van medewerkers van de inlichtingendiensten. Daar waar een klacht impliceert dat de 'klager' een persoonlijk nadeel ondervindt van het 'foute' gedrag van de medewerker, geldt dit in beginsel niet voor melders van integriteitsschendingen. Een melding kan bijgevolg worden gedaan en kan een onderzoek initiëren, zonder dat er verder nog intensief contact met de melder nodig is.

3.4. Eén integriteitsschending gemeld

Meldingen anno 2025 gedaan aan het Comité R/I in het kader van zijn opdracht als extern meldingskanaal werden geëvalueerd volgens de huidige wetgeving. Dat betekent dat de enige meldingen die ontvankelijk kunnen zijn, zich situeren binnen niet-opdrachtgerelateerde activiteiten van de inlichtingendiensten.[48] Een gegeven dat enigszins paradoxaal kan aanvoelen. In 2025 werd één dossier opgestart en ontvankelijk verklaard met betrekking tot een melding van een integriteitsschending. Dat onderzoek is in 2026 nog lopende.

Wil u als medewerker van de ADIV of de VSSE een integriteitsschending melden? Dat kan per e-mail (signalement_melding@comiteri.be), telefonisch (02/286.29.11 - vraag naar de Cel Integriteit) dan wel op afspraak. U kan ook schriftelijk een melding indienen (Comité R/I, Cel Integriteit, Leuvenseweg 48 bus 5, 1000 Brussel).

47 Artt. 28 en 29 Klokkenluiderswet.

48 De schendingen begaan in het kader van opdrachten inzake nationale veiligheid zijn niet ontvankelijk (onder het beschermingsstatuut van de Klokkenluiderswetgeving).

HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN EN -ADVIEZEN

EEN UITZONDERLIJK HOOG DOSSIERVOLUME

Het Beroepsorgaan is het administratief rechtscollege dat bevoegd is voor geschillen die betrekking hebben op veiligheidsmachtigingen en -adviezen. Het is een collegiaal orgaan dat is samengesteld uit de (plaatsvervang(st)ers van de) voorzit(s)ters van het Comité R/I, het Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit.

Het Beroepsorgaan verleent ofwel beslissingen, wanneer het wordt gevat met een beroep inzake veiligheidsmachtigingen, ofwel adviezen, wanneer het wordt gevat met een beroep betreffende een veiligheidsadvies. Gemakkelijkheidshalve wordt in wat volgt de term "beslissingen van het Beroepsorgaan" voor zowel de beslissingen als de adviezen die het Beroepsorgaan verleent, gehanteerd.

Het Comité R/I neemt het voorzitterschap en de griffie van het Beroepsorgaan waar. Het stelt de personeelsleden en middelen ter beschikking die nodig zijn voor de werking van het Beroepsorgaan, met name voor het bijhouden van de griffie, de organisatie van de zittingen, het opstellen van de processen-verbaal of de uitwerking van de beslissingen.

1. ALGEMENE TENDENSEN

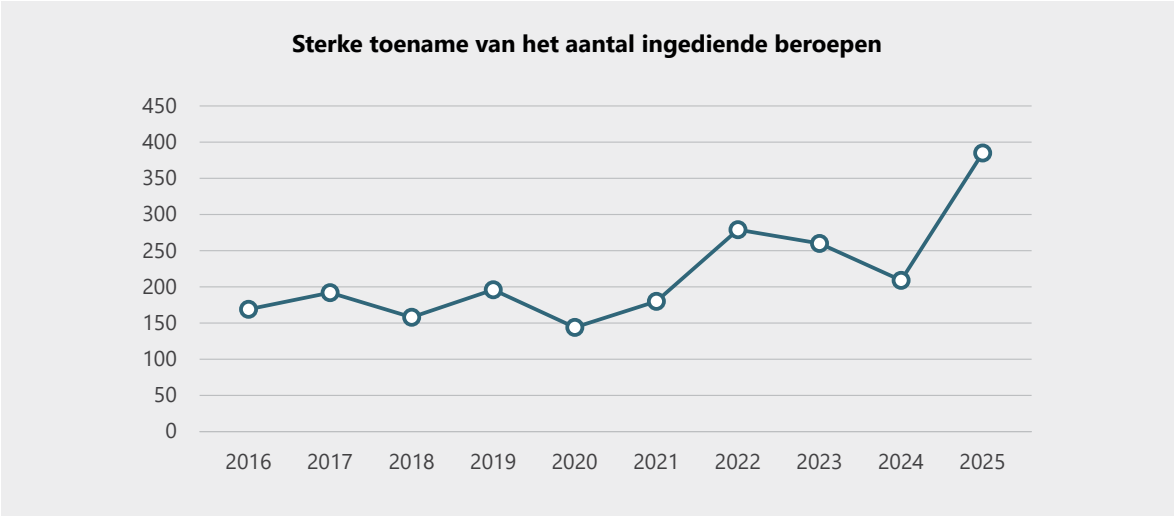
Het jaar 2025 werd gekenmerkt door het grote aantal beroepen dat werd ingediend en onderzocht door het Beroepsorgaan. De volgende paragrafen geven een overzicht van de activiteiten van het Beroepsorgaan. Ze geven onder andere een gedetailleerd beeld van het aantal ingediende beroepen volgens de aard van de betwiste beslissingen en de taal van de procedure, evenals van het aantal en het type beslissingen van het Beroepsorgaan of ook van de vastgestelde verwerkingstermijnen.

De voorgestelde cijfers zijn louter de weergave van geschillen die het Beroepsorgaan heeft behandeld. Ze geven geen beeld van het totale volume beslissingen of ongunstige adviezen van de veiligheids- en verificatieoverheden[49] [50], waarvan slechts een deel het voorwerp uitmaakt van een beroep. Bijgevolg mogen de waargenomen tendensen niet worden geïnterpreteerd als een directe indicator van de evolutie van de activiteiten van de betrokken instanties. Voor een volledig overzicht van het aantal veiligheidsmachtigingen en -adviezen die het afgelopen jaar zijn toegekend, wordt verwezen naar de activiteitenverslagen van de verschillende bevoegde autoriteiten.

49 Er bestaan drie veiligheidsautoriteiten: de Nationale Veiligheidsoverheid, de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid.

50 Het begrip "verificatieoverheid" verwijst naar de overheid die de veiligheidsadviezen aflevert. Tot die instanties behoren meer bepaald de Federale Politie, de ADIV ...

1.1. Sterke toename van het aantal ingediende beroepen



	2020	2021	2022	2023	2024	2025
NVO	91	86	183	188	77	97
VSSE	0	4	2	0	1	3
ADIV	41	84	76	56	65	88
FANC	7	6	12	11	10	14
Federale Politie	4	0	1	4	56	182
Lokale Politie	1	0	5	1	0	1
TOTAAL	**144**	**180**	**279**	**260**	**209**	**385**

In 2025 is het aantal ingediende beroepen sterk gestegen, van 209 in 2024 tot 385 in 2025, wat neerkomt op een toename met 84%. Deze stijging betreft voornamelijk beroepen tegen veiligheidsadviezen, hoewel beroepen inzake veiligheidsmachtigingen ook aanzienlijk zijn toegenomen (cf. *infra*).

De evolutie wordt ook gekenmerkt door een toename van het aantal beroepen volgens de taal van de procedure. De toename is het grootst voor beroepen die in het Nederlands zijn ingediend, i.e. van 76 beroepen in 2024 tot 195 beroepen in 2025, een stijging van 156% (zie *infra*). Het aantal in het Frans ingediende beroepen blijft gestaag stijgen, van 133 in 2024 naar 190 in 2025, een stijging van 43%.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Frans	99	115	83	101	83	86	201	159	133	190
Nederlands	70	77	75	95	61	94	123	101	76	195
Duits	0	0	0	0	0	0	0	0	0	0

1.2. Verdeling van de beroepen volgens de aard van de betwiste beslissingen

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Machtigingen	50	40	36	51	32	60	83	105	102	145
Adviezen	101	122	92	115	99	108	157	134	85	234
Attesten	18	30	30	30	13	12	39	21	22	6
TOTAAL	**169**	**192**	**158**	**196**	**144**	**180**	**279**	**260**	**209**	**385**

1.2.1. Veiligheidsmachtigingen

In 2025 is het aantal in verband met veiligheidsmachtigingen ingediende beroepen sterk gestegen, van 102 dossiers in 2024 tot 145, een toename met 42%. Het Beroepsorgaan beschikt niet over de elementen die toelaten de oorzaak van de toename van het aantal beroepen vast te stellen. Op te merken valt dat 23% van deze beroepen (33 van 145) werd ingediend omdat de veiligheidsinstantie niet binnen de wettelijke termijn een beslissing nam (of de aanvrager niet in kennis stelde van zijn beslissing).

1.2.2. Veiligheidsadviezen

De meest in het oog springende evolutie deed zich voor bij de veiligheidsadviezen, met 234 beroepen in 2025 tegenover 85 in 2024, of een toename met 175%. Deze stijging houdt voornamelijk verband met de beroepen die zijn ingediend tegen een negatief veiligheidsadvies om een functie in een havengebied uit te voeren. De veiligheidsscreening voor toegang tot havens die sinds 2024 verplicht is, ligt dus grotendeels aan de oorsprong van deze stijging. Gezien de geopolitieke situatie is het bovendien waarschijnlijk dat de screenings strenger zullen worden, wat dan weer zou kunnen leiden tot een toename van het aantal negatieve veiligheidsadviezen en, bijgevolg, van het aantal beroepen dat wordt ingediend.

Bovendien heeft ook de afschaffing van de veiligheidsattesten (zie *infra*) bijgedragen tot de evolutie van het aantal verleende veiligheidsadviezen; voortaan is immers een advies vereist voor functies en sectoren waarvoor in het verleden slechts een attest noodzakelijk was.

1.2.3. Veiligheidsattesten

Aangezien het systeem van de veiligheidsattesten werd afgeschaft (zie *infra*), worden er sinds 1 februari 2025 geen attesten meer afgeleverd. Deze hervorming heeft logischerwijs geleid tot een afname van het aantal beroepen ter zake. Het Beroepsorgaan behandelde in 2025 echter nog wel zes dossiers met betrekking tot weigeringen van veiligheidsattesten waartoe werd beslist vóór de afschaffing van dit systeem.

1.3. Beslissingen van het Beroepsorgaan

1.3.1. Volume en verdeling volgens de aard van de beslissingen

De toename van het aantal ingediende beroepen in 2025 leidde tot een toename van het aantal beslissingen van het Beroepsorgaan. Op te merken valt dat sommige van deze beslissingen betrekking hebben op dossiers die in 2024 werden ingediend, en dat sommige van de beroepen die in 2025 zijn ingediend, pas in 2026 zullen worden behandeld. Zo is het totale aantal beslissingen van het Beroepsorgaan gestegen van 261 in 2024 tot 357 in 2025, een stijging van 37%.

Deze beslissingen hadden betrekking op:
- 164 veiligheidsmachtigingen (46% van het totaal);
- 177 veiligheidsadviezen (49,5%);
- 16 veiligheidsattesten (4,5%).

1.3.2. Hervormingen en intrekkingen

Van alle beroepen die in 2025 werden behandeld, besliste het Beroepsorgaan tot hervorming[51] van 47 beslissingen inzake veiligheidsmachtigingen op 164 (of 28,7%), zes beslissingen inzake veiligheidsattesten op 16 (of 37,5%) en 62 veiligheidsadviezen op 177 (of 35%). Dit resultaat getuigt van een doeltreffende controle door het Beroepsorgaan, dat een diepgaand onderzoek verricht dat in een significant aantal gevallen leidt tot de wijziging van de bestreden beslissingen.

Bovendien valt op te merken dat een niet te verwaarlozen deel van de beslissingen leidt tot een akte van intrekking van beroep: 12,3% van alle verleende beslissingen en adviezen (44 op 357) en 17,7% van de verleende beslissingen inzake veiligheidsmachtigingen (29 op 164). Een intrekking betekent dat de aanvrager een einde wenst te stellen aan de procedure. Dat gebeurt meestal wanneer een beroep is ingediend wegens het ontbreken van een beslissing binnen de wettelijke termijn en de veiligheids- of verificatieoverheid uiteindelijk een beslissing neemt, terwijl het geding loopt.

1.3.3. Termijn voor verwerking van de beroepen

In 2025 duurde het gemiddeld 125,9 dagen om dossiers te behandelen, of iets meer dan 4 maanden vanaf het moment dat het beroep werd ingediend. Dit resultaat laat zien dat het Beroepsorgaan in staat is een groter aantal dossiers te beheren in vergelijking met vorig jaar. Dit werd met name mogelijk gemaakt door de recente uitbreiding van het personeel van de griffie (cf. *infra*), waardoor het groeiend aantal beroepen meer efficiënt kon worden verwerkt en tegelijk de kwaliteit van de genomen beslissingen en uitgebrachte adviezen kon worden gehandhaafd.

Sinds medio 2025 komt het Beroepsorgaan wekelijks bijeen. Gezien de brede waaier van opdrachten van het Comité en de instanties die samen het Beroepsorgaan vormen, is het echter moeilijk om meer dan één zitting per week te organiseren.

51 "Een beslissing hervormen" betekent dat het Beroepsorgaan de initiële beslissing vervangt door een nieuwe beslissing.

Tevens valt op te merken dat de verwerkingstermijn niet alleen afhangt van het Beroepsorgaan. Deze termijn wordt ook bepaald door de (te lange) termijnen waarbinnen de veiligheids- en verificatie-overheden de administratieve dossiers van de aanvragers doorsturen; dit punt wordt hieronder nader toegelicht.

1.4. Termijn voor ontvangst van de administratieve dossiers

Het Beroepsorgaan wordt regelmatig geconfronteerd met vertragingen bij de toezending van de administratieve dossiers door de verificatie- en veiligheidsoverheden. Deze termijnen hebben een directe impact op de duur van de verwerking van de beroepen, aangezien het Beroepsorgaan slechts op zinvolle wijze uitspraak kan doen op voorwaarde dat het beschikt over het (volledige) administratieve dossier.

In 2025 waren de termijnen voor toesturen van de administratieve dossiers als volgt verdeeld:

a. Inzake veiligheidsadviezen:
   - 48 dossiers ontvangen binnen de wettelijke termijn van 10 dagen;
   - 71 dossiers ontvangen binnen een termijn van 11 tot 20 dagen;
   - 37 dossiers ontvangen binnen een termijn van 21 tot 30 dagen;
   - 77 dossiers ontvangen binnen een termijn van meer dan 30 dagen, waarvan 19 dossiers binnen een termijn van meer dan 100 dagen.

In totaal werd meer dan 75% van de administratieve dossiers inzake veiligheidsadviezen buiten de wettelijke termijn van 10 dagen ontvangen.

b. Inzake veiligheidsmachtigingen:
   - 25 dossiers ontvangen binnen de wettelijke termijn van 15 dagen;
   - 48 dossiers ontvangen binnen een termijn van 16 tot 30 dagen;
   - 52 dossiers ontvangen binnen een termijn van 31 tot 99 dagen;
   - 17 dossiers ontvangen binnen een termijn van meer dan 100 dagen.

In totaal werd meer dan 80% van de administratieve dossiers inzake veiligheidsmachtigingen buiten de wettelijke termijn van 15 dagen ontvangen. Deze vertraging draagt bij aan de langere tijd die het Beroepsorgaan nodig heeft om beroepen te behandelen.

2. EVOLUTIE VAN HET RECHTSKADER EN DE RECHTSPRAAK

2.1. Nieuwe wetgeving

De Wet van 2 juni 2024 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, veiligheidsattesten, veiligheidsadviezen en de publiek geregu-

leerde dienst is in werking getreden op 1 februari 2025. Dit bracht enkele belangrijke wijzigingen met zich mee.

2.1.1. Afschaffing van de veiligheidsattesten

Daar waar er aanvankelijk drie soorten screeningsresultaten waren (de veiligheidsmachtigingen, -attesten en -adviezen), werden door de hogervermelde wet de veiligheidsattesten afgeschaft. Sinds 1 februari 2025 is een veiligheidsadvies vereist voor de functies en sectoren waarvoor in het verleden een veiligheidsattest moest worden verkregen.

2.1.2. Wijzigingen met betrekking tot de veiligheidsadviezen

Onder de door voornoemde wet aangebrachte wijzigingen, voert artikel 36 van de Wet van 11 december 1998 ("de classificatiewet") twee nieuwe types van positieve veiligheidsadviezen in, namelijk het positieve veiligheidsadvies met individuele waarschuwing en het positieve veiligheidsadvies met administratieve waarschuwing.

Een positief veiligheidsadvies met individuele waarschuwing betekent dat de overheid niet over voldoende elementen beschikt om een negatief advies uit te brengen, maar de aanvrager waarschuwt voor de noodzaak om zijn gedrag te verbeteren wat betreft de aangehaalde punten.

Een positief veiligheidsadvies met administratieve waarschuwing wordt afgegeven wanneer de aanvrager niet in België verbleef gedurende de periode van vijf jaar die het voorwerp uitmaakt van de veiligheidsverificatie en de overheid niet over voldoende informatie beschikt in verband met de betrokkene.

Bovendien is het sedert 1 februari 2025 ook mogelijk om een beroep in te dienen wanneer de verificatieoverheid geen veiligheidsadvies heeft verleend binnen de wettelijke termijn.

2.2. Prejudiciële vraag aan het Grondwettelijk Hof

In 2024 stelde het Beroepsorgaan aan het Grondwettelijk Hof een prejudiciële vraag om te weten of de artikelen 17 en 18 van het Gerechtelijk Wetboek, die betrekking hebben op het vereiste van een reeds verkregen en dadelijk belang om beroep in te stellen, verenigbaar zijn met de artikelen 10 en 11 van de Grondwet. Deze vraag had inzonderheid betrekking op de ontvankelijkheid van een beroep voor het Beroepsorgaan in geval van weigering om een veiligheidsmachtiging te verlenen wanneer de aanvrager de verbreking van zijn contract niet eerst had betwist ten overstaan van het bevoegde rechtscollege.

In de bewuste zaak had de Nationale Veiligheidsoverheid (NVO) geweigerd om de veiligheidsmachtiging van de aanvrager, werknemer bij de NAVO, te verlengen en als gevolg daarvan was zijn arbeidsovereenkomst beëindigd.

In zijn arrest nr. 36/2025 van 27 februari 2025 meende het Hof dat de vereiste van een reeds verkregen en dadelijk belang, i.e. het feit dat de aanvrager aantoont het verlies van zijn betrekking te

hebben betwist, op onevenredige wijze afbreuk deed aan het recht op toegang tot een rechter. Deze vereiste ontnam ook de nuttige uitwerking aan het specifieke beroep waarin is voorzien voor beslissingen inzake veiligheidsmachtigingen. Het Hof valideerde dus een interpretatie van de wet die toelaat beroep in te dienen bij het Beroepsorgaan vanaf de weigering of intrekking van een veiligheidsmachtiging of, in geval van gebrek aan beslissing binnen de vastgestelde termijn, zonder bijkomende voorwaarde. Het arrest bekrachtigt daarmee een ruime interpretatie van het recht op beroep, door elke overdreven vereiste inzake belang om te handelen te weren, teneinde de daadwerkelijkheid van het beroep te garanderen.

2.3. Ontvankelijkheid van het beroep en bevoegdheid van de Raad van State versus het Beroepsorgaan

De vraag naar de bevoegdheid van het Beroepsorgaan deed zich voor in het kader van een zaak waarover de Afdeling Bestuursrechtspraak van de Raad van State zich begin september 2025 heeft uitgesproken in zijn arrest.[52] In dit dossier had de verzoeker, een contractueel medewerker voor de Europese Commissie die was aangeworven om in een post in het buitenland te werken, een veiligheidsmachtiging van het niveau "EU SECRET" aangevraagd die vereist is om deze functie uit te oefenen.

De Nationale Veiligheidsoverheid (NVO) verklaarde "geen gunstig gevolg te kunnen geven aan deze aanvraag" omdat ze meende dat het veiligheidsonderzoek niet kon worden uitgevoerd waardoor ze niet bij machte was om voldoende informatie te verzamelen om te beoordelen of de verzoeker de vereiste garanties bood. De NVO verwees meer bepaald naar het feit dat de verzoeker gedurende bijna de hele onderzoeksperiode functies in het buitenland had uitgeoefend en al vele jaren niet meer in België woonde. In de kennisgeving stond dat de verzoeker in geval van onenigheid een verzoek tot nietigverklaring van deze beslissing kon indienen bij de Raad van State.

De advocate van de verzoeker twijfelde aan de bevoegdheid van de Raad van State en diende uit voorzorg beroep in bij beide instanties. Ze voerde aan dat het wel degelijk ging om een beslissing om een veiligheidsmachtiging te verlenen.

De Raad van State bevestigde deze analyse en oordeelde dat de NVO, door te verklaren dat ze geen "gunstig gevolg" kon geven aan de aanvraag van veiligheidsmachtiging, op impliciete maar zekere wijze had geweigerd deze machtiging te verlenen. Artikel 4, §1, W.Beroepsorg. kent aan het Beroepsorgaan echter uitdrukkelijk de bevoegdheid toe om kennis te nemen van beslissingen tot weigering van machtigingen. De Raad van State oordeelde dus dat hij een dergelijke beslissing niet kon vernietigen of opschorten. De Raad van State preciseerde ook dat de redenen die de NVO aanvoerde, namelijk het langdurige verblijf in het buitenland en het ontbreken van een woonplaats in België, daar niets aan veranderden. Aangezien het gaat om een weigering komt de bevoegdheid toe aan het Beroepsorgaan, los van de aangevoerde redenen.

52 Arrest nr. 264.054 van 3 september 2025.

2.4. Onmogelijkheid van onderzoek

De 'onmogelijkheid van onderzoek' werd door de NVO aangevoerd in andere soortgelijke dossiers. Er werden bij het Beroepsorgaan immers meerdere dossiers aanhangig gemaakt waarin de NVO oordeelde dat het onmogelijk was een veiligheidsonderzoek te voeren omdat de verzoeker in het buitenland verbleef. Zoals supra uiteengezet, betwistte de NVO de bevoegdheid van het Beroepsorgaan omdat de aangevochten handeling geen 'weigering om een machtiging te verlenen' vormde, maar veeleer een gewone vaststelling van de onmogelijkheid om een onderzoek te voeren.

Volgend op voornoemd arrest van de Raad van State heeft het Beroepsorgaan zich bevoegd verklaard in deze verschillende dossiers. Het was van oordeel dat de NVO zich niet systematisch kon beroepen op een onmogelijkheid om een onderzoek in te stellen zodra de verzoekende partij een loopbaan in het buitenland uitoefende, terwijl de betrokken functie vereiste dat de houder ervan in het buitenland verbleef.

In het kader van deze dossiers wees het Beroepsorgaan erop dat de inlichtingen- en veiligheidsdiensten over ruime bevoegdheden beschikken om in het kader van een veiligheidsonderzoek diverse stappen te ondernemen, ook buiten het Belgische grondgebied.[53] Het is ook van mening dat een veiligheidsoverheid redelijke inspanningen moet leveren om haar onderzoek uit te voeren. Het Beroepsorgaan is bijvoorbeeld van mening dat het mogelijk is om rekening te houden met de professionele beoordelingen van de verzoeker, om een interview met hem te organiseren, zijn banden met België in aanmerking te nemen, contact op te nemen met de regionale veiligheidsofficier of nog om de aanname van verzachtende maatregelen te overwegen. Gezien het bovenstaande was het Beroepsorgaan van mening dat het mogelijk was een onderzoek in te stellen in deze verschillende dossiers.

2.5. Screening als verdoken human resources-maatregel

Het Beroepsorgaan stelt vast dat regelmatig screenings negatief worden afgesloten om redenen die niet conform de wettelijke bepalingen zijn. Uit de behandelde dossiers is gebleken dat soms een veiligheidsmachtiging wordt geweigerd of een negatief veiligheidsadvies wordt verstrekt op basis van redenen die geen gevaar inhouden voor de democratische rechtsorde of de nationale veiligheid. Dit houdt een onjuiste toepassing in van de geldende wettelijke bepalingen.

Een veiligheidsmachtiging is enkel vereist als de betrokkene toegang moet hebben tot geclassificeerde informatie. De betrokken persoon moet dan voldoende garanties bieden op het vlak van integriteit, loyauteit en discretie. Een veiligheidsmachtiging mag alleen worden geweigerd als er concrete elementen zijn dat de betrokkene een risico vormt voor de nationale veiligheid. Het Beroepsorgaan moet controleren of de beslissing van de veiligheidsoverheid voldoet aan de wettelijke criteria.

53 Zie de artikelen 18 en 19 van de wet van 11 december 1998 betreffende de classificatie, de veiligheidsmachtigingen, de veiligheidsadviezen en de publiek gereguleerde dienst.

2.6. Screening op basis van een reglementair besluit

Ondanks een grote toename in de veiligheidsscreenings, dient het Beroepsorgaan er waakzaam voor te blijven dat deze screenings steeds een reglementaire basis hebben wanneer ze worden uitgevoerd. Zo werd een screening uitgevoerd op deelnemers aan een info-sessie over 'werken bij de Lokale politie' die plaatsvond in de infrastructuur van een lokale politiezone. Het Beroepsorgaan ging in eerste instantie na op basis van welke reglementair besluit de verificatie was gebaseerd. Echter, in deze situatie, was de screening enkel opgelegd voor personen die tijdelijk een opdracht of functie zouden uitoefenen in de infrastructuur van de Lokale Politie. Het Beroepsorgaan oordeelde dat het volgen van een infosessie geenszins onder de categorie valt van 'uitoefenen van functie of opdracht'. De persoon in kwestie was bijgevolg onterecht geweigerd om de infosessie te volgen, meer nog, de facto waren alle deelnemers aan de infosessie onterecht gescreend.

Het spreekt voor zich dat, zeker gelet op het stijgend aantal screenings, er blijvend aandacht moet zijn voor het rechtmatig uitvoeren ervan. Het blijft belangrijk na te gaan of in bepaalde gevallen een veiligheidsscreening al dan niet noodzakelijk is en of met de screening wel het doel wordt bereikt waarvoor het instrument wordt inzet.

2.7. Toepassing van artikel 5 § 3 W.Beroepsorgaan

In het kader van het recht van verdediging moet de verzoeker in de mogelijkheid zijn te weten wat de reden/motivering is om hem of haar een veiligheidsmachtiging te weigeren of een negatief veiligheidsadvies te verlenen. Het kan voorkomen dat bepaalde informatie niet kan of mag getoond worden op risico dat andere belangen worden geschonden: persoonlijke informatie over derden, de werking van de inlichtingen- en veiligheidsdiensten, het verloop van een gerechtelijk onderzoek, de bescherming van bronnen.

Op basis van art. 5 §3 W.Beroepsorgaan kunnen de veiligheidsoverheden of verificatieoverheden aan het Beroepsorgaan vragen om bepaalde informatie om voormelde redenen niet te laten inkijken aan de verzoeker of zijn/haar raadsman. Op dat moment dient een afweging te worden gemaakt om de verzoeker minstens ook een echte kans te geven om zichzelf te verdedigen en een negatieve beslissing of advies op ernstige wijze te kunnen aanvechten. Concreet betekent dit dat niet alle verzoeken om informatie onder 'embargo' te plaatsen, per definitie worden ingelost.

3. BEROEPEN INGESTELD BIJ ANDERE RECHTSCOLLEGES

3.1. Cassatie voor de Raad van State

In 2025 werden drie Cassatieberoepen ingediend tegen beslissingen van het Beroepsorgaan. Eén dossier werd ontoelaatbaar verklaard op basis van het gebrek aan ontvankelijke middelen. De twee andere dossiers waren nog lopende eind 2025. Tot slot werd een dossier dat in 2024 werd opgestart in 2025 verworpen door de Raad van State. Als reden van verwerping van het Cassatieberoep

werd gesteld dat er geen schending van de wettelijke bepalingen werd vastgesteld. De verzoeker in Cassatie had aangehaald dat zijn hoorrecht geschonden was alsook de motiveringsplicht. Beide middelen werden verworpen.

3.2. Verzoekschrift voor het Europees Hof voor de Rechten van de Mens

Er werd ook een verzoekschrift ingediend voor het Europees Hof voor de Rechten van de Mens. Het gaat om een beroep tegen een negatief veiligheidsadvies.

De verzoeker beroept zich op artikel 6 van het Europees Verdrag voor de Rechten van de Mens en meent dat de onmogelijkheid om toegang te hebben tot doorslaggevend bewijsmateriaal dat aan het Beroepsorgaan was overgelegd en het gebrek aan duidelijke motivering van de beslissing van dat orgaan, een schending van zijn recht op een eerlijk proces vormen. Hij beroept zich ook op artikel 8 van het Verdrag en voert aan dat het negatieve veiligheidsadvies een inbreuk op zijn privéleven vormt, met name met betrekking tot zijn beroepsleven. De zaak was eind 2025 nog niet afgerond.

4. INTERNE ORGANISATIE EN WERKING VAN DE GRIFFIE

4.1. Interne organisatie en personeel

De toename van het aantal beroepen dat in 2025 werd ingediend (zie supra), had een directe weerslag op de organisatie van de zittingen en de werklast van het Beroepsorgaan.

Sinds het voorjaar van 2025 worden er twee zittingen per maand georganiseerd voor Franstalige dossiers, zodat er 12 tot 15 dossiers per zitting kunnen worden onderzocht.

Vanaf medio 2025 is, als gevolg van de aanzienlijke toename van het aantal in het Nederlands ingestelde beroepen, hetzelfde ritme van twee maandelijkse zittingen ingevoerd voor Nederlandstalige dossiers, met een gelijkwaardig aantal onderzochte dossiers.

De activiteiten van het Beroepsorgaan vertegenwoordigen een bijzonder zware werklast voor het Comité R/I, ook al gaat het om slechts een van de vele opdrachten die aan het Comité zijn toevertrouwd. Om het hoofd te kunnen bieden aan de toename van het aantal geschillen en de groeiende hoeveelheid administratieve taken, werden in september en oktober 2025 twee personeelsleden aangeworven om de griffie van het Beroepsorgaan te versterken. Dankzij deze versterking konden er redelijke verwerkingstermijnen worden gehandhaafd en dat ondanks de toename van de activiteit op het vlak van geschillen. De behandeling van de dossiers vereist momenteel het equivalent van twee juristen (één Franstalige en één Nederlandstalige) en vier voltijdse secretariaatsmedewerkers. De voorzitster en de betrokken raadsheer besteden hier ongeveer 20% van hun werktijd aan.

4.2. Digitalisering en modernisering van de procedure

In 2025 is een grondige denkoefening opgestart over de digitalisering van de beroepsprocedure bij het Beroepsorgaan. Het tweeledige doel bestaat er meer bepaald in om (a) de werklast van de griffie te verlichten en (b) het voor burgers gemakkelijker te maken om beroep in te stellen.

Dit project omvat een functionele analyse van de verschillende fasen van de procedure, IT-ontwikkeling evenals een herziening van de regels voor het indienen en onderzoeken van beroepen. Dit is een langetermijnproces dat vanwege de vereiste ingrijpende technische en regelgevende aanpassingen in 2026 zal worden voortgezet.

Op termijn is het de bedoeling dat aanvragers kunnen kiezen voor een elektronische procedure. Een dergelijke evolutie zou moeten leiden tot een significante afname van het aantal aangetekende zendingen door het Beroepsorgaan en moeten bijdragen tot een vermindering van de kosten in verband daarmee (momenteel geraamd op ca. € 50 per dossier in de eenvoudigste gevallen). Digitalisering zou ook zorgen voor een betere traceerbaarheid van uitwisselingen, kortere termijnen voor toesturen van de stukken en een vereenvoudiging van het werk van de griffie.

(INTER)NATIONALE SAMENWERKING

KENNIS EN EXPERTISE DELEN

1. INTERNATIONALE UITWISSELINGEN

In tijden van alsmaar toenemende internationale samenwerking (informatie-uitwisseling inbegrepen) tussen de inlichtingen- en veiligheidsdiensten, is het Comité R/I overtuigd van de noodzaak aan meer doorgedreven internationale samenwerking tussen toezichthoudende autoriteiten. Ongeacht of dit gebeurt in de vorm van bilaterale ontmoetingen of in het kader van bredere, multilaterale werkgroepen, maakt dergelijke samenwerking het mogelijk om goede praktijken inzake toezicht op de inlichtingendiensten te identificeren, manieren te vinden om dit toezicht te versterken en vervolgens aan te passen aan de hedendaagse uitdagingen.

In 2025 waren artificiële intelligentie, de aankoop van omvangrijke volumes gegevens (bulk data) en het Verdrag 108+ de belangrijkste thema's op de internationale fora waaraan het Comité R/I heeft deelgenomen.

Ontmoeting met de *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, 2 april 2025, Brussel

Een delegatie van de Nederlandse Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) kwam in april 2025 op bezoek bij het Comité R/I. Deze ontmoeting bood de gelegenheid om van gedachten te wisselen over de specifieke kenmerken van eenieders toezichtorgaan alsook over de gemeenschappelijke uitdagingen waaraan het hoofd moet worden geboden. Onder meer de strijd tegen de georganiseerde misdaad en de aankoop van omvangrijke volumes gegevens maakten het voorwerp uit van gedachtewisselingen. Dit bezoek legde de basis voor een versterkte, bilaterale samenwerking tussen beide toezichthouders.

European Intelligence Oversight Network, 20 mei 2025, Brussel

In 2025 was de workshop van het *European Intelligence Oversight Network* (EION)[54] gewijd aan het gebruik door de inlichtingen- en veiligheidsdiensten van gegevens verkregen uit commerciële bronnen. De besprekingen vormden de gelegenheid om een stand van zaken op te maken van de vigerende regelgeving alsook het dagdagelijkse toezicht op de werkzaamheden van de inlichtingendiensten. Ook het Verdrag 108+ en die mogelijkheden die het biedt voor versterkte, internationale samenwerking tussen toezichthoudende autoriteiten, waren het voorwerp van bespreking.

Intelligence Oversight Working Group, 21-23 mei 2025, Kopenhagen

Een *technical meeting* van de *Intelligence Oversight Working Group* (IOWG)[55] vond eind mei 2025 plaats in Kopenhagen. Na de gebruikelijke rondvraag over de nieuwigheden bij de nationale toe-

54 Het EION brengt vertegenwoordigers samen van de toezichthoudende autoriteiten van België, Canada, Denemarken, Duitsland, Frankrijk, Litouwen, Nederland, Noorwegen, Servië, het Verenigd Koninkrijk, de Verenigde Staten, Zweden en Zwitserland.

55 In het kader van de IOWG komen de toezichthoudende instanties samen van België, Canada, Denemarken, Nederland, Noorwegen, het Verenigd Koninkrijk, Zweden en Zwitserland.

zichthouders afzonderlijk, bespraken de deelnemers het toezicht op het gebruik van artificiële intelligentie door inlichtingendiensten en het beheer van de databanken. Het technische luik werd gevolgd door een zgn. *staff meeting* tijdens dewelke de IOWG-leden de uitdagingen hebben besproken waarmee ze tijdens hun controles te maken krijgen. Het ging bijvoorbeeld over personeelsbeheer, de soms lange termijnen om onderzoeken te voeren, de communicatiestrategie of nog, de toegang tot de inlichtingendiensten.

Intelligence Oversight Working Group, 4-5 november 2025, Zürich

De IOWG-leden kwamen eind 2025 opnieuw samen in Zürich. De debatten tijdens deze bijeenkomst gingen met name over het gebruik van cryptomunten door inlichtingendiensten, het beheer van kennis en expertise binnen toezichthoudende autoriteiten en de opleiding van hun personeel. De *technical*- en *staff meeting* werden gevolgd door een *Chairmeeting* tijdens dewelke de Canadese toezichtsinstantie, te weten het *Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR – NSIRA)*, tot dan waarnemend lid, officieel werd aangenomen als volwaardig IOWG-lid. Volgend op de vaststellingen die werden gedaan op de vergaderingen van mei en november 2025, werden twee werkgroepen opgericht: de werkgroep *AI Oversight* ziet toe op het gebruik (en het toezicht daarop) van artificiële intelligentie in de context van de nationale veiligheid, terwijl de werkgroep *Oversight Gap* zich buigt over mogelijke oplossingen voor internationale samenwerking tussen toezichthoudende autoriteiten.

Coloquium "'National Security' and the Politics of Security Screenings in a Globalized World", 5 november 2025, Oslo

In november 2025 werd een beroep gedaan op de expertise van het Comité R/I in het kader van een colloquium gewijd aan de problematiek van veiligheidsscreenings en georganiseerd door de *Oslo Metropolitan University* (Oslomet). Het ging onder meer over de uitdagingen in verband met veiligheidsonderzoeken die op nationaal niveau worden gevoerd in een geglobaliseerde wereld alsook over de methodologie die inlichtingendiensten gebruiken om personen te kwalificeren.

European Intelligence Oversight Conference, 5-6 november 2025, Zürich

In november 2025 nam het Comité R/I deel aan de tweede *European Intelligence Oversight Conference* (EIOC). Het EIOC werd in 2018 opgericht en heeft tot doel ruimte voor ontmoetingen en besprekingen te creëren voor zowel toezichthoudende autoriteiten als vertegenwoordigers vanuit het middenveld. In 2025 gingen de uitwisselingen meer bepaald over de *bulk data* en de lacunes inzake toezicht van de inlichtingen- en veiligheidsdiensten.

International Intelligence Oversight Forum, 18-19 november 2025, Austin

Nog in november 2025 vond het *International Intelligence Oversight Forum* (IIOFF) plaats in Austin, Texas. De presentaties, georganiseerd rond het thema "*Intelligence Oversight in Complex Security*

Environments", hadden betrekking op de relaties tussen toezichthoudende autoriteiten en gecontroleerde diensten, het gebruik van tools voor artificiële intelligentie in het kader van de nationale veiligheid alsook over het Verdrag 108+.[56] Het Comité maakte van zijn verplaatsing naar Austin gebruik om leden van het *Strauss Center for International Security and Law* van de universiteit van Texas, een onderzoekscentrum gewijd aan recht en internationale veiligheid, te ontmoeten.

Ontmoeting met de *Toetsingscommissie Inzet Bevoegdheden*, 27 november 2025, Brussel

Het Comité R/I ontving in november 2025 een delegatie van de Toetsingscommissie Inzet Bevoegdheden (TIB) ontvangen in Brussel. In Nederland is deze commissie belast met het *a priori* toezicht op de inlichtingenmethoden die worden toegepast door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Tijdens deze ontmoeting bespraken beide instellingen hun wettelijke verplichtingen en gebruiken inzake communicatie, het gebruik van artificiële intelligentie door de inlichtingen- en veiligheidsdiensten en het interne toezicht dat door hen wordt georganiseerd.

2. DE BELGISCHE TOEZICHTGEMEENSCHAP

Naast de internationale samenwerking investeert het Comité ook in contacten en uitwisselingen met de Belgische partners. Om te zorgen voor een doeltreffend toezicht op de inlichtingen- en veiligheidsdiensten is nauwe samenwerking immers noodzakelijk tussen alle spelers in de 'toezichtgemeenschap', die verder gaat dan alleen het Comité R/I.

2.1. Gemeenschappelijke vergaderingen met het Comité P

Artikel 52 van de W.Toezicht voorziet in ten minste twee vergaderingen per jaar tussen het Comité R/I en het Comité P. In 2025 zijn de Comités ook effectief tweemaal samengekomen, (in juli en december). Beide Comités bespraken de voortgang van meerdere gemeenschappelijke dossiers, het ontwerp tot herziening van een protocolakkoord over de uitoefening van de bevoegdheden van toezichthoudende autoriteiten voor de verwerking van persoonsgegevens alsook de dossiers en werking van het Beroepsorgaan.

Tegelijk vonden er talrijke uitwisselingen plaats met het Comité P, meer bepaald in het kader van gemeenschappelijke toezichtonderzoeken en de gezamenlijke behandeling van klachten.

56 Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens.

2.2. Platform Mensenrechten

Sinds 2015 zijn alle instellingen met een mandaat inzake mensenrechten de verbintenis aangegaan om praktijken en werkmethoden uit te wisselen, gemeenschappelijke kwesties te onderzoeken en wederzijdse samenwerking te bevorderen.[57] Deze uitwisselingen vinden plaats binnen het overlegplatform Mensenrechten.

In 2025 vonden er zeven vergaderingen plaats onder het voorzitterschap van het Vlaams Mensenrechteninstituut en vervolgens van het Federaal Instituut voor de Bevordering en de Bescherming van de Rechten van de Mens (FIRM). De besprekingen tijdens deze vergaderingen hadden meer bepaald betrekking op het federale regeerakkoord, geestelijke gezondheidszorg in de gevangenis, de opvangcrisis, de Europese verordening inzake artificiële intelligentie en meer algemeen over de uitdagingen inzake het gebruik van artificiële intelligentie door openbare diensten en nog, de beleidsontwikkelingen aangaande het Europees Hof voor de Rechten van de Mens.

57 Protocolakkoord van 13 januari 2015 tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens.

INTERNE WERKING

EEN ORGANISATIE MET VERHOOGDE SLAGKRACHT

SAMENSTELLING VAN HET COMITÉ R/I

Vanessa Samain en Séverine Merckx oefenden hun respectieve mandaat van voorzitster en Franstalig lid van het Comité R/I in 2025 verder uit. Linda Schweiger werd vervangen door Filip Vanneste, raadsheer in het hof van beroep van Antwerpen, die op 22 april 2025 de eed heeft afgelegd als Nederlandstalig lid. Tijdens de plenaire vergadering van de Kamer van volksvertegenwoordigers op 6 november 2025, werd hij gemandateerd voor een nieuwe periode van zes jaar.[1]

De Dienst Enquêtes onder leiding van Frederic Verspeelt telde zeven commissaris-auditoren. De administratie, onder leiding van griffier Frédéric Givron, werd versterkt met de aanwerving van een secretaris, een bediende, een jurist en een *Chief Information Security Officer* (CISO). Eind 2025 waren er 22 administratieve medewerkers actief.

INTERNE REORGANISATIE

De reorganisatie van de interne structuur van het Comité, die tot stand kwam in overleg met de medewerkers, werd vanaf januari 2025 ontplooid. Naast de ondersteunende functies (secretariaat, IT, boekhouding, personeelszaken) is de administratie nu opgedeeld in twee secties: *Legal,* belast met juridische zaken en analyses en *Perspective & Analysis,* als documentatie- en expertisecentrum. Tegelijk werden transversale werkgroepen (WG) opgericht bestaande uit medewerkers van verschillende diensten binnen het Comité; het doel bestaat erin de multidisciplinaire benadering van de opdrachten en verantwoordelijkheden van het Comité te bevorderen (WG Bijzondere inlichtingenmethoden, WG Interne en externe communicatie, WG Horizon 2030, enz.).

Met deze nieuwe organisatie wil het Comité de taken en verantwoordelijkheden van elk team verduidelijken, en dit meer bepaald sinds de versterking van het personeelsbestand. Bovendien werd met de hervorming ook tegemoetgekomen aan meerdere aanbevelingen die het Rekenhof in zijn audit van 2024 had geformuleerd.

De reorganisatie werd voor het eerst geëvalueerd tijdens twee *teambuildings*, respectievelijk in juni 2025 voor de leden van de Dienst Enquêtes en in oktober 2025 voor de administratieve medewerkers. Deze seminaries hebben toegelaten om concrete pistes te identificeren en nieuwe werkprocessen te definiëren. De besprekingen leverden ook bredere input voor de opmaak van het toekomstige, strategische plan van het Comité R/I.

1 Bij deze gelegenheid werden Vinciane Boon en Isabelle Goes benoemd tot respectievelijk eerste en tweede Franstalige plaatsvervangende leden van het Comité R/I.

EEN NIEUWE VISUELE IDENTITEIT

Nog in 2025 heeft het Comité zijn visuele identiteit hervormd. Deze aanpak sluit aan bij een streven om het vertrouwen te versterken, het professionalisme te onderstrepen en de fundamentele waarden en principes te weerspiegelen die het handelen van het Comité leiden. Wettelijkheid, integriteit, onafhankelijkheid, transparantie en striktheid: deze principes, de pijlers van de werking van het Comité, verdienen een imago dat ze uitdrukt en versterkt.

Als dotatiegerechtigde instelling van de Kamer van volksvertegenwoordigers richt het Comité zich dagelijks tot de parlementsleden en politieke verantwoordelijken. Zij zijn echter niet de enige doelgroep' van het Comité; de producten van het Comité zijn ook bestemd voor de bredere toezichtgemeenschap, die wordt gevormd door institutionele partners, het maatschappelijk middenveld of nog, de pers. Maar bovenal wil het Comité zijn werking resoluut op de burgers richten. Vanwege zijn complexe en veelzijdige opdrachten die worden uitgevoerd in de periferie van de vertrouwelijke sector van de nationale veiligheid, blijft het Comité immers weinig bekend bij het grote publiek. De activiteiten van het Comité, die essentieel zijn in een rechtsstaat, kunnen echter een directe weerslag hebben op (de rechten van) burgers – bijv. via de behandeling van klachten. De nieuwe visuele identiteit van het Comité is dan ook bedoeld om de zichtbaarheid van het Comité alsook die van het toezicht op de inlichtingendiensten te versterken.

Het nieuwe logo symboliseert meerdere metaforen die de weergave vormen van de identiteit van het Comité. De metafoor van de boom staat een organisatie die door haar geschiedenis is geworteld in een stevig fundament van waarden. De stam belichaamt stabiliteit en betrouwbaarheid, terwijl de takken de diversiteit van zijn opdrachten illustreren. De verschillende opdrachten van het Comité worden autonoom uitgevoerd, maar blijven onlosmakelijk met elkaar verbonden.

De discrete verwijzing naar de nationale driekleur verwijst naar de democratische principes waarop de Belgische staat is gebaseerd. Ze verwijst naar de verantwoordelijkheid van het Comité om onafhankelijk, onpartijdig en transparant te handelen, in het belang van elke burger.

Samen vormen deze grafische elementen een vingerafdruk als symbool van de unieke identiteit van het Comité als *sui generis* orgaan. Die afdruk weerspiegelt het unieke karakter, de authenticiteit en de betrouwbaarheid van de instelling en herinnert ons tegelijk aan het belang van vertrouwelijkheid en de striktheid die zijn opdrachten aansturen.

PARLEMENTAIRE BEGELEIDINGSCOMMISSIE

De voorzitter van de Kamer, Peter De Roover (N-VA), is tevens voorzitter van de Parlementaire Begeleidingscommissie van het Vast Comité van toezicht op de politiediensten en het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (de Begeleidingscommissie). In 2025 waren de

stemgerechtigde leden Paul Van Tigchelt (Anders), Sammy Mahdi (cd&v), Stefaan Van Hecke (Ecolo-Groen), Benoît Lutgen (Les Engagés), Denis Ducarme (MR), Benoît Piedboeuf (MR), Peter Buysrogge (N-VA), Christoph D'Haese (N-VA), Maaike De Vreese (N-VA), Khalil Aouasti (PS), Eric Thiébaut (PS), Greet Daems (PVDA-PTB), Francesca Van Belleghem (VB), Marijke Dillen (VB) en Brent Meuleman (Vooruit).

In de loop van 2025 vonden twee vergaderingen van de Commissie plaats waar de besprekingen betrekking hadden op een toezichtonderzoek, het activiteitenverslag 2024, enkele lopende dossiers evenals de interne werking van het Comité R/I.

OPEN VOOR EXTERNE EXPERTISE

Het Comité R/I besteedt ook aandacht aan interne denkoefeningen rond bredere, hedendaagse uitdagingen inzake inlichtingen, veiligheid of democratische controle. Daarvoor doet het Comité beroep op externe deskundigen die worden uitgenodigd om hun inzichten te komen delen ter gelegenheid van lunches die telkens in het teken van een bepaald thema staan.

In 2025 werden er twee dergelijke sessies georganiseerd. In juni stelde Bernard Siman (Egmont-instituut/VUB) een exposé voor over hybride oorlogsvoering en de evolutie op het vlak van oorlogs- en vredespraktijken. Op de tweede sessie in september verwelkomde het Comité de voorzitter van het Coördinatiecomité voor Inlichting en Veiligheid, Pascal Petry, adviseur Federale Politie, die een presentatie gaf over de dagelijkse, concrete werking van dit platform dat centraal staat in de Belgische veiligheidsarchitectuur.

BUDGET

Het budget voor 2025 van het Comité R/I werd vastgesteld op € 6.393.778 een toename met 1,6% tegenover 2024 en dat overeenstemt met de indexering en de baremieke verhogingen van de lonen van het personeel.

De door de Kamer van volksvertegenwoordigers toegekende financiering is als volgt samengesteld: 81% als dotatie, de enige inbreng in netto kasmiddelen, en 19% boni 2023. Dit is de enige bron van financiering van het Comité doch laat toe alle activiteiten van het Comité financieel te dekken.

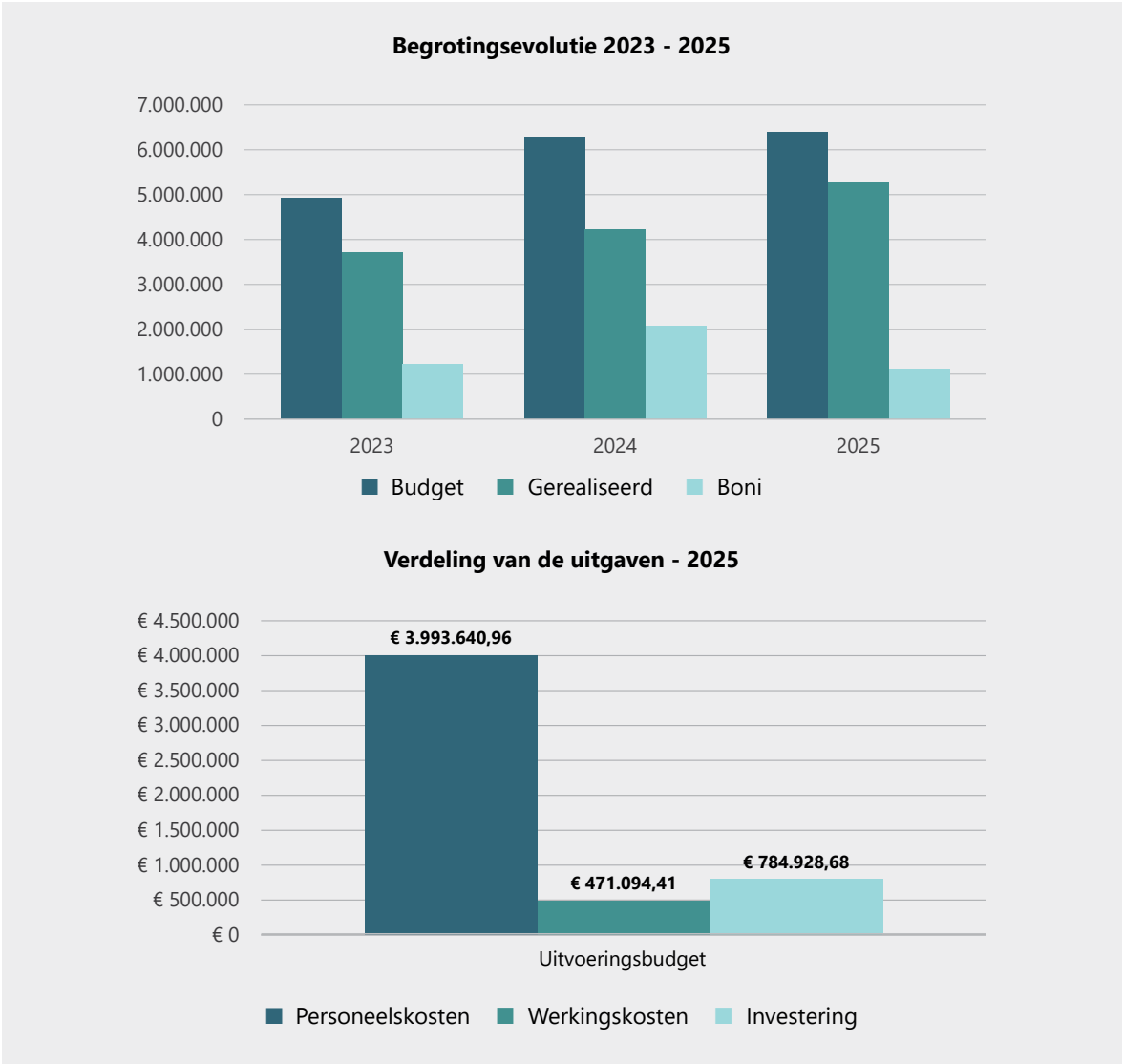
De uitvoering van het budget 2025 leverde een boekhoudkundig resultaat of boni op van € 1.125.013 te weten het verschil tussen het goedgekeurde budget en de vastgestelde uitgaven. De boekhoudkundige boni wordt gelijk verdeeld tussen personeels- en werkingskosten. Twee factoren kunnen een verklaring bieden voor deze aanzienlijke boni.

› Het Comité heeft vanaf 2024 een uitzonderlijke financiering over een periode van drie jaar gevraagd om zijn processen te digitaliseren en zijn IT-infrastructuur te vernieuwen. De uitvoering van dit project is onderworpen aan de veiligheidscontroles die inherent zijn aan de aard van de activiteiten van het Comité (de noodzakelijke veiligheidsmachtigingen voor bedrijven en personeel die worden toegekend na veiligheidsonderzoeken, die gemiddeld negen maanden duren)

alsook aan het streven naar optimalisatie van de middelen. Als gevolg daarvan is er vaak vertraging met de identificatie van potentiële leveranciers, beschikbare raamovereenkomsten, controle van de offertes en toewijzingen van opdrachten, wat de volledige vereffening van de beschikbare kredieten verhindert.

› In de afgelopen jaren hebben de sterke toename in het kader van de reeds bestaande toezichtopdrachten van het Comité, het ontstaan van nieuwe, erg diverse opdrachten ten gevolge van wetswijzigingen evenals de toename van de werklast in verband met het beheer van het Beroepsorgaan, ertoe geleid dat het Comité nieuw personeel heeft aangeworven. Tijdens de werkingsjaren 2023, 2024 en 2025, werden meerdere aanwervingen of vervangingen geïnitieerd. Door de duur van het wervingsproces, de tijd die nodig is om de vereiste veiligheidsmachtigingen te verkrijgen, en rekening houdende met eventuele opzegtermijnen, kan er meer dan een jaar verstrijken tussen de oproep tot kandidaturen en de effectieve indiensttreding van de betrokken medewerker. Deze duur voedt automatisch het boekhoudkundig resultaat van het jaar waarin de rekrutering loopt. Het Comité is zich bewust van deze uitdaging en doet bijkomende inspanningen om de duur van het rekruteringsproces te verkorten, alvast wat betreft de parameters die tot zijn bevoegdheid behoren.

Er wordt dus verwacht dat de indiensttreding van de nieuwe medewerkers in 2026 en zelfs 2027 alsook de voltooiing van het digitaliseringsproject zullen leiden tot een nieuw evenwicht van het goedgekeurde budget en de vastgestelde uitgaven evenals de afname van de boni.



DIGITALISERING

Eind 2023 kende de Kamer van volksvertegenwoordigers het Comité R/I een specifiek budget toe om een grootschalig digitaliseringsproject te implementeren teneinde zijn werking te moderniseren.

Volgend op de aanzienlijke investeringen in *hardware* en *software* die in 2024 werden gerealiseerd, focusten de projecten van 2025 op de digitalisering van de werkprocessen. Inzonderheid de modernisering van de werking van de griffie van het Beroepsorgaan zal het mogelijk maken om de administratieve taken te verlichten. Tegelijk legt het Comité de laatste hand aan de ontwikkeling van een digitale bibliotheek die een modern en intuïtief beheer van zijn documentatie mogelijk moet maken.

Er werd tevens een oplossing voor beveiliging van de hardware geïnstalleerd om de doorgifte in één richting van gegevens tussen twee netwerken mogelijk te maken. Concreet verloopt de doorgifte van bestanden van het *online* geconnecteerde netwerk naar het beveiligde netwerk van het Comité voortaan bijna in *realtime* waarbij de veiligheidsnormen strikt in acht worden genomen.

Deze IT-ontwikkelingen zijn van cruciaal belang met het oog op het behoud van een evenwichtige aanwending van de middelen van het Comité ten opzichte van al zijn opdrachten. Bovendien beschikken de medewerkers hiermee over moderne en flexibele tools die toelaten om samen te werken en tegelijk een passend veiligheidsniveau garanderen.

Ook zijn er verschillende projecten opgestart om het geclassificeerde netwerk van het Comité te moderniseren; daarnaast is er ook een *Chief Information Security Officer* (CISO) in dienst getreden.

Ook de website van het Beroepsorgaan, die door het Comité wordt beheerd, werd in 2025 vernieuwd. De inhoud ervan werd aangepast als gevolg van de ingrijpende opeenvolgende wetswijzigingen inzake veiligheidsmachtigingen en -adviezen. Het Comité R/I zal in 2026 over een nieuwe website beschikken die voldoet aan alle hedendaagse normen en verwachtingen.

AFKORTINGEN

ADIV	Algemene Dienst Inlichting en Veiligheid
Begeleidingscommissie	Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
BIM	Bijzondere inlichtingenmethoden
BIM-Commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BS	Belgisch Staatsblad
BTA	Bevoegde Toezichthoudende Autoriteit
CCIV	Coördinatiecomité voor Inlichting en Veiligheid
COC	Controleorgaan voor politionele informatie
Conventie 108+	Verdrag nr. 108 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens
DPO	Data Protection Officer (functionaris voor de gegevensbescherming)
EMB	Executief van de Moslims in België (Moslimexecutieve)
ETIAS	European Travel Information and Autorisation System
EVRM	Europees Verdrag voor de Rechten van de Mens
FIRM	Federaal Instituut voor de Bescherming en de Bevordering van de Rechten van de Mens
GBA	Gegevensbeschermingsautoriteit
GBW	Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Gegevensbeschermingswet)
GGB TER	Gemeenschappelijke gegevensbanken TER
IOWG	Intelligence Oversight Working Group
LIVC-R	Lokale Integrale Veiligheidscellen inzake radicalisme, extremisme en terrorisme
LTF	Local Task Force
NSIP	Nationaal Strategisch Inlichtingenplan
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
PFCECT	Platform Counter Extremism & Counter Terrorism
PNR	Passenger Name Record
Strategie TER	Strategische nota Extremisme en Terrorisme
Comité R/I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Comité P	Vast Comité van Toezicht op de politiediensten
VSSE	Veiligheid van de Staat
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse