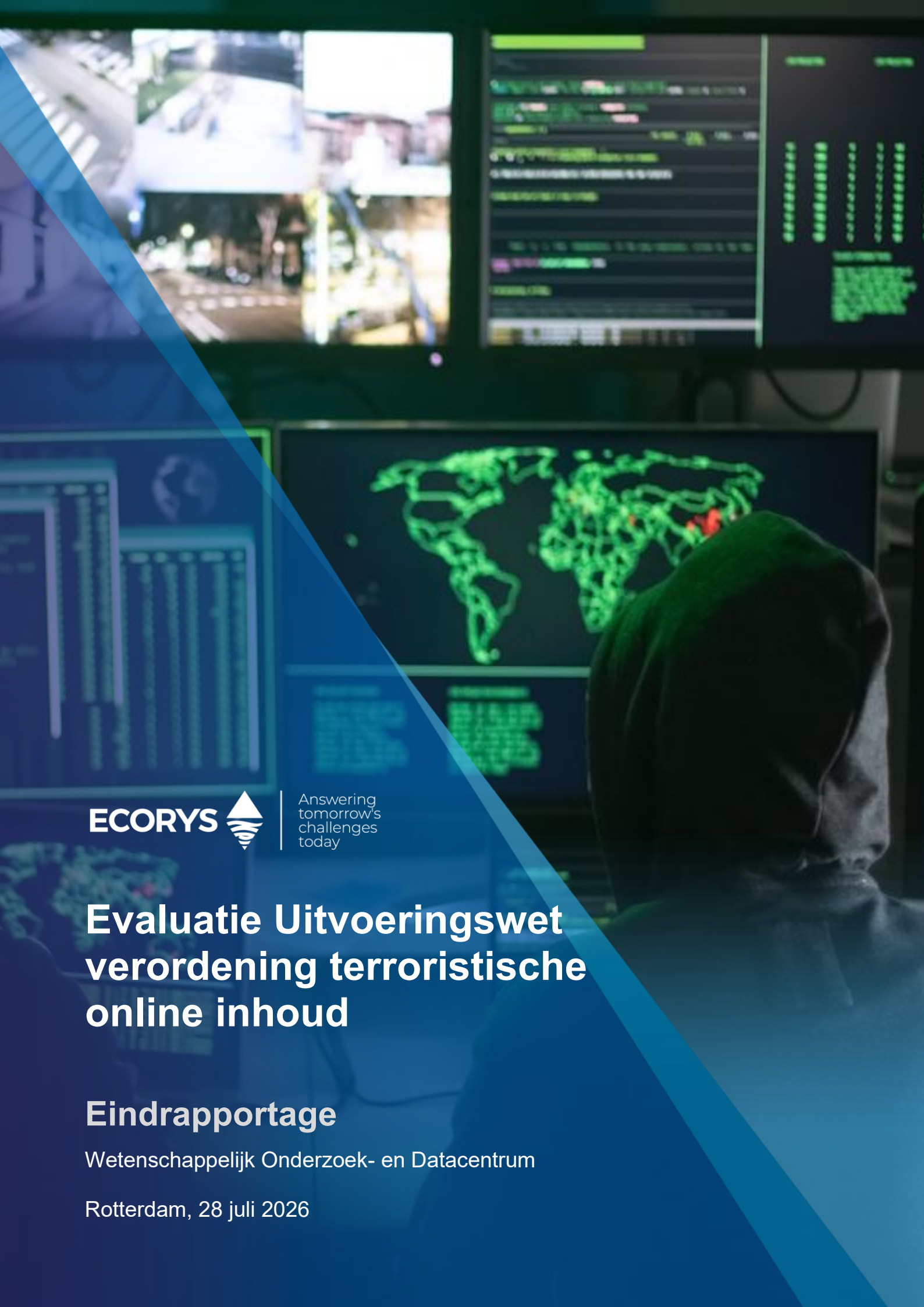


ECORYS

Answering tomorrow's challenges today

Evaluatie Uitvoeringswet verordening terroristische online inhoud

Eindrapportage

Wetenschappelijk Onderzoek- en Datacentrum

Rotterdam, 28 juli 2026

Evaluatie Uitvoeringswet verordening terroristische online inhoud

Eindrapportage

In opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC)

Rotterdam, 28 juli 2026

Auteurs:
Dr. Mike Beke
Gabriëlle op ’t Hoog, MSc
Sabine Hellemons, MSc
Tessa van den Adel, MSc
Dr. Bibi van Ginkel, LLM
Linette de Swart, LLM, MSc

Met dank aan de begeleidingscommissie:
Prof. dr. Richard Rogers, voorzitter (Universiteit van Amsterdam)
Dr. Mariëlle Stel (Universiteit Twente)
Dr. Marieke van Genugten (Radboud Universiteit)
Mr. Dr. Michael Klos (Universiteit Leiden)
Medewerker NCTV (NCTV/JenV)
Drs. Theo van Mullekom (WODC)

Inhoudsopgave

Afkortingen en definities **4**

Samenvatting **7**

1 Aanleiding en methodologie **15**
1.1 Aanleiding 15
1.2 Doel, onderzoeksvragen en afbakening 16
1.3 Methodologie 17
1.4 Leeswijzer 19

2 Achtergrond van de Uitvoeringswet TOI **20**
2.1 Beleidscontext van de Uitvoeringswet TOI 20
2.2 TOI cyclus 27

3 Bevindingen **36**
3.1 Juiste toepassing en naleving van verwijderbevelen 36
3.2 Juridische aspecten van verwijderbevelen 49
3.3 Capaciteit, uitvoerbaarheid en administratieve lasten 58
3.4 Governance en samenwerking 63
3.5 Effectiviteit en impact op online veiligheid 78

4 Conclusies en aanbevelingen **83**
4.1 Conclusies 83
4.2 Aanbevelingen 86

Bijlage I – Bibliografie **89**

Bijlage II – Methodologie **95**
Onderzoeksvragen 95
Methodologisch raamwerk 96

Bijlage III – Respondentenoverzicht **103**

Afkortingen en definities

Afkortingen

ACM	Autoriteit Consument en Markt
AI	Artificiële intelligentie
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AMS-IX	Amsterdam Internet Exchange
ATKM	Autoriteit Online Terroristisch en Kinderpornografisch Materiaal
Awb	Algemene wet bestuursrecht
BKA	Bundeskriminalamt (federale recherchedienst)
BNetzA	Bundesnetzagentur (federaal netwerkagentschap)
CNAM	Coimisiún na Meán (media commissie)
CRM	College voor de Rechten van de Mens
DSA	Digital Services Act (Verordening digitale diensten)
ECP	Electronic Commerce Platform Nederland
EU	Europese Unie
Europol	European Union Agency for Law Enforcement Cooperation
EU-verordening	Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online inhoud
EVRM	Europees Verdrag voor de Rechten van de Mens
FRA	European Union Agency for Fundamental Rights
Fte	Full-time equivalent
HSP	Hosting Service Provider
IRU	Internet Referral Unit
ISF	Internal Security Fund
LIRC	Landelijk Internationaal Rechtshulp Centrum
Ministerie EZK	Ministerie van Economische Zaken en Klimaat
Ministerie JenV	Ministerie van Justitie en Veiligheid
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
NCTS	Nederlandse contraterrorisme strategie
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
NetzDG	Netwerkhandhavingswet
OFP	Organisatie- en Formatieplan
OM	Openbaar Ministerie
OSINT	Open-Source Intelligence
PERCI	Plateforme Européenne de Retraits de Contenus Illégaux sur Internet
Polisen	Polismyndigheten (nationale politie)
SÄPO	Säkerhetspolisen (veiligheidsdienst)
SIENA	Secure Information Exchange Network Application
TOI	Terroristische online inhoud
Uitvoeringswet TOI	Uitvoeringswet verordening terroristische online inhoud
Wpg	Wet politiegegevens
Zbo	Zelfstandig bestuursorgaan

Definities

Borderline content	Materiaal dat niet duidelijk onder de wettelijke definities van terroristische online inhoud of anderszins illegale inhoud valt, maar desalniettemin een ondermijnend effect heeft op democratische waarden en sociale cohesie. Dit type inhoud wordt daarom ook wel aangeduid als ‘awful but lawful’ (schadelijk maar rechtmatig). Borderline content voor de ATKM betreft materiaal wat net niet geclassificeerd kan worden als terroristisch materiaal. Het kan wel dezelfde effecten hebben als content die daar wel onder valt.
Hosting Service Provider	Elke aanbieder van diensten die bestaan uit het opslaan van informatie die door de afnemer van de dienst (oftewel de gebruiker die de content plaatst) wordt verstrekt, ongeacht de vestigingsplaats van de aanbieder, zolang de dienst binnen de EU wordt aangeboden.
PERCI	PERCI is een digitaal platform, ontwikkeld door Europol, dat de veilige en uniforme overdracht van verwijderbevelen en verwijderverzoeken tussen EU-lidstaten en aanbieders van online diensten standaardiseert.
SIENA	Centraal communicatieplatform van Europol dat opsporings-autoriteiten in de EU en partners in staat stelt om op een veilige en snelle manier gevoelige operationele en strategische informatie over criminaliteit uit te wisselen.
Terroristische online inhoud	Verordening (EU) 2021/784 definieert terroristische online inhoud als materiaal dat: • aanzet tot het plegen van terroristische misdrijven; • deze misdrijven aanmoedigt of verdedigt; • instructies geeft voor het plegen van terroristische misdrijven; • bevordert dat mensen deelnemen aan activiteiten van terroristische organisaties; • instructies biedt voor het vervaardigen of gebruiken van explosieven of wapens om terroristische misdrijven te plegen of daar een bijdrage aan te leveren; • een dreiging vormt om terroristische misdrijven te plegen.
Trusted flaggers	*Trusted flaggers* zijn aangewezen organisaties onder de DSA. Zij zijn gespecialiseerd in het detecteren van bepaalde soorten schadelijke online content en hebben de taak dit door te zetten naar online platformen en, indien nodig, toezichthouders.

Verwijderbevel	Verordening (EU) 2021/784 introduceert de mogelijkheid voor bevoegde autoriteiten om een verwijderbevel uit te vaardigen aan aanbieders van hostingdiensten en sancties op te leggen als deze niet worden opgevolgd. Een verwijderbevel verplicht aanbieders van hostingdiensten in de EU om materiaal dat is geïdentificeerd als terroristische online inhoud te verwijderen of ontoegankelijk te maken binnen 60 minuten.
Verwijderverzoek	Een verwijderverzoek (referral) is een formele melding bij een HSP die de aanbieder attent maakt dat het geïdentificeerde materiaal niet voldoet aan de gebruikersvoorwaarden van het platform, in dit geval omdat het terroristisch van aard is, met het verzoek om dit daarom vrijwillig te verwijderen of ontoegankelijk te maken.
Zelfstandig bestuursorgaan	Organisatie die taken van de centrale overheid uitvoert maar niet hiërarchisch onder het gezag van een minister staat.

Samenvatting

Aanleiding, doel en onderzoeksvragen

Om de verspreiding van terroristische online inhoud tegen te gaan, trad in 2022 Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online inhoud (EU-Verordening) in werking. Deze verordening introduceert een kader waarmee bevoegde autoriteiten in EU-lidstaten aanbieders van hostingdiensten (HSPs) kunnen verplichten terroristische online inhoud te verwijderen of ontoegankelijk te maken. Nederland heeft deze verordening geïmplementeerd via de Uitvoeringswet verordening terroristische online inhoud (Uitvoeringswet TOI) en daartoe de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) aangewezen als bevoegde autoriteit.

De Uitvoeringswet TOI dient binnen drie jaar na inwerkingtreding te worden geëvalueerd. Met deze evaluatie wordt invulling gegeven aan deze wettelijke verplichting. De evaluatie heeft twee centrale doelstellingen: het beoordelen van de doeltreffendheid van de Uitvoeringswet TOI en het in kaart brengen van de wijze waarop de wet in de praktijk functioneert. De centrale onderzoeksvraag luidt:

"In hoeverre is de Uitvoeringswet TOI doeltreffend en hoe functioneert de wet, in het bijzonder voor wat betreft de toepassing en werking van de wet in de praktijk, de bestuurlijke constructie waarvoor is gekozen, alsook de balans tussen enerzijds de toepassing van de wet en anderzijds de rechtsstatelijke bescherming van aanbieders van hostingdiensten, internetplatformen en gebruikers van internetinhoud?"

De onderzoeksvraag is uitgewerkt langs vijf onderzoeksthema's:

a. Juiste toepassing en naleving van verwijderbevelen;
b. Juridische aspecten van verwijderbevelen;
c. Capaciteit, uitvoerbaarheid en administratieve lasten;
d. Governance en samenwerking;
e. Effectiviteit en impact op online veiligheid.

Onderzoeksaanpak

De evaluatie is uitgevoerd in de periode van december 2025 tot en met juli 2026 en heeft betrekking op de periode vanaf de inwerkingtreding van de Uitvoeringswet TOI op 1 september 2023 tot en met juni 2026.[1] Om de onderzoeksvragen te beantwoorden, is gebruikgemaakt van verschillende onderzoeksmethoden.

Allereerst is een literatuur- en documentenstudie uitgevoerd naar wetenschappelijke literatuur, beleidsdocumentatie, parlementaire stukken en relevante nationale en internationale publicaties. Daarnaast zijn 28 semigestructureerde interviews gehouden met vertegenwoordigers van de ATKM, Nederlandse overheidsorganisaties, EU instellingen, buitenlandse bevoegde autoriteiten, HSPs, maatschappelijke organisaties en academische experts.

[1] Alleen artikel 13 en 16 van de Uitvoeringswet TOI zijn later, in augustus 2025, in werking getreden. Zie: Ministerie van Justitie (2025), Nota van toelichting, Staatsblad. 2025, 216.

Verder is een zogenoemde rode draad sessie georganiseerd, waarin de werking van de wet en de uitvoering daarvan stap voor stap zijn gereconstrueerd. Tevens zijn casestudies uitgevoerd in Duitsland, Ierland en Zweden; hierbij lag het accent op het in kaart brengen van hoe andere EU-lidstaten de bevoegde autoriteit hebben ingericht. De voorlopige bevindingen zijn ten slotte besproken tijdens een validatieworkshop met betrokken organisaties. De resultaten van deze verschillende onderzoeksmethoden zijn vervolgens met elkaar vergeleken en samengebracht in dit eindrapport.

De Uitvoeringswet TOI in het kort

De Europese verordening en de Uitvoeringswet verordening terroristische online inhoud beogen de verspreiding van terroristische online inhoud te beperken. Centraal staat daarbij het verwijderbevel. Met een verwijderbevel kan een bevoegde autoriteit een HSP verplichten om terroristische online inhoud binnen één uur na ontvangst van het bevel ontoegankelijk te maken. Daarnaast bevat de EU-verordening bepalingen over grensoverschrijdende samenwerking, rechtsbescherming, transparantie, sancties en blootstellingsbesluiten. Via een blootstellingsbesluit kan een HSP die herhaaldelijk met terroristische online inhoud wordt geconfronteerd, worden verplicht om structurele maatregelen te nemen.

In Nederland is de ATKM verantwoordelijk voor de uitvoering van deze taken. De ATKM heeft enerzijds de taak terroristische online inhoud te identificeren en het ontoegankelijk maken daarvan te bevorderen of af te dwingen. Anderzijds heeft zij een bredere signalerende en kennisgerichte functie en is het de bedoeling dat zij kennis en inzichten over ontwikkelingen op het gebied van terroristische online inhoud deelt met relevante partners. De ATKM is daarbij nadrukkelijk geen opsporingsinstantie en houdt zich niet bezig met de vervolging van personen die terroristische content produceren of verspreiden.

Bevindingen

Juiste toepassing en naleving van verwijderbevelen

De Uitvoeringswet TOI wordt in de praktijk zorgvuldig toegepast. De ATKM heeft een gestructureerd werkproces ingericht voor het identificeren, beoordelen en het versturen van verwijderbevelen opdat HSPs terroristische online inhoud ontoegankelijk maken. Terroristische online inhoud wordt hoofdzakelijk geïdentificeerd via handmatige openbrondetectie (OSINT) door gespecialiseerde medewerkers. Geautomatiseerde detectietooling is op dit moment niet beschikbaar, waardoor de detectiecapaciteit grotendeels afhankelijk blijft van handmatige monitoring.

Na identificatie wordt materiaal beoordeeld aan de hand van juridische, inhoudelijke en grondrechtelijke criteria. Daarbij wordt niet alleen gekeken naar de inhoud zelf, maar ook naar de context waarin deze wordt verspreid. De beoordeling vindt in beginsel plaats door meerdere beoordelaars en omvat een expliciete afweging van de vrijheid van meningsuiting. Er komen geen aanwijzingen naar voren voor structurele fouten, het overmatig ontoegankelijk maken van legale inhoud of andere ongewenste neveneffecten.

Tegelijkertijd leidt slechts een deel van de geïdentificeerde content uiteindelijk tot een verwijderbevel. De ATKM schat dat ongeveer driekwart van de gesignaleerde content afvalt omdat de content zich bevindt in een grijs gebied van extremistische of anderszins zorgwekkende uitingen die niet eenduidig onder de wettelijke definitie van terroristische online inhoud vallen of omdat inhoud op het moment dat een verwijderbevel verstuurd kan worden

niet (meer) toegankelijk is (bijv. omdat een bevoegde autoriteit in een andere lidstaat al eerder een bevel heeft verstuurd of omdat HSPs de inhoud zelfstandig ontoegankelijk hebben gemaakt). Hierdoor bestaat er een verschil tussen de bredere online problematiek die stakeholders waarnemen en het deel waarop de Uitvoeringswet TOI daadwerkelijk kan interveniëren.

De naleving van verwijderbevelen door HSPs is hoog. In 2024 en 2025 zijn circa 330 verwijderbevelen uitgevaardigd en vrijwel alle bevelen zijn binnen de wettelijke termijn nageleefd. Wat verder opvalt is dat de ATKM verantwoordelijk is voor 20% van de verwijderbevelen die de bevoegde autoriteiten in de lidstaten in 2024 en 2025 hebben uitgestuurd. Er zijn geen boetes of dwangsommen opgelegd wegens niet-naleving. Ook HSPs beoordelen de uitvoering van verwijderbevelen over het algemeen positief. Wel signaleren zij uitdagingen rond de éénuursregel.

Het voornaamste aandachtspunt bevindt zich niet bij de naleving van verwijderbevelen, maar in de periode die daaraan voorafgaat. Met name de juridische beoordeling, administratieve verwerking en het deconflictieproces[2] met politie nemen tijd in beslag. Hierdoor kan terroristische online inhoud gedurende enige tijd online beschikbaar blijven voordat daadwerkelijk wordt opgetreden.

Daarnaast zijn verschillende onderdelen van het wettelijke instrumentarium nog niet benut. Er zijn tot op heden geen bezwaar- of beroepsprocedures gestart. Ook zijn geen blootstellingsbesluiten uitgevaardigd en is geen gebruikgemaakt van de geschilbeslechtingsprocedure. Hierdoor ontbreekt nog praktijkervaring met een aantal belangrijke onderdelen van het stelsel en is de werking daarvan nog beperkt zichtbaar. Ten aanzien van de effectiviteit van de ATKM is het onbenut laten van de blootstellingsbesluiten met name een gemiste kans.

Juridische aspecten van verwijderbevelen

De uitvoering van de Uitvoeringswet TOI blijft binnen de kaders van de vrijheid van meningsuiting en andere fundamentele rechten. De ATKM hanteert een zorgvuldige beoordelingsprocedure, waarin inhoudelijke, juridische en grondrechtelijke afwegingen expliciet worden meegewogen. Er zijn geen aanwijzingen gevonden voor structurele overblokkering, *chilling effects* of andere onbedoelde neveneffecten voor legale online inhoud.

Tegelijkertijd kent deze conclusie een belangrijke beperking. Tot op heden zijn geen bezwaar- of beroepsprocedures gestart tegen verwijderbevelen van de ATKM. Hierdoor heeft nog geen onafhankelijke rechterlijke toetsing plaatsgevonden van de wijze waarop de wettelijke criteria worden geïnterpreteerd en toegepast.

Een terugkerend aandachtspunt betreft *borderline content*: extremistische of radicaliserende content die wel als zorgwekkend wordt beschouwd, maar niet kwalificeert als terroristische online inhoud. Het huidige mandaat van de ATKM richt zich uitsluitend op terroristische online inhoud, waardoor de organisatie voor dergelijke borderline content geen handelingsgrondslag heeft.

---

[2] Deconflictie is de controle waarbij de ATKM vooraf afstemt met politie of geïdentificeerde online content onderdeel is van een lopend onderzoek, zodat een verwijderbevel geen opsporings- of inlichtingenonderzoek verstoort.

De Uitvoeringswet TOI sluit het gebruik van niet-bindende verwijderverzoeken niet expliciet uit. Over de wenselijkheid van het gebruik van dergelijke verzoeken lopen de opvattingen uiteen. Voorstanders zien mogelijkheden om sneller op te treden tegen terroristische online inhoud, terwijl tegenstanders wijzen op risico's voor de rechtsbescherming en het gevaar dat inhoudelijke afwegingen van de overheid naar private platformen worden verschoven.

Capaciteit, uitvoerbaarheid en administratieve lasten

De ATKM heeft in korte tijd een operationele organisatie opgebouwd en een werkend primair proces ingericht. Tegelijkertijd blijft de organisatie in belangrijke mate afhankelijk van een beperkte groep gespecialiseerde medewerkers en wordt een aanzienlijk deel van het werk nog handmatig uitgevoerd.

Een belangrijk aandachtspunt is het ontbreken van geautomatiseerde detectietooling. Hierdoor is de detectiecapaciteit beperkt en blijft de organisatie sterk afhankelijk van handmatige monitoring. Daarnaast is de ruimte voor aanvullende activiteiten zoals trendanalyse, kennisontwikkeling en het benutten van aanvullende instrumenten beperkt. De huidige personele en technische capaciteit sluit niet volledig aan bij de ambities en verantwoordelijkheden van de organisatie.

Ook voor HSPs brengt de wet uitvoeringslasten met zich mee. Dit geldt in het bijzonder voor de verplichting om verwijderbevelen binnen één uur op te volgen. Grote internationale platformen beschikken doorgaans over uitgebreide systemen en processen om aan deze verplichting te voldoen. Voor kleinere aanbieders kan dit echter een grotere uitdaging vormen. Het onderzoek laat tevens zien dat aanbieders zonder Europese vestiging of vertegenwoordiging relatief moeilijk bereikbaar zijn en dat handhaving richting deze categorie beperkt effectief is.

Governance en samenwerking

De keuze om de ATKM als zelfstandig bestuursorgaan (zbo) vorm te geven, wordt over het algemeen positief beoordeeld. De onafhankelijke positie van de organisatie stelt de ATKM in staat een constructieve samenwerkingsrelatie met HSPs op te bouwen. Bovendien heeft de status van de ATKM als zbo bijgedragen aan de ontwikkeling van de organisatie als expert op het gebied van terroristisch materiaal. Ook internationaal heeft de organisatie in korte tijd een sterke positie opgebouwd. Verschillende buitenlandse partners beschrijven de ATKM als een deskundige, proactieve en goed samenwerkende bevoegde autoriteit.

Tegelijkertijd brengt deze inrichting ook beperkingen met zich mee. Omdat de ATKM geen opsporingsinstantie is, blijft zij voor bepaalde werkzaamheden afhankelijk van de politie. Dit speelt onder meer bij deconflictie, informatie-uitwisseling en de toegang tot Europol-systemen zoals SIENA. De voordelen van onafhankelijkheid gaan daarmee gepaard met bepaalde operationele afhankelijkheden, die ook van invloed zijn op de efficiëntie van de ATKM.

De samenwerking met nationale ketenpartners, buitenlandse bevoegde autoriteiten, Europol en HSPs wordt overwegend positief beoordeeld.

Effectiviteit en impact op online veiligheid

De evaluatie laat zien dat de Uitvoeringswet TOI aantoonbaar effect sorteert op het niveau van individuele interventies. Wanneer terroristische online inhoud wordt geïdentificeerd en een

verwijderbevel wordt uitgevaardigd, wordt deze inhoud in vrijwel alle gevallen ontoegankelijk gemaakt. Op dit niveau kan de wet als effectief worden beschouwd.

Het is echter aanzienlijk moeilijker om uitspraken te doen over de impact op het bredere fenomeen van terroristische online inhoud of op de nationale veiligheid. Een nulmeting ontbreekt, waardoor niet kan worden vastgesteld hoe groot het totale probleem is of hoeveel materiaal door de wet wordt geraakt. Daarnaast verschuift terroristische content regelmatig tussen platformen en wordt een deel van de activiteit verplaatst naar besloten of versleutelde omgevingen, die buiten de reikwijdte van de EU-verordening vallen.

Daar komt bij dat de ATKM, net als andere bevoegde autoriteiten in Europa, waarschijnlijk slechts een deel van de online beschikbare terroristische content daadwerkelijk detecteert. Hierdoor kan geen directe relatie worden gelegd tussen de werking van de wet en een algemene afname van terroristische online inhoud op internet als geheel. Wel is het aannemelijk dat de wet een bijdrage levert aan het verminderen van de zichtbaarheid en beschikbaarheid van specifieke vormen van terroristische online inhoud.

Conclusies

De evaluatie laat zien dat de Uitvoeringswet TOI in de praktijk grotendeels functioneert zoals beoogd. De ATKM heeft in relatief korte tijd een werkende organisatie opgebouwd voor de identificatie, beoordeling en het ontoegankelijk maken van terroristische online inhoud. De organisatie heeft hiervoor een gestructureerd proces ingericht, waarin juridische zorgvuldigheid, grondrechtelijke afwegingen en expertise centraal staan.

Verwijderbevelen worden zorgvuldig voorbereid en vrijwel altijd binnen de termijn van 1 uur nageleefd door HSPs. De ATKM levert bovendien een aanzienlijke bijdrage aan het totaal aantal verstuurde verwijderbevelen. Er zijn geen aanwijzingen voor systematische schendingen van grondrechten, het overmatig ontoegankelijk maken van legale inhoud of andere onbedoelde neveneffecten van de toepassing van de wet. Tegelijkertijd heeft nog geen onafhankelijke rechterlijke toetsing plaatsgevonden, omdat tot op heden geen bezwaar- of beroepsprocedures zijn gestart en het blootstellingsbesluit nog niet is uitgevoerd.

De werking van de wet wordt in belangrijke mate begrensd door factoren die samenhangen met de inrichting van het instrumentarium, de beschikbare capaciteit en de kenmerken van het online landschap waarop de wet van toepassing is. Zo rust de uitvoering van de Uitvoeringswet TOI vrijwel volledig op één instrument, namelijk het verwijderbevel. Een ander instrument waarin de wet voorziet, het blootstellingsbesluit, is gedurende de onderzochte periode niet ingezet. Dit instrument kan in potentie bijdragen aan aanpassingen door HSPs die meer structurele resultaten opleveren. Dit instrument wordt vooralsnog niet ingezet vanwege het ontbreken van een helder en uniform kader voor de inzet van dit instrument en het beoordelen van de genomen (specifieke) maatregelen. . Verder blijkt dat de Uitvoeringswet TOI het gebruik van niet-bindende verwijderverzoeken niet expliciet uitsluit, maar dat de opvattingen over de wenselijkheid hiervan uiteenlopen vanwege de afweging tussen effectiviteit enerzijds en rechtsbescherming anderzijds.

Daarnaast wordt de effectiviteit van de wet mede begrensd door de manier waarop terroristische online inhoud wordt gedetecteerd. Detectie vindt handmatig plaats. Hierdoor is

het aannemelijk dat slechts een deel van de beschikbare terroristische online inhoud daadwerkelijk in beeld komt.

Bovendien valt een aanzienlijk deel van de door de ATKM gedetecteerde inhoud uiteindelijk buiten het bereik van de wet. Een deel bevindt zich in een zogenoemd grijs gebied van extremistische, radicaliserende of anderszins zorgwekkende content die echter niet eenduidig onder de wettelijke definitie van terroristische online inhoud valt. Een ander deel van de content wordt reeds ontoegankelijk gemaakt voordat de ATKM een verwijderbevel kan versturen (bijv. omdat een bevoegde autoriteit in een andere lidstaat al eerder een bevel heeft verstuurd of omdat HSPs de inhoud zelfstandig ontoegankelijk hebben gemaakt). Hierdoor ontstaat een verschil tussen de bredere online problematiek die door verschillende stakeholders wordt waargenomen en het deel waarop de Uitvoeringswet TOI daadwerkelijk kan interveniëren. Over in hoeverre de ATKM hierop zou moeten kunnen acteren, lopen de meningen uiteen.

Ook de gekozen bestuurlijke inrichting kent zowel voordelen als beperkingen. De keuze voor de ATKM als zelfstandig bestuursorgaan heeft bijgedragen aan de onafhankelijkheid van de besluitvorming en heeft de organisatie in staat gesteld een constructieve relatie op te bouwen met HSPs. De ATKM heeft zich bovendien ontwikkeld tot een internationaal gewaardeerde partner en vervult een actieve rol in Europese initiatieven gericht op harmonisatie van de aanpak van terroristische online inhoud. Tegelijkertijd leidt de keuze voor een bestuurs-rechtelijke toezichthouder ertoe dat de ATKM voor bepaalde werkzaamheden afhankelijk blijft van anderen, in het bijzonder de politie. Dit geldt onder andere voor deconflictie, toegang tot bepaalde informatiebronnen en internationale informatie-uitwisseling. Hoewel deze samen-werking in de praktijk goed verloopt, heeft zij invloed op de snelheid en efficiëntie van de uitvoering.

Ten aanzien van de doeltreffendheid van de wet ontstaat een genuanceerd beeld. Op het niveau van individuele interventies kan worden vastgesteld dat de wet werkt: terroristische online inhoud wordt geïdentificeerd, verwijderbevelen worden uitgevaardigd en de betreffende inhoud wordt in vrijwel alle gevallen binnen de gestelde termijn ontoegankelijk gemaakt. Het is echter niet mogelijk om vast te stellen in welke mate de wet heeft geleid tot een bredere vermindering van terroristische online inhoud of tot een aantoonbare verbetering van de nationale veiligheid. De omvang van het totale fenomeen is onbekend, een nulmeting ontbreekt en een deel van de online activiteiten vindt plaats in besloten of versleutelde omgevingen die buiten de reikwijdte van de wet vallen.

Aanbevelingen

Op basis van de bevindingen uit deze evaluatie komen verschillende aandachtspunten naar voren voor de verdere ontwikkeling van de Uitvoeringswet TOI en de uitvoering daarvan. Deze zijn opgesplitst in aanbevelingen voor het Ministerie van Justitie en Veiligheid en de regering en aanbevelingen voor de ATKM.

Aanbevelingen voor het Ministerie van Justitie en Veiligheid en de regering:

1. Heroverweeg de geschilbeslechtingsprocedure van artikel 16 Uitvoeringswet TOI

Nederland is de enige lidstaat die een aanvullende geschilbeslechtingsprocedure heeft opgenomen in de implementatiewet. De procedure is tot op heden niet benut. Bovendien beschouwt de ATKM haar dubbele rol als complex: als autoriteit neemt zij

blootstellingsbesluiten en als geschillenbeslechter bestaat de kans dat zij (de acties die voortvloeien uit) de besluiten moet toetsen. Daarnaast verwacht de ATKM dat de toepassing ervan capaciteitsintensief zal zijn. Gelet op het feit dat gebruikers via een bestuursrechteljke procedure en via de DSA al adequate rechtsbescherming genieten, verdient heroverweging, dan wel vereenvoudiging, van deze procedure aanbeveling.

2. Onderzoek de beleidsmatige haalbaarheid van een verwijderverzoek van TOI als aanvullend instrument voor de ATKM

Nederland is een van de weinige EU-lidstaten die uitsluitend het bindende verwijderbevel gebruikt. Veel lidstaten werken ook met niet-bindende verzoeken en grijpen pas naar een bevel bij niet-naleving. Een verwijderverzoek verkort de doorlooptijd, verlaagt de administratieve last en geeft de HSP meer tijd om te reageren. De juridische ruimte voor een verwijderverzoek ten aanzien van TOI-content is in de huidige wet aanwezig. De inzet van verzoeken naast bevelen kent voor- en nadelen en op basis hiervan is een zorgvuldige afweging ten aanzien van het al dan niet inzetten van verzoeken op zijn plaats.

3. Onderzoek de juridische haalbaarheid van een ruimer mandaat voor de ATKM om ook te ageren tegen borderline content

Verzoeken kunnen op dit moment door de ATKM expliciet niet op *borderline content* ingezet worden. Indien dit wenselijk wordt geacht, zouden andere routes verkend moeten worden, waaronder uitbreiding van het wettelijk kader of het aanmerken van de ATKM als *DSA trusted flagger*.

4. Investeer in de technische en personele randvoorwaarden voor de ATKM

Het huidige budget en de huidige bezetting zijn onvoldoende voor een ATKM die ook op de middellange termijn effectief kan opereren. De automatisering en financiering van geautomatiseerde detectieinstrumenten, een bezetting die continuïteitsrisico's beperkt en adequate huisvesting die rekening houdt met de bijzondere aard van het werk zijn geen luxe maar randvoorwaarden voor effectieve wetsuitvoering.

5. Faciliteer de toegang van de ATKM tot relevante Europol-informatie

De informatiepositie van de ATKM wordt begrensd door het ontbreken van directe toegang tot Europol-producten, zoals Check the Web en *hashlists*.[3] In afstemming met Europol en de politie verdient het aanbeveling om afspraken te maken over de gestructureerde en tijdige aanlevering van deze informatie aan de ATKM, zonder hierbij de principiële scheiding tussen toezicht (ATKM) en opsporing (politie) uit het oog te verliezen.

Aanbevelingen aan de ATKM

6. Zet in op het operationaliseren van geautomatiseerde detectietooling als strategische prioriteit

Handmatige detectie is de voornaamste bottleneck in het primaire proces. Geautomatiseerde detectie is niet alleen een efficiëntiewinst, maar ook een voorwaarde voor schaalbaarheid (onder andere meer detectie, maar ook bijvoorbeeld detectie buiten kantooruren). De ATKM dient het maatwerktraject voor detectiesoftware te prioriteren en waar mogelijk interimoplossingen te benutten die de periode tot implementatie op korte termijn overbruggen.

7. Ontwikkel een kader voor de inzet van het blootstellingsbesluit

[3] Hashlists zijn digitale vingerafdrukken van reeds geclassificeerd materiaal.

Het blootstellingsbesluit is bij uitstek een instrument dat structurele gedragsverandering bij HSPs kan afdwingen. De ATKM dient, bij voorkeur in EU-verband, een werkwijze te ontwikkelen voor de toepassing ervan, inclusief criteria voor wanneer een blootstellingsbesluit proportioneel is en hoe de naleving van de inspanningsverplichting kan worden beoordeeld. De ATKM wordt aangemoedigd om op Europees niveau voor opheldering ten aanzien van de inzet van dit instrument te verzoeken.

8. Structureer de terugkoppeling van trendkennis naar ketenpartners

De ATKM bouwt waardevolle kennis op over terroristische online inhoud, narratieven en patronen. Deze kennis vloeit nog onvoldoende structureel terug naar partners als de nationale politie en de NCTV. Het inrichten van periodieke rapportages of feedbackmechanismen versterkt de positie van de ATKM in de keten en vergroot de bredere maatschappelijke waarde van haar werk.

9. Vergroot de zichtbaarheid van het meldpunt en analyseer de instroom

Het openbare meldpunt voor derden (zoals burgers, maatschappelijke organisaties of wetenschappers) van de ATKM[4] is in november 2025 geopend, maar hierover is tot op heden (juni 2026) nog nauwelijks gecommuniceerd. Actievere bekendmaking van het meldpunt en het opzetten van een analysekader voor de instroom, ook om te leren van meldingen die niet als TOI kwalificeren, versterkt zowel het detectievermogen als de leeropgave van de ATKM.

[4] Het meldpunt van de ATKM is beschikbaar via deze link.

1 Aanleiding en methodologie

1.1 Aanleiding

Terrorisme vormt een ernstige bedreiging voor de Europese veiligheid. Recente dreigingsbeelden tonen aan dat jihadistisch extremisme, rechts- en (in mindere mate) linksextremisme zich blijven ontwikkelen en manifesteren, ook in de digitale ruimte.[5] Er bestaan in Nederland ook toenemende zorgen over nihilistisch extremisme (online).[6]

HSPs worden door extremistische groeperingen misbruikt om ideologieën te verspreiden, leden te rekruteren, aanslagen voor te bereiden en financiële middelen te vergaren.[7] Daarnaast wordt er ook gebruikgemaakt van versleutelde communicatiekanalen, zoals Telegram, Whatsapp, Signal en andere alternatieve platformen.[8] Specifiek voor de financiering van terroristische activiteiten worden *crowdfunding*, het verkopen van merchandise en cryptovaluta ingezet.[9]

In 2022 is de Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online inhoud (hierna: EU-verordening) in werking getreden.[10] Deze verordening geeft bevoegde toezichthoudende autoriteiten in de lidstaten onder andere de mogelijkheid om op te treden tegen terroristisch materiaal online en daarmee tracht de Europese Commissie bij te dragen aan het bestrijden van terrorisme. De EU-verordening is in Nederland vertaald naar de Uitvoeringswet Terroristische Online inhoud (hierna: Uitvoeringswet TOI).[11] In Nederland is de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (hierna: ATKM) aangewezen als bevoegde toezichthoudende autoriteit.[12] Zie voor een uitgebreidere introductie van de EU-verordening, de Uitvoeringswet TOI en de ATKM hoofdstuk 2.

Conform artikel 21 van de Uitvoeringswet TOI moet de Minister van Justitie en Veiligheid binnen drie jaar na de inwerkingtreding van de wet een evaluatie delen met de Tweede Kamer.[13] Met deze evaluatie wordt de minister in staat gesteld om aan deze opdracht te voldoen.

---

5 Europol (2025), EU Terrorism Situation and Trend Report (TE-SAT); NCTV (2025), Dreigingsbeeld Terrorisme Nederland 2025; AIVD (2026), Jaarverslag 2025.

6 NCTV (2026), Dreigingsbeeld Terrorisme Nederland.

7 FRA (2026), Regulating online terrorist content – Balancing public safety and fundamental rights; Europol (2025), EU Terrorism Situation and Trend Report (TE-SAT).

8 AIVD (2025), Een web van haat - De online grip van extremisme en terrorisme op minderjarigen; Europol (2024), Online Jihadist Propaganda - 2023 in review.

9 Zie bijvoorbeeld: Visser, R. (2024), Crowdfunding conspiracists: grassroots giving to January 6 participants.

10 Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online inhoud.

11 Uitvoeringswet TOI trad op 1 september 2023 in werking. Artikelen 13 en 16 traden later in werking, namelijk in augustus 2025.

12 Tweede Kamer (2022), Memorie van toelichting: Uitvoeringswet verordening terroristische online-inhoud, 36 138, nr. 3.

13 Tweede Kamer (2022), Verslag plenair debat: Uitvoeringswet verordening terroristische online-inhoud. 36 138, nr. 6.

1.2 Doel, onderzoeksvragen en afbakening

Deze evaluatie kent twee doelstellingen, namelijk: het evalueren van de doeltreffendheid van de Uitvoeringswet TOI en het in kaart brengen van haar effecten in de praktijk. Hierbij wordt ook aandacht besteed aan de keuze voor de ATKM als bevoegde toezichthoudende autoriteit, de keuze voor de ATKM als zbo en de balans tussen de toepassing van de Uitvoeringswet TOI en de rechtstatelijke bescherming van aanbieders en gebruikers van online inhoud. De concrete onderzoeksvraag luidt:

'In hoeverre is de Uitvoeringswet TOI doeltreffend en hoe functioneert de wet, in het bijzonder voor wat betreft de toepassing en werking van de wet in de praktijk, de bestuurlijke constructie waarvoor is gekozen, alsook de balans tussen enerzijds de toepassing van de wet en anderzijds de rechtsstatelijke bescherming van aanbieders van hostingdiensten en internetplatformen en gebruikers van internetinhoud?'

Deze vraag valt uiteen in vijf thema's en subvragen:

1. Juiste toepassing en naleving van verwijderbevelen
   a. Op welke wijze identificeert de ATKM terroristische online inhoud?
   b. Hoe frequent worden verwijderbevelen uitgevaardigd? Zijn er hierbij trends te ontwaren?
   c. In welke mate geven hostingdiensten en internetplatformen daadwerkelijk en tijdig opvolging aan verwijderbevelen (inclusief de één-uursregel)?
   d. Wat zijn de ervaringen van hostingdiensten en internetplatformen met het proces rondom bevelen en rondom bezwaar- en beroepsprocedures?
   e. Wordt er in de praktijk gebruikgemaakt van bezwaar of beroep? Hoe vaak en met welk resultaat?
   f. Wordt er in de praktijk gebruikgemaakt van de mogelijkheid tot blootstellingsbesluit en wat zijn de verklarende factoren?
   g. Hoe wordt de mogelijkheid tot geschilbeslechting ervaren?

2. Juridische aspecten van verwijderbevelen
   a. In hoeverre valt de reikwijdte van verwijderbevelen binnen de kaders van de in Nederland beschermde grondrechten, met name de vrijheid van meningsuiting?
   b. Zijn er aanwijzingen van *chilling effects* of andere onbedoelde neveneffecten op toelaatbare online inhoud?
   c. Is het wenselijk dat de ATKM ook verwijderverzoeken kan uitvaardigen? Biedt het huidige wettelijke kader ruimte voor de ATKM om ook verwijderverzoeken te doen?
   d. Wordt de balans tussen effectiviteit en rechtsstatelijke bescherming in voldoende mate geborgd?

3. Capaciteit, uitvoerbaarheid en administratieve lasten
   a. Zijn de personele, juridische en technische middelen van de ATKM toereikend voor een effectieve uitvoering van haar taken en bevoegdheden?
   b. In hoeverre ervaren de ATKM of ketenpartners knelpunten in de capaciteit, uitvoerbaarheid of administratieve lasten (of anderszins) bij de Uitvoeringswet TOI?
   c. Wordt de uitvoerbaarheid van de verplichtingen als werkbaar ervaren door hostingdiensten en internetplatformen?

4. Governance en samenwerking
   a. Hoe werkt de keuze voor ATKM als zelfstandig bestuursorgaan door in een effectieve en efficiënte uitvoering van de TOI? In hoeverre zou de ATKM haar wettelijke taken en bevoegdheden (met name ten aanzien van internationale politiesamenwerking en toegang tot informatie) anders kunnen uitvoeren als ze een opsporingsinstantie zou zijn?
   b. Hoe functioneert de samenwerking tussen de ATKM en nationale actoren (zoals politie, Openbaar Ministerie, toezichthouders)?
   c. Hoe functioneert de samenwerking met de buitenlandse bevoegde autoriteiten onder de EU-verordening?
   d. Worden internationale verplichtingen en samenwerkingsstructuren effectief benut?
   e. Welke invloed heeft het samenvoegen van de TOI-taak met de KP-taak binnen de ATKM op de uitvoering van de TOI-taak door de ATKM?

5. Effectiviteit en impact op online veiligheid
   a. Heeft de Uitvoeringswet TOI bijgedragen aan een aantoonbare vermindering van de beschikbaarheid van terroristische online inhoud?
   b. Is het waarschijnlijk dat de Uitvoeringswet TOI heeft bijgedragen aan verbetering van de (online) veiligheid in het kader van nationale veiligheid en terrorismebestrijding?
   c. Zijn aanpassingen in de wetgeving of uitvoering aan te raden om de effectiviteit van de Uitvoeringswet TOI te verbeteren. Zo ja, welke aanpassingen?

De evaluatie is uitgevoerd in de periode van december 2025 tot en met juli 2026. De evaluatie omvat de periode vanaf de inwerkingtreding van de Uitvoeringswet TOI op 1 september 2023 tot en met juni 2026.

1.3 Methodologie

De methodologische basis van deze evaluatie bestaat uit drie samenhangende analytische instrumenten: een interventielogica, een evaluatiematrix en een uitwerking van de TOI cyclus.

De interventielogica brengt in kaart welke problematiek de Uitvoeringswet TOI beoogt te adresseren, welke instrumenten hiervoor beschikbaar zijn en welke resultaten en effecten daarmee worden beoogd. Op basis hiervan is een evaluatiematrix opgesteld waarin de onderzoeksvragen zijn vertaald naar beoordelingscriteria, indicatoren en informatiebronnen. De interventielogica en evaluatiematrix vormen daarmee het kader voor de dataverzameling en analyse.

Daarnaast is een TOI-cyclus ontwikkeld, die de verschillende processtappen binnen de uitvoering van de wet beschrijft; van het signaleren van terroristische online inhoud tot en met het opleggen van verwijderbevelen en eventuele bezwaar- en beroepsprocedures. Deze cyclus fungeerde als rode draad gedurende het onderzoek en werd gebruikt om de praktische werking van de wet inzichtelijk te maken en knelpunten in de uitvoering te identificeren.

Er zijn verschillende activiteiten uitgevoerd om de evaluatie uit te voeren. Deze activiteiten worden hieronder kort beschreven; een uitgebreide beschrijving is opgenomen in bijlage II.

Literatuur- en documentenstudie

De literatuur- en documentenstudie omvat verschillende typen bronnen. Zo zijn onder andere wet- en regelgeving, parlementaire stukken, beleidsdocumenten, jaarverslagen, transparantierapporten en relevante wetenschappelijke literatuur geanalyseerd. Voor de systematische analyse van de verzamelde documentatie is vervolgens een codeboek ontwikkeld, zodat op transparante, consistente en reproduceerbare wijze gecodeerd kan worden in Atlas.ti, een analysesoftware die kwalitatieve analyse ondersteunt. Zie bijlage I voor een overzicht van alle geraadpleegde bronnen.

Rode draad sessie

In het begin van het onderzoek (januari 2026) is een rode draad sessie georganiseerd met partijen die nauw betrokken zijn bij de uitvoering van de wet. Aan de hand van fictieve casussen is de TOI-cyclus doorlopen en zijn het proces alsook knelpunten geïdentificeerd. De opbrengsten van deze sessie zijn gebruikt voor de verdere uitwerking van het onderzoek en de ontwikkeling van de interviewleidraden.

Semigestructureerde interviews

De semigestructureerde interviews zijn uitgevoerd met als doel de inzichten uit de literatuur- en documentenstudie te valideren en waar nodig te verdiepen en aan te vullen. Aan de hand van deze interviews is nagegaan in hoeverre de bevindingen uit het literatuuronderzoek herkenbaar zijn in de praktijk en welke aanvullende perspectieven en ervaringen stakeholders hierbij kunnen bieden. Daarnaast waren de interviews gericht op de werking van de wet in de praktijk, ervaren knelpunten, de effectiviteit van het instrumentarium en mogelijke verbeteringen. In totaal zijn 28 stakeholders geïnterviewd. Een overzicht van de gesprekken en de respondenten is te vinden in bijlage III.

Casestudy

Er zijn drie casestudy's uitgevoerd. Deze hadden tot doel de Nederlandse uitvoeringspraktijk in een EU-perspectief te plaatsen. Duitsland, Ierland en Zweden zijn geselecteerd omdat deze lidstaten verschillende modellen hanteren voor de uitvoering van de EU-verordening en daardoor inzicht bieden in variaties in toezicht, handhaving en samenwerking met HSPs. De casestudy's richten zich op een institutionele inrichting, de toepassing van het instrumentarium en ervaringen met de uitvoering van de EU-verordening. De casestudy's zijn uitgevoerd op basis van literatuur- en documentenstudie en interviews met relevante partijen in de betreffende lidstaten.

Validatieworkshop

De voorlopige onderzoeksbevindingen zijn besproken tijdens een validatiesessie met betrokken partijen. Deze sessie had als doel de feitelijke juistheid, herkenbaarheid en

volledigheid van de bevindingen te toetsen. Een overzicht van de partijen die aanwezig waren bij de sessie is te vinden in bijlage III.

Resultaten uit bovenstaande dataverzamelingsmethoden zijn getrianguleerd en in dit rapport verwerkt. In de volgende hoofdstukken wordt in voetnoten verwezen naar onderliggende bronnen, interviews, sessies of workshops. Inzichten uit casestudy's zijn verwerkt in tekst-vakken.

1.4 Leeswijzer

In het volgende hoofdstuk wordt de Uitvoeringswet TOI alsook de TOI-cyclus nader toegelicht. In hoofdstuk 3 worden bevindingen gepresenteerd en wordt antwoord gegeven op ieder van de subvragen. Conclusies en aanbevelingen worden in hoofdstuk 4 gepresenteerd. In de bijlagen zijn de geraadpleegde literatuur opgenomen en wordt een uitgebreide beschrijving van de toepaste methodologie gepresenteerd.

2 Achtergrond van de Uitvoeringswet TOI

2.1 Beleidscontext van de Uitvoeringswet TOI

EU-Verordening inzake het tegengaan van de verspreiding van terroristische online inhoud

Op EU-niveau wordt sinds 2015 gewerkt aan het aanpakken van terroristisch online materiaal.[14] In 2015 werd de online component van terrorisme en extremisme opgenomen in het beleid.[15] Daarnaast is het EU Internet Forum opgericht, waar lidstaten, Europol en grote techbedrijven samenkomen om, onder andere, de verspreiding van terroristische online inhoud tegen te gaan.[16] De focus lag lang grotendeels op vrijwillige samenwerking en het gebruik of opleggen van niet-juridische maatregelen. Het vrijwillige karakter beperkte echter zowel de reikwijdte als de afdwingbaarheid van de maatregelen.[17] Dit vormde daarom aanleiding voor het opstellen van bindende wetgeving.

In 2022 is de Verordening (EU) 2021/784 inzake het tegengaan van de verspreiding van terroristische online inhoud (hierna: EU-verordening) in werking getreden.[18] De EU-verordening heeft als doel te zorgen voor de goede werking van de digitale eengemaakte markt in een open en democratische samenleving, door misbruik van hostingdiensten voor terroristische doeleinden tegen te gaan en bij te dragen tot de openbare veiligheid in de Unie. De werking van de digitale eengemaakte markt moet worden verbeterd door aanbieders van hostingdiensten meer rechtszekerheid te bieden, het vertrouwen van de gebruikers in de online-omgeving te vergroten en de waarborgen voor de vrijheid van meningsuiting, inclusief de vrijheid om inlichtingen of denkbeelden te ontvangen en door te geven in een open en democratische samenleving, evenals de waarborgen voor de vrijheid en het pluralisme van de media, solider te maken.[19] De EU-verordening introduceert hiervoor een aantal kerninstrumenten en verplichtingen. Tabel 2.1 geeft een overzicht van de voornaamste wetsartikelen van de EU-verordening in het kader van dit onderzoek.

Tabel 2.1 Voornaamste wetsartikelen van de EU-verordening in het kader van dit onderzoek

Wetsartikel	Uitleg op hoofdlijnen
Artikel 3. Verwijderbevelen	De bevoegde autoriteit van elke lidstaat heeft de bevoegdheid om een verwijderingsbevel uit te vaardigen op grond waarvan aanbieders van hostingdiensten terroristische inhoud moeten verwijderen of de toegang daartoe in alle lidstaten moeten blokkeren (artikel 3 lid 1).

[14] In deze paragrafen worden alleen de maatregelen of ontwikkelingen besproken die ingaan op de digitale component in de bestrijding van terrorisme en extremisme.
[15] Europese Commissie (2026), Counter-terrorism and radicalisation.
[16] Europese Commissie (2026), EU Internet Forum.
[17] Europese Commissie (2018), Impact Assessment accompanying in the document Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online; Tweede Kamer (2022), Memorie van toelichting: Uitvoeringswet verordening terroristische online-inhoud, 36 138, nr. 3
[18] Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online inhoud.
[19] Preambule 1, Verordening (EU) 2021/784.

Wetsartikel	Uitleg op hoofdlijnen
Artikel 4. Procedure voor grensoverschrijdende verwijderbevelen	Met inachtneming van artikel 3 dient de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd, indien de aanbieder van hostingdiensten geen hoofdvestiging of wettelijke vertegenwoordiger heeft in de lidstaat van die bevoegde autoriteit, tegelijkertijd een afschrift van het verwijderingsbevel in bij de bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft (artikel 4 lid 1).
Artikel 5. Specifieke maatregelen	Een aanbieder van hostingdiensten die aan terroristische inhoud als bedoeld in lid 4 is blootgesteld, neemt, voor zover van toepassing, in zijn algemene voorwaarden bepalingen op om het misbruik van zijn diensten voor de verspreiding van terroristische inhoud onder het publiek tegen te gaan, en hij past die bepalingen toe. Dit doet hij op zorgvuldige, evenredige en niet-discriminerende wijze, met inachtneming onder alle omstandigheden van de grondrechten van de gebruikers, en met name rekening houdend met het fundamentele belang van de vrijheid van meningsuiting en van informatie in een open en democratische samenleving, teneinde te voorkomen dat materiaal dat geen terroristische inhoud uitmaakt, wordt verwijderd (artikel 5 lid 1). Een aanbieder van hostingdiensten die aan terroristische inhoud is blootgesteld als bedoeld in lid 4, neemt specifieke maatregelen om zijn diensten te beschermen tegen de verspreiding van terroristische inhoud onder het publiek (artikel 5 lid 2). De EU-Verordening legt verschillende opties voor specifieke maatregelen neer in artikel 5 lid 2.
Artikel 7. Transparantie-verplichtingen voor aanbieders van hostingdiensten	Een aanbieder van hostingdiensten die op grond van deze verordening in een bepaald kalenderjaar maatregelen heeft genomen of heeft moeten nemen om de verspreiding van terroristische inhoud tegen te gaan, maakt een transparantieverslag openbaar over de maatregelen die in die periode zijn genomen. Hij publiceert dat verslag vóór 1 maart van het volgende jaar (artikel 7 lid 2).
Artikel 9. Bezwaar-en beroepsprocedure	Aanbieders van hostingdiensten die een op grond van artikel 3, lid 1, uitgevaardigd verwijderingsbevel, een besluit op grond van artikel 4, lid 4, of een besluit op grond van artikel 5, lid 4, lid 6 of lid 7, hebben ontvangen, hebben recht op een doeltreffende voorziening in rechte (Artikel 9 lid 1). Aanbieders van inhoud die na een verwijderingsbevel verwijderd is of waartoe de toegang na een verwijderingsbevel geblokkeerd is, hebben recht op een doeltreffende voorziening in rechte (artikel 9 lid 2).
Artikel 18. Sancties	De lidstaten stellen voorschriften vast ten aanzien van de sancties die van toepassing zijn op inbreuken op deze verordening door aanbieders van hostingdiensten, en nemen alle nodige maatregelen om ervoor te zorgen dat die sancties worden uitgevoerd (artikel 18 lid 1).
Artikel 12. Aanwijzing van bevoegde autoriteiten	Elke lidstaat wijst de bevoegde autoriteit of autoriteiten aan voor a) het uitvaardigen van verwijderingsbevelen op grond van artikel 3, b) het toetsen van verwijderingsbevelen op grond van artikel 4, c)

Wetsartikel	Uitleg op hoofdlijnen
	het toezien op de uitvoering van specifieke maatregelen op grond van artikel 5 en d) het opleggen van sancties op grond van artikel 18 (artikel 12 lid 1).

Centraal in de EU-verordening staat het verwijderbevel, waarmee bevoegde autoriteiten HSPs kunnen verplichten om terroristische online inhoud binnen één uur ontoegankelijk te maken. Met name de toepassing van deze bevoegdheid in grensoverschrijdende situaties vormde een belangrijk discussiepunt tijdens de totstandkoming van de EU-verordening.

Grensoverschrijdende verwijderbevelen
Artikel 4 van de EU-verordening maakt het mogelijk dat een lidstaat een verwijderbevel rechtstreeks richt aan een HSP gevestigd in een andere lidstaat, zonder tussenkomst van de bevoegde autoriteit in die lidstaat. Tijdens het opstellen van de verordening leidde dit bij verschillende lidstaten, waaronder Nederland, tot zorgen over rechtsbescherming, omdat bedrijven in de voorgestelde EU-verordening geen mogelijkheid hadden om in de eigen lidstaat bezwaar te maken tegen een bevel.[20]

Deze zorgen zijn uitgebreid geuit tijdens de onderhandelingen over de EU-verordening. Als gevolg is de EU-verordening zo gewijzigd dat wanneer een andere lidstaat een verwijderbevel stuurt, dit zowel naar de HSP als naar de nationale bevoegde autoriteit wordt gestuurd. De HSP moet het materiaal nog steeds binnen één uur ontoegankelijk te maken. De bevoegde autoriteit van de lidstaat waar de aanbieder van hostingdiensten zijn hoofdvestiging of waar zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats heeft, kan op eigen initiatief binnen 72 uur na ontvangst van het verwijderingsbevel, het verwijderingsbevel toetsen om te bepalen of het (onder anderen) een ernstige of kennelijke inbreuk op deze verordening of op de grondrechten en vrijheden inhoudt. Daarnaast heeft de HSP 48 uur de mogelijkheid om bij de bevoegde autoriteit in de eigen lidstaat een verzoek in te dienen om het bevel te laten toetsen.[21]

Naast deze bevoegdheden introduceert de EU-verordening verschillende verplichtingen en waarborgen om een evenwicht te waarborgen tussen effectieve handhaving en de bescherming van fundamentele rechten.

Zo is materiaal dat voor educatieve, journalistieke, artistieke of onderzoeksdoeleinden of dat met het oog op het voorkomen of bestrijden van terrorisme onder het publiek wordt verspreid, uitgezonderd van de EU-verordening.

De EU-verordening bepaalt verder dat een HSP als blootgesteld kan worden aangemerkt wanneer deze in de voorafgaande twaalf maanden twee of meer definitieve verwijderingsbevelen heeft ontvangen (en de bevoegde autoriteit in de lidstaat een besluit heeft genomen waarbij is vastgesteld dat de aanbieder van hostingdiensten aan terroristische inhoud is blootgesteld en dat dit besluit aan de aanbieder van hostingdiensten heeft meegedeeld).[22] In dat geval is de HSP verplicht specifieke maatregelen te treffen om zijn

[20] Tweede Kamer (2018), Motie van de leden Van Nispen en van Toorenburg over verzet tegen een verwijderingsbevel uit andere lidstaten. 22 112, nr. 2724.
[21] Artikel 4, Verordening (EU) 2021/784.
[22] Artikel 5, Verordening (EU) 2021/784.

diensten te beschermen tegen verdere verspreiding van terroristische online inhoud. De bevoegde autoriteit is verantwoordelijk voor het opleggen van sancties indien de genomen maatregelen door de HSP onvoldoende doeltreffend zijn.[23]

Bovendien bevat de EU-verordening specifieke waarborgen ter bescherming van fundamentele rechten. Verwijderbevelen moeten daarom voldoende gedetailleerde gemotiveerd worden waarom de inhoud als terroristische inhoud wordt beschouwd alsook een verwijzing van het relevant soort materiaal.

Aanbieders van hostingdiensten die een verwijderingsbevel hebben ontvangen, hebben bovendien recht op een doeltreffende voorziening in rechte. Dit omvat het recht om een dergelijk verwijderingsbevel te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd (bezwaar) en het recht om een dergelijk besluit te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het besluit heeft genomen (beroep).

Aanbieders van inhoud waartoe na een verwijderingsbevel de toegang geblokkeerd is, hebben ook recht op een doeltreffende voorziening in rechte. Dit omvat het recht om een verwijderingsbevel te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het verwijderingsbevel heeft uitgevaardigd (bezwaar) en het recht om een besluit te betwisten bij de rechterlijke instanties van de lidstaat van de bevoegde autoriteit die het besluit heeft genomen (beroep).

Tot slot stelt de EU-verordening eisen aan de rechtsbescherming van gebruikers en aan transparantie. HSPs moeten beschikken over een ‘doeltreffend en toegankelijk mechanisme’ waarmee aanbieders van inhoud waartoe de toegang geblokkeerd is ten gevolge van specifieke maatregelen een klacht betreffende die blokkering van de toegang kunnen indienen waarbij om het herstel of het weer toegankelijk maken van de inhoud wordt verzocht.[24]

Zowel bevoegde autoriteiten als HSPs zijn daarnaast gebonden aan transparantie-verplichtingen. Een aanbieder van hostingdiensten die op grond van deze verordening in een bepaald kalenderjaar maatregelen heeft genomen of heeft moeten nemen om de verspreiding van terroristische inhoud tegen te gaan, maakt een transparantieverslag openbaar over de maatregelen die in die periode zijn genomen.[25] Daarnaast publiceren de bevoegde autoriteiten publiceren jaarlijkse transparantieverslagen over hun activiteiten in het kader van deze verordening. Die verslagen bevatten ten minste de volgende informatie over het betrokken kalenderjaar.[26]

Naast de EU-verordening speelt de Digital Services Act een belangrijke rol op EU-niveau met betrekking tot verschillende vormen van illegale online content en het beschermen van gebruikersrechten.

---

23 De invulling van ‘specifieke maatregelen’ is aan de HSPs en de invulling van ‘sancties’ laat de EU-verordening aan de lidstaten. Zie voor invulling door Nederland verderop in deze paragraaf.

24 Artikel 10, Verordening (EU) 2021/784.

25 Artikel 7, Verordening (EU) 2021/784.

26 Artikel 8, Verordening (EU) 2021/784.

De Digital Services Act

In 2022 is de Digital Services Act (DSA) aangenomen.[27] Deze verordening biedt een algemeen kader voor het aanpakken van verschillende vormen van illegale online content en het beschermen van gebruikersrechten. Terroristische online inhoud is een van de vormen van illegaal materiaal dat onder de DSA valt.[28] Bij de DSA zijn *trusted flaggers* onder meer verantwoordelijk voor het detecteren van potentieel illegale inhoud. Binnen de DSA ondersteunen *trusted flaggers* het detecteren van bepaalde soorten schadelijke online content en hebben ze de taak dit door te zetten naar onlineplatformen en, indien nodig, toezicht-houders. *Trusted flaggers* zijn aangewezen organisaties onder de DSA, gespecialiseerd in de detectie van dit soort materiaal.

De DSA fungeert als het algemene Europese kader voor de regulering van online platforms en illegale online inhoud. De EU-verordening geldt als sectorspecifieke regelgeving voor terroristische online inhoud en kan worden beschouwd als een lex specialis ten opzichte van de DSA. Dit betekent dat voor onderwerpen die expliciet in de EU-verordening zijn geregeld, de specifieke bepalingen van die verordening gelden. Voor overige aspecten blijft de DSA van toepassing.

De Uitvoeringswet verordening terroristische online-inhoud

De EU-verordening heeft rechtstreekse werking in Nederland. De Uitvoeringswet TOI legt de praktische implementatie van de EU-verordening in Nederland vast.[29] Zo geeft de wet vorm aan een nieuw zelfstandig bestuursorgaan (zbo) als bevoegde autoriteit, namelijk de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM). Deze autoriteit heeft in Nederland de verantwoordelijkheid voor alle taken en bevoegdheden die in de EU-verordening zijn vastgelegd. Naast het aanwijzen van de bevoegde autoriteit bevat de Uitvoeringswet TOI bovenop de EU-verordening een aantal aanvullende bepalingen. Tabel 2.2 geeft hiervan een overzicht.

Tabel 2.2 Aanvullende bepalingen Uitvoeringswet TOI

Wetsartikel	Uitleg
Artikel 2. De Autoriteit	De Autoriteit Online Terroristisch en Kinderpornografisch Materiaal is de bevoegde autoriteit bedoeld in artikel 12, eerste lid, onderdelen a tot en met d, van de verordening en heeft de taken die de verordening aan de bevoegde autoriteit toekent. De Autoriteit heeft met het oog op de maatregelen bedoeld in artikel 1, eerste lid, onderdeel b, van de verordening tot taak: a) terroristische inhoud te identificeren en het ontoegankelijk maken van online terroristische inhoud te bevorderen en zo nodig af te dwingen; en b) onderzoek te doen naar, en informatie te verstrekken over, de aanwezigheid van online terroristisch materiaal teneinde de verspreiding daarvan onder het publiek te beperken, waar mogelijk in samenwerking met private en publieke partijen. De leden van de Autoriteit en de bij besluit van de Autoriteit aangewezen ambtenaren zijn belast met het toezicht op de naleving van de artikelen 3, derde en zesde lid, artikel 4, tweede en zevende lid, artikel 5, eerste, tweede, derde, vijfde en zesde lid, artikelen 6, 7, 10 en 11, artikel 14, vijfde lid, artikel 15, eerste lid

27 Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening).

28 Tweede Kamer (2022), Nota naar aanleiding van het verslag: Uitvoeringswet verordening terroristische online-inhoud, 36 138, nr 7.

29 Tweede Kamer (2022), Memorie van toelichting: Uitvoeringswet verordening terroristische online-inhoud, 36 138, nr. 3.

	en artikel 17 van de verordening. De Autoriteit heeft tevens tot taak het nemen van beslissingen als bedoeld in artikel 16.
Artikel 8. Afstemming	Ter bevordering van de coördinatie van te nemen maatregelen overlegt de Autoriteit over de uitoefening van zijn taken en bevoegdheden met de politie, het openbaar ministerie en de Algemene Inlichtingen- en Veiligheidsdienst en Militaire Inlichtingen- en Veiligheidsdienst.
Paragraaf 3. Sancties	De ATKM kan een last onder dwangsom (artikel 11) of bestuurlijke boete (artikel 12) opleggen om verwijderbevelen en specifieke maatregelen te handhaven. Het beluit tot het opleggen van een bestuurlijke boete kan openbaar worden gemaakt (artikel 13).
Paragraaf 4. Klachten	Een aanbieder van hostingdiensten die zijn hoofdvestiging in Nederland heeft of waarvan zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats in Nederland heeft, wijst aanbieders van inhoud waartoe de toegang geblokkeerd is ten gevolge van specifieke maatregelen, steeds op de mogelijkheid om een klacht in te dienen en op de mogelijkheid van geschillenbeslechting door de Autoriteit (artikel 14). Elke aanbieder van hostingdiensten die zijn hoofdvestiging in Nederland heeft of waarvan zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats in Nederland heeft, bericht de Autoriteit over alle bij hem ingediende klachten als bedoeld in artikel 10 (artikel 15). Een aanbieder van inhoud die een geschil heeft over de afhandeling van een klacht met een aanbieder van hostingdiensten die zijn hoofdvestiging in Nederland heeft of waarvan zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats in Nederland heeft, kan binnen een termijn van zes maanden na de klachtafhandeling door de aanbieder van hostingdiensten over het geschil een klacht indienen bij de Autoriteit (artikel 16).

De belangrijkste toevoeging aan de EU-verordening in de Uitvoeringswet TOI betreft de geschilbeslechtingsprocedure (artikel 16). Deze procedure geeft gebruikers die een geschil hebben over de afhandeling van een klacht met een aanbieder van hostingdiensten die zijn hoofdvestiging in Nederland heeft of waarvan zijn wettelijke vertegenwoordiger zijn verblijf- of vestigingsplaats in Nederland heeft, een klacht in te dienen bij de bevoegde autoriteit. Het gaat hierbij alleen om geschillen ten gevolge van specifieke maatregelen uitgevoerd door HSPs als gevolg van een blootstellingsbesluit. De gedachte hierachter was dat de Nederlandse overheid op deze manier zicht kan blijven houden op de aard en omvang van de klachtenstroom en mogelijk onrechtmatige inbreuk op de vrijheid van meningsuiting.[30]

Ten aanzien van sancties heeft de ATKM in juni een toezicht en handhavingsbeleid opgesteld[31] en als nadere uitwerking daarvan een dwangsom- en boetebeleid opgesteld.[32] In het dwangsom- en boetebeleid is vastgelegd wanneer en onder welke omstandigheden de ATKM kiest voor een bepaalde bestuurlijke sanctie, hoe hoog de dwangsom of de boete in beginsel bedraagt bij bepaalde overtredingen en welke omstandigheden de ATKM meeweegt bij het vaststellen van de hoogte in een concreet geval en (in het geval van de dwangsom) hoe vaak een dwangsom kan verbeuren. Of een last onder dwangsom of een bestuurlijke boete (of allebei) in het concrete geval een geschikt, noodzakelijk en evenwichtig middel is, bepaalt de ATKM mede aan de hand van een interventiematrix, waarbij de ernst van de overtreding in combinatie met het gedrag van de overtreder wordt afgewogen. De volgende tabel geeft het beleid ten aanzien van dwangsommen en boetes weer.

30 Tweede Kamer (2022), Amendement van het Lid Leijten: Uitvoeringswet verordening terroristische online inhoud, 36 138, nr. 10.
31 ATKM (2026). Handhavingsbeleid van de ATKM.
32 ATKM (2026), Dwangsom- en boetebeleid Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM).

Tabel 2.3 Dwangsom en boetebeleid ATKM voor EU-verordening

Wettelijke bepaling	Omschrijving	Ernst categorie	Boete maximum	Dwangsom
Artikel 3, derde lid	Niet naleven bevel om materiaal ontoegankelijk te maken	IV	Tweede categorie. Bij systematisch of aanhoudend zesde categorie of 4% jaaromzet	€ 20.000,-
Artikel 3, zesde lid	Kennisgeving verwijdering/blokkering van ATKM, zonder onnodige vertraging	I	Tweede categorie	€ 5.000,-
Artikel 4, tweede lid	Nodige maatregelen voor herstel of toegankelijk maken van inhoud	I	Tweede categorie	€ 5.000,-
Artikel 4, zevende lid	Herstellen of toegankelijk maken van inhoud	I	Tweede categorie	€ 5.000,-
Artikel 5, eerste lid	Inhoud algemene voorwaarden	III	Vijfde categorie	€ 15.000,-
Artikel 5, tweede lid	Treffen van specifieke beschermingsmaatregelen	III	Vijfde categorie	€ 15.000,-
Artikel 5, derde lid	Eisen aan specifieke beschermingsmaatregelen	III	Vijfde categorie	€ 15.000,-
Artikel 5, vijfde lid	Aanbieder moet binnen 3 maanden (en daarna jaarlijks) aan ATKM verslag uitbrengen over specifieke maatregelen die zijn genomen en zullen worden genomen	II	Vijfde categorie	€ 10.000,-
Artikel 5, zesde lid	Aanpassing specifieke maatregelen op verzoek ATKM. Nader besluit dat ertoe verplicht dat de nodige maatregelen alsnog worden genomen. In een geval dat de ATKM besluit dat de specifieke maatregelen niet aan de gestelde eisen voldoen	II	Vijfde categorie	€ 10.000,-
Artikel 6	Bewaren van verwijderde of geblokkeerde inhoud	I	Vijfde categorie	€ 5.000,-
Artikel 7	Transparantieverplichtingen	II	Vijfde categorie	€ 10.000,-
Artikel 10	Klachtenmechanismen	II	Vijfde categorie	€ 10.000,-
Artikel 11	Informatie voor aanbieders van inhoud	II	Vijfde categorie	€ 10.000,-
Artikel 14, vijfde lid	Meldplicht bij onmiddellijk levensbedreigend gevaar	IV	Vijfde categorie	€ 20.000,-
Artikel 15 eerste lid	Geen contactpunt	III	Vijfde categorie	€ 15.000,-
Artikel 17	Wettelijke vertegenwoordiger	II	Vijfde categorie	€ 10.000,-

Met ernstcategorie wordt het volgende bedoeld: I. Beperkt, II. Gemiddeld, III. Ernstig, IV. Zeer ernstig. De categorieën genoemd in de kolom boete maximum zijn bedoeld zoals omschreven in artikel 23, vierde lid, van het Wetboek van Strafrecht. Dit zijn: de tweede categorie: € 5.500, de vijfde categorie, € 110.000 en de zesde categorie, € 1.100.000.

De Autoriteit online Terroristisch en Kinderpornografisch Materiaal
De ATKM is in september 2023 opgericht en is operationeel sinds april 2024.[33] Onder artikel 2 van de Uitvoeringswet TOI heeft de autoriteit twee kerntaken.

De eerste taak is terroristische inhoud te identificeren en het ontoegankelijk maken van online terroristische inhoud te bevorderen en, zo nodig, af te dwingen. Het primaire proces van de ATKM omvat het identificeren van terroristisch online materiaal, het beoordelen of dit binnen de reikwijdte valt van de definitie van terrorisme die de uitvoeringswet TOI hanteert en het vaststellen of het ontoegankelijk maken van dit materiaal wettig, noodzakelijk en proportioneel is (zie ook paragraaf 2.2).

De tweede kerntaak is om onderzoek te doen naar en informatie te verstrekken over de aanwezigheid van online terroristisch materiaal teneinde de verspreiding daarvan onder het publiek te beperken, waar mogelijk in samenwerking met private en publieke partijen. Bij de formatie van de ATKM werd voorzien dat de autoriteit door haar hoge graad van thematische specialisatie over uitgebreide kennis zou beschikken over trends en ontwikkelingen rondom extremisme en terrorisme; inzichten die van grote waarde kunnen zijn voor ketenpartners die zelf niet genoeg capaciteit hebben om hier diepgaande expertise over op te bouwen.[34] Om preventief te kunnen optreden tegen terroristische en extremistische radicalisering heeft de ATKM daarom ook een signalerende functie binnen de keten en onder het bredere publiek.

De ATKM is expliciet niet belast met het opsporen of vervolgen van makers of verspreiders van terroristische content.[35]

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) is samen met de Directeur Rechtshandhaving en Criminaliteitsbestrijding bij het Directoraat-Generaal Rechtsbescherming en Rechtspleging opdrachtgever voor de ATKM.[36] Om haar taken uit te voeren, werkt de ATKM samen met onder andere de politie, het Openbaar Ministerie (OM), de NCTV, bevoegde autoriteiten van andere lidstaten, HSPs en Europol.[37]

De ATKM is verantwoordelijk voor het tegengaan van de verspreiding van zowel online terroristisch als kinderpornografisch materiaal.

2.2 TOI cyclus

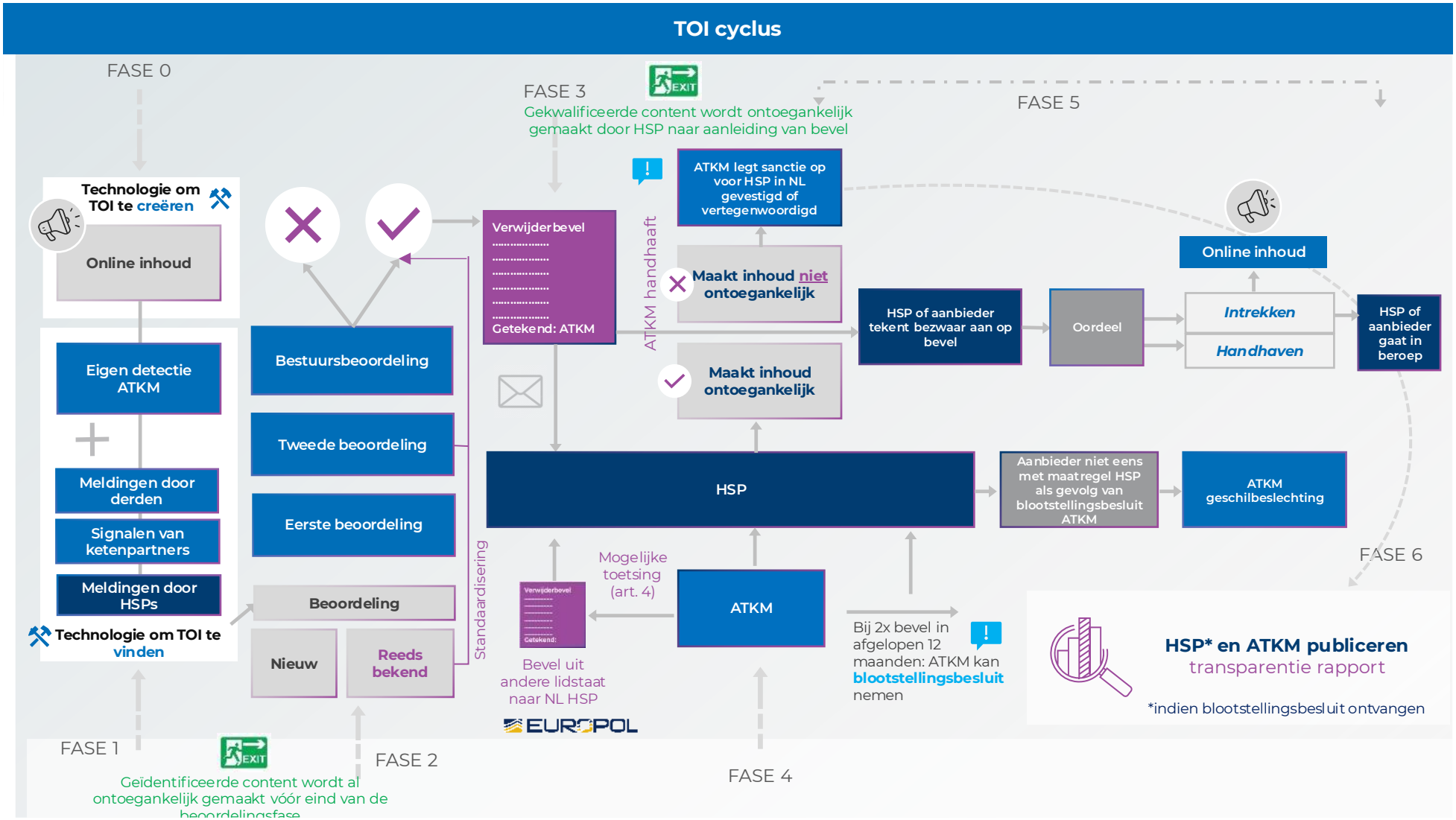
Terroristisch online materiaal gedetecteerd door de ATKM doorloopt een cyclus: van het moment waarop de terroristische online inhoud wordt gecreëerd en verspreid (behoort niet tot de scope van deze evaluatie) tot en met het moment waarop deze ontoegankelijk wordt gemaakt. De Uitvoeringswet TOI geeft deze cyclus vorm. Deze paragraaf beschrijft hoe dit in theorie werkt. De beschrijving is gebaseerd op gesprekken met de ATKM en ketenpartners en geeft inzicht in hoe de wet vorm krijgt in de praktijk.

---

33 ATKM (2025), Jaarverslag 2024.
34 Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM; NCTV (2020), Verkenning: Een competente autoriteit voor de uitvoering van de verordening Terroristische Content Online.
35 Ibid.
36 Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM.
37 ATKM (2025). Jaarverslag 2024; ATKM (2026). Jaarverslag 2025.

De cyclus bestaat uit de volgende fasen: 0) creatie en verspreiding, 1) identificatie en melding, 2) beoordeling en kwalificatie, 3) interventie, 4) opvolging en monitoring. 5) rechtsbescherming, en 6) verantwoording. In de onderstaande figuur wordt deze cyclus, met de zes fasen, op hoofdlijnen afgebeeld. Het figuur wordt vervolgens stapsgewijs toegelicht.

Figure 2.1 Cyclus vanuit perspectief ATKM



Bron: Ecorys (2026)

Fase 0. Creatie en verspreiding van online terroristische inhoud

De TOI cyclus begint bij een fase die zich buiten het bereik van de wet zelf afspeelt: het moment waarop terroristische online inhoud wordt gecreëerd en verspreid. Deze inhoud kan uiteenlopende vormen aannemen (video's, afbeeldingen, teksten, audiofragmenten of *memes*) en wordt geplaatst op HSPs of online platformen die actief zijn binnen de Europese Unie. Creatie en verspreiding vinden onder anderen plaats binnen de digitale omgeving van HSPs en buiten het directe zicht van overheden en toezichthouders. Dit vormt het startpunt van de verdere keten.

Nederland heeft van oudsher een sterke positie in de Europese digitale infrastructuur, mede dankzij de aanwezigheid van de Amsterdam Internet Exchange (AMS-IX).[38] Nederland herbergt een groot aantal HSPs, variërend van grote, internationaal opererende aanbieders tot kleine, gespecialiseerde providers. Bekende grote sociale mediaplatformen zoals Meta, TikTok, X en YouTube hebben een hoofdvestiging of wettelijke vertegenwoordiging in Ierland en vallen daarmee primair onder het toezicht van de Ierse bevoegde autoriteit. De grootste platforms die in Nederland een hoofdvestiging of wettelijke vertegenwoordiging hebben, zijn Snapchat, Reddit en Discord. Daarnaast hebben kleinere en gespecialiseerde hostingaanbieders een hoofdvestiging of wettelijke vertegenwoordiging in Nederland.[39]

Definitie Hosting Service Providers

In de EU-verordening en de Uitvoeringswet TOI wordt de term *aanbieder van hostingdiensten* gehanteerd. In internationaal gebruik afgekort als HSP, naar het Engelse *Hosting Service Provider*. De EU-verordening definieert een HSP als elke aanbieder van diensten die bestaan uit het opslaan van informatie die door de afnemer van de dienst (oftewel de gebruiker die de content plaatst) wordt verstrekt, ongeacht de plaats van de hoofdvestiging of wettelijke vertegenwoordiging van de aanbieder, zolang de dienst binnen de EU wordt aangeboden.[40]

In de praktijk is deze definitie breder dan de term 'hostingdienst' op het eerste gezicht doet vermoeden. Onder het begrip vallen niet alleen traditionele webhostingbedrijven, maar ook sociale mediaplatformen, videodiensten, berichtendiensten, cloudopslagdiensten en zelfs gamingplatformen. Kortom: elke dienst waarbij inhoud wordt opgeslagen op verzoek van een derde en openbaar toegankelijk wordt gemaakt. De wettelijke definitie beperkt zich tot diensten die bestaan uit het opslaan van door de gebruiker verstrekte informatie, waardoor partijen zonder eigen opslagfunctie, zoals zoekmachines of kleinere platforms met een hybride functie, niet onder dit begrip vallen. Desalniettemin is HSP als afkorting internationaal gangbaar en wordt het breed begrepen. In dit rapport wordt daarom de term HSP gehanteerd.

Fase 1. Identificatie en melding

Zodra terroristische online inhoud beschikbaar is, kan deze op verschillende manieren in beeld komen bij de ATKM. In de praktijk verloopt dit via verschillende sporen.

Het meest gebruikte spoor is de eigen detectie. De ATKM verricht zelfstandig Open Source Intelligence (OSINT)-onderzoek op het open internet door gespecialiseerde medewerkers die handmatig zoeken op basis van een intern opgebouwde en continu bijgewerkte lijst van

---

38 Dialogic (2024), Het belang van digitale infrastructuur voor de Nederlandse digitale knooppuntrol.
39 Interview met maatschappelijk middenveld, april 2026.
40 Artikel 2, lid 1, onder (f), Verordening (EU) 2021/784.

zoektermen, logo's, documenten en symboliek. Die zoeklijsten worden gevoed vanuit diverse bronnen: sanctielijsten, een deel van de informatie uit de TCO detect tool van Europol[41], Tech Against Terrorism[42], dreigingsanalyses van de NCTV, materiaal van de politie en eigen proactief onderzoek naar nieuwe narratieven en symbolen.[43] [44]

Andere manieren waarop terroristische online inhoud bij de ATKM terecht kan komen, zijn: signalen van ketenpartners zoals de politie, de NCTV, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD); en meldingen via een openbaar meldpunt[45] van derden, zoals burgers, maatschappelijke organisaties of wetenschappers. In theorie kunnen HSPs ook melding maken, dit doen ze wanneer sprake is van ‘immediate threat to life’.

Naast deze vier sporen gebruiken politiediensten Europols SIENA-platform om signalen met andere lidstaten uit te wisselen. Voor toegang hiertoe is de ATKM afhankelijk van de politie (zie ook paragraaf 3.4).

De ATKM doet geen livestream-monitoring. Het kan zijn dat de ATKM kennis neemt van livestreaming via bijvoorbeeld de eigen detectie. Als deze streams als TOI geclassificeerd kunnen worden kan de ATKM hierop handelen.[46] Wanneer terroristische online inhoud via een livestream wordt verspreid, wordt het EU Online Crisis Response Framework toegepast. Dit wordt beheerd door de Europese Commissie. In Nederland heeft de politie hierin een operationele rol.[47] De ATKM kan wel op de hoogte worden gesteld van het feit dat mogelijk materiaal van terroristische aard over het openbare internet wordt verspreid. Zij kan dan zelfstandig beoordelen of specifieke aandacht hiervoor nodig is.[48]

Fase 2. Beoordeling en kwalificatie

Na de identificatie volgt de inhoudelijke en juridische beoordeling van het materiaal. In deze fase wordt vastgesteld of de content daadwerkelijk kwalificeert als terroristische online inhoud in de zin van de EU-verordening. Dit is een sleutelmoment in de cyclus: de uitkomst bepaalt of verdere actie volgt en het vormt de juridische motivering voor een eventueel verwijderbevel.

De beoordeling verloopt gelaagd en sequentieel in vier stappen. In de eerste stap wordt de formele toepasselijkheid getoetst: betreft het publiek toegankelijke content op het open internet, valt de betrokken HSP binnen de reikwijdte van de EU-verordening en is de inhoud actueel en bereikbaar? In de tweede stap volgt de inhoudelijke kwalificatie: valt de content onder de wettelijke definitie van terroristische online inhoud? Daarbij wordt beoordeeld of het materiaal aanzet tot het plegen van terroristische misdrijven, deze verheerlijkt of rechtvaardigt, instructies bevat voor het plegen ervan, of deelname aan terroristische organisaties bevordert. In de derde stap vindt een grondrechtelijke weging plaats. Hier worden context, intentie,

---

41 Hiervoor is de ATKM afhankelijk van de politie.

42 Tech Against Terrorism is een initiatief dat technologiebedrijven ondersteunt bij het tegengaan van terroristisch gebruik van internet.

43 Hierbij dient expliciet genoemd te worden dat de ATKM geen toegang heeft tot Europols database (Check the Web). Zie voor specifieke toelichting op samenwerking ATKM en Europol paragraaf 3.5.

44 Interview met ATKM, mei 2026.

45 Het meldpunt van de ATKM is beschikbaar via deze link.

46 Schriftelijke Toelichting ATKM, juli 2026.

47 Ibid.

48 Schriftelijke Toelichting ATKM, juli 2026.

doelgroep en herkomst meegewogen om te beoordelen of een beperking van de vrijheid van meningsuiting gerechtvaardigd is. Ook worden uitzonderingsgronden hierbij in acht genomen. De beoordelingsprocedure is zo ingericht dat altijd sprake is van dubbele toetsing. Gestandaardiseerde content, materiaal dat eerder uitvoerig is beoordeeld en gedocumenteerd, zoals beelden van de aanslag in Christchurch in Nieuw-Zeeland die in 2019 plaatsvond, kan via een versnelde procedure worden afgehandeld. Voor nieuw, niet eerder beoordeeld materiaal geldt een volledige procedure.

Fase 3. Interventie: verwijderbevel of geen actie

Wanneer de ATKM concludeert dat sprake is van terroristische online inhoud, vaardigt zij een verwijderbevel uit. Op grond van de EU-verordening dient de betrokken HSP de inhoud binnen één uur na ontvangst ontoegankelijk te maken. De Uitvoeringswet TOI heeft deze bevoegdheid tot het uitvaardigden van een bevel exclusief bij de ATKM belegd.[49]

Voordat het bevel wordt verzonden, vindt deconflictie plaats. Dit is het proces waarbij de ATKM met de politie controleert of de geïdentificeerde content deel uitmaakt van een lopend onderzoek. In de praktijk stuurt de ATKM de relevante URL's door naar het Landelijk Internationaal Rechtshulp Centrum (LIRC) van de politie (met een kopie naar de afdeling CTER van de politie in Woerden), dat de inhoud binnen 48 uur nagaat. Geeft de politie geen reactie binnen die termijn, dan beschouwt de ATKM dit als groen licht om het bevel te verzenden. Deconflictie met de AIVD vindt daar waar nodig plaats maar ook daar geldt dat er een reactie uitblijft wanneer er geen bezwaar is.[50] Op EU-niveau verloopt de deconflictiebehandeling gedeeltelijk automatisch via PERCI: wanneer een URL in het systeem wordt ingevoerd, controleert het systeem of deze al door een andere bevoegde autoriteit in PERCI is ingevoerd. Dit voorkomt dat twee autoriteiten gelijktijdig aan dezelfde content werken.

Borderline content

Borderline content verwijst naar online materiaal dat op zichzelf niet illegaal is, maar wel schadelijk kan zijn omdat het extremistische ideeën kan normaliseren of radicalisering kan bevorderen.[51] Omdat borderline content niet als online terroristisch materiaal kwalificeert, valt het buiten het mandaat van de ATKM. De ATKM identificeert dit soort materiaal wel als onderdeel van haar taak om materiaal te identificeren maar mag hier vervolgens niets mee doen.

Het verwijderbevel wordt opgesteld op basis van een vast sjabloon, voorzien van een juridische motivering, en vervolgens ingevoerd in PERCI. Niet alle HSPs zijn op PERCI aangesloten. Sommige platforms hebben hun eigen systemen voor het ontvangen van bevelen, wat betekent dat een bevel in de praktijk via meerdere kanalen tegelijk wordt verstuurd. Het gehele administratieve proces, van het opstellen en aftekenen van het bevel tot en met de invoer in PERCI en de feitelijke verzending, kan in het snelste geval, bij gestandaardiseerde content, binnen 1 uur worden verstuurd.[52]

---

49 Ter verduidelijking: andere partijen kunnen wel zelf melden bij de HSP via de procedures onder de DSA (art. 16).

50 Interview met ATKM, mei 2026; ATKM (2025), Jaarverslag 2024.

51 Saltman, E., & Hunt, M. (2023), Borderline content: understanding the grey zone.

52 Interview met ATKM, mei 2026; Rode draad sessie, januari 2026.

De ATKM verstuurt bevelen via PERCI aan HSPs ongeacht waar de hoofdvestiging of wettelijke vertegenwoordiging van de HSP is gevestigd, zolang zij diensten aanbieden binnen de EU. Bij grensoverschrijdende bevelen (waarbij de ATKM een bevel richt aan een HSP met een hoofdvestiging of wettelijke vertegenwoordiging in een andere lidstaat) wordt de bevoegde autoriteit van die lidstaat via PERCI op de hoogte gebracht.[53] Omgekeerd ontvangt de ATKM bevelen van buitenlandse autoriteiten gericht aan HSPs met een hoofdvestiging of wettelijke vertegenwoordiging in Nederland en is zij verantwoordelijk voor het toezicht op naleving in die gevallen. De ATKM kan dan op eigen initiatief binnen 72 uur na ontvangst van het verwijderingsbevel, het verwijderingsbevel toetsen om te bepalen of het (onder anderen) een ernstige of kennelijke inbreuk op deze verordening of op de grondrechten en vrijheden inhoudt. De betrokken HSP kan binnen 48 uur een verzoek tot toetsing indienen.[54]

In gevallen waarin de ATKM tijdens haar detectiewerk stuit op een concrete dreiging (content die duidt op een onmiddellijk levensgevaar) wordt dit onmiddellijk gemeld aan de Nederlandse politie, Europol of de betreffende buitenlandse politiedienst.[55]

HSP's kunnen materiaal ontoegankelijk maken. Dit kan inhouden dat zij het materiaal verwijderen of dat zij een geo-blokkade opleggen. Deze blokkade zorgt ervoor dat de content niet meer toegankelijk is vanuit een bepaalde regio. Dit wordt bepaald op basis van IP-adressen (geo-blokkades zijn echter eenvoudig te omzeilen met gebruik van een VPN verbinding).[56] In dit onderzoek worden de woorden ‘verwijderd’ en ‘ontoegankelijk maken van materiaal’ afwisselend gebruikt.

Fase 4. Opvolging en monitoring

Na het uitvaardigen van een verwijderbevel is de HSP verantwoordelijk voor de tijdige uitvoering ervan. De ATKM verifieert of het bevel is nageleefd. De ATKM is verantwoordelijk voor de handhaving bij HSPs met een hoofdvestiging of wettelijke vertegenwoordiging in Nederland. Dit gaat momenteel om o.a. Snapchat, Reddit en Discord.

Wanneer een HSP in de voorafgaande twaalf maanden twee of meer definitieve verwijderingsbevelen heeft ontvangen dan kan de ATKM een blootstellingsbesluit opleggen (mits de aanbieder gevestigd is in Nederland of een wettelijke vertegenwoordiger in Nederland heeft). Dit verplicht de aanbieder om structurele preventieve maatregelen te nemen om herhaling te voorkomen, bijvoorbeeld aanscherping van eigen moderatieprocessen en detectiemechanismen. De EU-verordening legt hierbij geen resultaatverplichting op: HSPs hoeven niet aan algemene monitoring te doen, maar moeten wel gerichte, redelijke maatregelen treffen tegen herplaatsing. Dit betekent dat vooral wordt getoetst of de aanbieder actie heeft ondernomen, en in mindere mate of die actie ook daadwerkelijk effect heeft gehad.

Bij grensoverschrijdende bevelen (waarbij een buitenlandse bevoegde autoriteit een bevel richt aan een HSP die een hoofdvestiging of wettelijke vertegenwoordiging heeft in Nederland) is de buitenlandse bevoegde autoriteit verantwoordelijk voor het toezicht op de naleving en, in het geval van Nederland, de ATKM verantwoordelijk voor het toezicht op de handhaving. Zij kan de buitenlandse autoriteit informeren bij problemen in de uitvoering, maar neemt het bevel

---

53 Artikel 17 Verordening (EU) 2021/784 verplicht HSPs die services aanbieden in de EU een wettelijke vertegenwoordiging in een EU lidstaat aan te wijzen.

54 Artikel 4, Verordening (EU) 2021/784; Interview met ATKM, april 2026.

55 ATKM (2025), Jaarverslag 2024; Interview met ATKM, april 2026.

56 Schriftelijke toelichting ATKM, juli 2026.

niet opnieuw in overweging en treedt niet in de plaats van de autoriteit die het bevel heeft uitgevaardigd.[57]

Fase 5. Rechtsbescherming: bezwaar en beroep

De EU-verordening en de Uitvoeringswet TOI voorzien in rechtsbescherming voor zowel de aanbieder van de content (de partij die het materiaal op het platform heeft geplaatst) als de HSP. De Uitvoeringswet TOI bevat expliciete bezwaar en beroepsclausules. Bovendien is een verwijderbevel op basis van de Uitvoeringswet TOI een besluit in de zin van de Algemene wet bestuursrecht (Awb), waardoor de reguliere bestuursrechtelijke rechtsbescherming automatisch van toepassing is. HSPs en inhoudsaanbieders kunnen binnen zes weken bezwaar indienen bij de ATKM. Indien het bezwaar ongegrond wordt verklaard, staat het beroep open bij de bestuursrechter, gevolgd door de mogelijkheid van hoger beroep bij de Afdeling bestuursrechtspraak van de Raad van State. Gedurende de procedure blijft de verwijdering van kracht: de content blijft ontoegankelijk totdat anders wordt beslist.[58]

Naast de reguliere bezwaar- en beroepsprocedure bevat de Uitvoeringswet TOI een aanvullende geschilbeslechtingsprocedure voor aanbieders van internetinhoud, neergelegd in artikel 16. Nederland is de enige lidstaat die een dergelijke procedure heeft opgenomen in de implementatiewet.[59] Het betreft een extra mogelijkheid voor aanbieders van inhoud om, in het geval van een geschil tussen de aanbieder en de HSP, een door de HSP ontoegankelijk gemaakt stuk content ter beoordeling voor te leggen aan de ATKM, los van de reguliere Awb-procedure.

Tot slot is er nog een mogelijkheid om de autoriteit in een lidstaat een toetsing te laten doen van een bevel.[60] Bijvoorbeeld: een buitenlandse autoriteit stuurt een bevel naar een partij in Nederland om content ontoegankelijk te maken. Er zijn dan twee situaties denkbaar: óf de HSP vraagt om een toets bij de lidstaat waar zij een hoofdvestiging of wettelijke vertegenwoordiging heeft (in dit geval Nederland), óf de bevoegde autoriteit in de lidstaat waar de HSP een hoofdvestiging of wettelijke vertegenwoordiging heeft (in het geval van Nederland is dit de ATKM) voert een ambtelijke toets uit op eigen initiatief. Indien de conclusie is dat het bevel rechtmatig is blijft het staan en moet de HSP het bevel naleven. Indien de conclusie is dat het niet rechtmatig is wordt een veto uitgesproken.

Fase 6. Verantwoording

De cyclus sluit af met verantwoording. De ATKM legt verantwoording af via haar jaarverslag, waarin zij rapporteert over het aantal uitgevaardigde verwijderbevelen, de naleving daarvan en de bredere uitvoering van haar wettelijke taken.[61] Daarnaast stelt de ATKM een transparantierapport op waarin zij rapporteert over haar activiteiten in het kader van de Europese Verordening (o.a. het aantal verwijderingsbevelen en de uitvoering daarvan, het aantal uitgevaardigde blootstellingsbesluiten, het aantal gerechtelijke toetsingsprocedures en het aantal opgelegde sancties). Deze transparantieverslagen

---

57 Artikel 4, Verordening (EU) 2021/784; Rode draad sessie, januari 2026.
58 Artikel 10 en 11, Verordening (EU) 2021/784; Artikel 11 en 12, Uitvoeringswet TOI.
59 Artikel 16, Uitvoeringswet TOI; Rode draad sessie, januari 2026; Interview met ATKM, april 2026.
60 Artikel 4, Verordening (EU) 2021/784.
61 ATKM (2025), Jaarverslag 2024; ATKM (2026), Jaarverslag 2025.

worden gedeeld met de Europese Commissie, die op basis van rapportages van alle lidstaten toezicht houdt op de implementatie van de EU-verordening.[62]

HSPs zijn op grond van artikel 7 van de EU-verordening verplicht om jaarlijks een transparantierapport te publiceren. Daarin vermelden zij het aantal ontvangen verwijderbevelen, het aantal verwijderde of geblokkeerde contentstukken en de specifieke maatregelen die zijn genomen om de verspreiding van terroristische inhoud te voorkomen. Een aantal grote platforms (waaronder X, Instagram, Discord, Google en Twitch) publiceert dergelijke rapporten.[63]

Tot slot

Met deze zes fasen doorloopt elk geval van (potentieel) terroristische online inhoud een vast traject van signalering tot afhandeling. De fasen zijn niet strikt opeenvolgend: deconflictie, monitoring en eventuele bezwaar- en beroepsprocedures kunnen parallel lopen, en niet elk geval doorloopt alle stappen.

---

62 Artikel 8, Verordening (EU) 2021/784.

63 X (2026), Transparantierapport TOI; Instagram (2026), Transparantierapport TOI; Discord (2026), Transparantierapport TOI; Google (2026), Transparantierapport TOI; Twitch (2026), Transparantierapport TOI; Snap Inc. (2026), Transparantierapport TOI.

3 Bevindingen

3.1 Juiste toepassing en naleving van verwijderbevelen

Bevindingen in het kort

- De ATKM detecteert terroristische online inhoud vrijwel uitsluitend via handmatig open source intelligence (OSINT) onderzoek; geautomatiseerde detectie is nog niet operationeel.
- Van alle geïdentificeerde content bereikt naar schatting een kwart de beoordelingsfase. De rest valt voornamelijk af, onder anderen omdat content niet eenduidig als TOI kwalificeert.
- In 2024 en 2025 zijn respectievelijk circa 150 en 180 verwijderbevelen uitgevaardigd; vrijwel alle zijn tijdig nageleefd.
- Er zijn tot op heden geen sancties opgelegd wegens niet-naleving.
- Het knelpunt in de keten ligt niet bij naleving na ontvangst, maar bij de doorlooptijd van detectie tot verzending, met name het deconflictieproces waar 48 uur voor staat.
- *Borderline content* blijft structureel buiten bereik: de ATKM detecteert deze content wel maar kan hierop niet acteren omdat dit materiaal buiten de reikwijdte van de Uitvoeringswet TOI valt.
- Bezwaar- en beroepsprocedures, blootstellingsbesluiten en de geschilbeslechtings-procedure zijn tot op heden niet benut.

3.1.1 Op welke wijze identificeert en beoordeelt de ATKM terroristische online inhoud?

De ATKM identificeert terroristische online inhoud hoofdzakelijk via eigen handmatige detectie. Gespecialiseerde medewerkers zoeken op het open internet op basis van een intern opgebouwde lijst met zoektermen, logo's, documenten en symbolen. Deze lijst wordt continu bijgesteld op basis van eerder beoordeeld materiaal, dreigingsanalyses van de NCTV, Europols TOI-detectdatabase (Check the Web), input van Tech Against Terrorism en de politie, en eigen proactief onderzoek naar nieuwe narratieven en symbolen.[64] De ATKM werkt daarbij tijdens kantooruren; buiten die uren vindt er geen actieve detectie plaats.[65]

Geautomatiseerde detectie is nog niet gerealiseerd. Een aanbestedingsprocedure voor Open Source Intelligence (OSINT)-software heeft niet het gewenste resultaat opgeleverd, onder meer omdat het aflopen van een raamovereenkomst van het ministerie van Justitie en Veiligheid het aanbod van geschikte aanbieders beperkte.[66] De ATKM heeft daarop besloten zelf een ontwikkelteam aan te stellen dat de gewenste applicaties naar verwachting in de loop van 2026 moet opleveren. In de tussentijd wordt een deel van de detectie uitbesteed aan externe OSINT-bedrijven.[67]

HSPs melden spontaan vrijwel nooit terroristische online inhoud aan de ATKM. Wanneer een platform zelf terroristische inhoud signaleert, verwijdert het die doorgaans direct via eigen

---

64 Interview met ATKM, mei 2026.
65 Rode draad sessie, januari 2026.
66 Interview met ATKM, mei 2026.
67 ATKM (2025), Jaarverslag 2024; Interview met ATKM, mei 2026.

moderatieprocessen zonder melding.[68] Er is voor aanbieders geen toegevoegde waarde om hier melding van te maken bij de ATKM.[69]

Signalen van ketenpartners en meldingen via het openbare meldpunt leveren aanvullende input, maar vormen tot op heden een klein deel van het identificatievolume. De AIVD en MIVD reageren in beginsel niet op signalen die de ATKM hen toestuurt (bijv. geïdentificeerde trends). De politie wisselt wel beeldmateriaal uit met de ATKM, maar specifieke informatie, zoals *hashlists* (digitale vingerafdrukken van reeds geclassificeerd materiaal) van Europol of het Check the Web-systeem, wordt op het moment van schrijven niet systematisch gedeeld (zie voor nadere toelichting paragraaf 3.4).[70] Het openbare meldpunt is in 2025 in werking getreden en midden 2026 start een publiekscampagne om dit meer zichtbaarheid te geven. Er wordt verwacht dat dit de hoeveelheid geïdentificeerde terroristische online inhoud zal doen toenemen. Omdat het portaal anoniem is, heeft de ATKM geen zicht op wie meldingen doet.[71] Ook is het mogelijk dat *trusted flaggers*[72] een rol spelen bij het opschalen van de hoeveelheid geïdentificeerde content.[73] Deze trusted flaggers kunnen geïdentificeerde content direct melden bij het desbetreffende platform en kunnen hierover, in het geval van TOI materiaal, ook in contact treden met ATKM.

Deze samenwerking is momenteel al zichtbaar in andere domeinen, zoals kinderpornografisch materiaal. Organisaties zoals Stichting Offlimits spelen in de praktijk een aanvullende rol: zij beschikken over een eigen meldpunt op het gebied van kinderpornografisch materiaal en zetten materiaal dat platforms niet verwijderen door naar de ATKM.[74] De ATKM verwijst op haar eigen meldpunt naar het meldpunt van Offlimits, een teken dat de samenwerking tussen de ATKM en Stichting Offlimits op gebied van kinderpornografisch materiaal hecht is. De ATKM ziet deze aanvullende rol vooralsnog niet op gebied van terroristische online inhoud. Voor kinderpornografisch materiaal is een classificatie doorgaans eenduidiger, terwijl bij terroristische online inhoud veel materiaal *borderline content* betreft, waardoor een vergelijkbare doorzetfunctie minder goed van de grond komt.

In het ATKM Jaarverslag van 2025 is een uitsplitsing opgenomen van de hoeveelheid materiaal per stap in het detectie en beoordelingsproces.[75] In totaal werden 1400 casussen onderzocht, werden 800 casussen doorgezet voor verdere beoordeling. In 460 gevallen is geoordeeld dat het ging op terroristische inhoud en uiteindelijk zijn 187 verwijderbevelen uitgestuurd. Het verschil tussen de 460 gevallen waarvan geoordeeld is dat het ging om terroristische inhoud en de 187 verwijderbevelen kan deels (maar niet uitsluitend) worden verklaard door het feit dat een deel van het materiaal door de HSP is verwijderd, terwijl de onderzoek- en analysefase bij de ATKM nog niet was afgerond. Dit materiaal is dus verwijderd vóór het oordeel van de ATKM.[76] In dergelijke gevallen verwijderen HSPs content bijvoorbeeld

---

68 Rode draad sessie, januari 2026; Interview met HSP, juni 2026.
69 Ibid.
70 Interview met opsporingsdienst, april 2026; Interview met opsporingsdienst, april 2026.
71 Rode draad sessie, januari 2026.
72 *Trusted flaggers* zijn aangewezen organisaties onder de DSA. Zij zijn gespecialiseerd in het detecteren van bepaalde soorten schadelijke online content en hebben de taak dit door te zetten naar online platformen en, indien nodig, toezichthouders.
73 Hierbij dient opgemerkt te worden dat geen van de Nederlandse DSA-flaggers terroristische online inhoud als expertise gebied hebben aangemerkt. Europese Commissie (n.d), Trusted flaggers under the Digital Services Act (DSA).
74 Interview met maatschappelijk middenveld, april 2026.
75 ATKM (2026), Jaarverslag 2025.
76 Schriftelijke Toelichting ATKM, juli 2026.

omdat deze niet voldoet aan de eigen gebruikersvoorwaarden. Het komt ook voor dat een bevoegde autoriteit in een andere lidstaat al eerder een bevel heeft verstuurd.

De ATKM geeft bovendien aan dat van alle geïdentificeerde content naar schatting slechts een kwart de beoordelingsfase bereikt. Het overige materiaal valt grotendeels af omdat het in *borderline* gebied blijft en niet als TOI gekwalificeerd kan worden.[77] Dit weerspiegelt deels een bewuste keuze van de ATKM voor zorgvuldigheid, maar ook structurele beperkingen van het instrument.

Los hiervan geldt dat de voornamelijk handmatige detectie, beperkt tot kantooruren, inhoudt dat een deel van de online terroristische inhoud naar verwachting nooit door de ATKM wordt geïdentificeerd. Een harde schatting van de omvang hiervan ontbreekt; EU-brede signalen wijzen wel op structurele beperkingen in geautomatiseerde detectie van schadelijke online content.[78] De ATKM (en andere toezichthouders in de EU-lidstaten) hebben daardoor mogelijk slechts zicht op een deel van de daadwerkelijke omvang van terroristische online inhoud.

Bij de content die wél wordt doorgezet naar de beoordelingsfase maakt de ATKM onderscheid tussen twee categorieën. Enerzijds is er reeds bekende, gestandaardiseerde content: materiaal dat inhoudelijk overeenkomt met eerder uitvoerig beoordeeld en juridisch gemotiveerd materiaal, zoals beelden van de aanslag in Christchurch in Nieuw-Zeeland (2019). Het gaat hierbij niet om een exacte technische match (zoals *hash-matching*), maar om een inhoudelijke herkenning dat dit hetzelfde fenomeen is waarvoor al een sluitende juridische onderbouwing bestaat. Voor deze categorie is een versnelde procedure van toepassing, waarbij na beoordeling door één beoordelaar direct een verwijderbevel kan worden opgesteld. Anderzijds is er nieuwe content: materiaal dat voor het eerst wordt aangetroffen en waarvan de kwalificatie als TOI nog niet is vastgesteld. Voor deze categorie geldt een uitgebreidere procedure met ten minste twee beoordelaars. Dit onderscheid is relevant voor de snelheid en de belasting van de beoordelingscapaciteit.

Zoals geïntroduceerd in hoofdstuk 2, is de beoordelingsprocedure zo ingericht dat altijd sprake is van dubbele toetsing. In de initiële werkwijze van de ATKM doorliep elk dossier achtereenvolgens een eerste beoordelaar, een tweede beoordelaar en het bestuur. Inmiddels is de interne mandatering aangepast: het bestuur hoeft niet langer bij elk bevel betrokken te zijn, maar dubbele inhoudelijke toetsing blijft altijd vereist.[79] Een uitzondering geldt voor gestandaardiseerde content: materiaal dat eerder uitvoerig is beoordeeld en gedocumenteerd (zoals beelden van de aanslag in Christchurch), kan via een versnelde procedure worden afgehandeld. Voor dergelijke content is één beoordelaar voldoende; de tweede toetsingslaag vervalt. Voor nieuw, niet eerder beoordeeld materiaal geldt de volledige procedure. Het bestuur van de ATKM voert regelmatig overleg met de beoordelaars om twijfelgevallen te bespreken en het corpus aan gestandaardiseerde content verder uit te breiden, met als doel het proces op termijn te versnellen.[80]

Een structureel knelpunt in deze fase is de zogenoemde *borderline content*: content die extremistisch of zorgwekkend is, maar niet of niet eenduidig onder de wettelijke definitie van

---

77 Interview met ATKM, mei 2026.
78 FRA (2023), Online content moderations: Current challenges in detecting hate speech.
79 Interview met ATKM, mei 2026.
80 Rode draad sessie, januari 2026.

terroristische online inhoud valt. Denk aan *memes* met gecodeerde extremistische boodschappen, opiniestukken die terroristische ideologie normaliseren zonder expliciete oproep tot geweld, of symboliek die afhankelijk van de context wel of niet als TOI kwalificeert. De beoordeling van dergelijk materiaal is tijdsintensief en vraagt om diepgaande inhoudelijke en juridische expertie.[81]

De ATKM ziet dit als een leeropgave: beter begrijpen waarom zoveel content niet als TOI kwalificeert, kan helpen het proces te verbeteren.[82] Om deze reden voert de organisatie casusanalyses en trendonderzoek uit. Het begrijpen waarom bepaalde content wel of niet als TOI wordt gekwalificeerd, draagt bij aan het aanscherpen van zoeklijsten, het verbeteren van beoordelingsprocessen en het verhogen van de effectiviteit van de organisatie op de lange termijn.[83] In de praktijk staat deze ambitie echter nog in de kinderschoenen: de ATKM houdt op dit moment geen systematische registratie bij van de doorlooptijd per casus en de capaciteit voor structurele trendanalyse is thans beperkt.[84]

3.1.2 Hoe frequent worden verwijderbevelen uitgevaardigd? Zijn er hierbij trends te ontwaren?

In 2024 heeft de ATKM ongeveer 150 verwijderbevelen uitgevaardigd, waarvan ongeveer 80 gericht op extreemrechts materiaal (60%) en 70 gericht op jihadistisch materiaal (40%). In 2025 heeft de ATKM 187 verwijderbevelen uitgevaardigd, waarvan 159 gericht op extreemrechts materiaal (85%), en 28 gericht op jihadistisch materiaal (15%). In de eerste helft van 2026 (tot en met 8 juli) heeft de ATKM 107 verwijderbevelen uitgevaardigd, waarvan 58 gericht op extreemrechts materiaal (54%) en 49 gericht op jihadistisch materiaal (46%).[85] [86]

Deze verdeling van bevelen op extreemrechts of jihadistisch materiaal zegt vooral iets over waar de ATKM haar detectie-inspanning op richt en welke content online het meest wordt aangetroffen; het weerspiegelt niet noodzakelijk de onderliggende dreigingsinschatting van de NCTV, waarin de jihadistische dreiging in Nederland onverminderd substantieel blijft, naast een groeiende zorg over de normalisering van rechts-extremistisch gedachtegoed en nihilistisch extremisme. De bevelen in 2024 resulteerden in de verwijdering of blokkering van ongeveer 80 kanalen; omdat één bevel doorgaans meerdere inhoudselementen tegelijk ontoegankelijk maakt, lag het werkelijke aantal verwijderde berichten en afbeeldingen aanzienlijk hoger.[87]

De ATKM houdt geen gegevens bij over of gedetecteerde content reeds bekend is bij de ATKM of dat dit ‘nieuwe’ content betreft. Wel kan op basis van de ervaringen van detectie- en beoordelingsmedewerkers worden gesteld dat met grote regelmaat ‘soortgelijk’ materiaal wordt gedetecteerd. Het gaat dan om bijvoorbeeld (beelden van) livestreams, manifesten of content over bekende aanslagplegers. Vaak betreft het materiaal dat wordt ‘gerecycled’; het

---

81 Ministerie Justitie en Veiligheid (2023), Contourenbrief Versterkte Aanpak Online extremistische en terroristische content; Saltman, E. & Hunt, M. (2023), Borderline Content: Understanding the Gray Zone.

82 Ibid.

83 Ibid.

84 Interview met ATKM, april 2026.

85 Schriftelijke toelichting ATKM, juli 2026.

86 Op basis van deze cijfers kunnen geen conclusies worden getrokken met de betrekking tot de hoeveelheid van beide typen materiaal die aanwezig is op internet, noch over de focus van de ATKM. Aangezien werkprocessen in ontwikkeling zijn en de algehele focus van de ATKM op het internet nog onvolledig is, kan de verhouding (met name over 2025) het gevolg zijn van de relatief gemakkelijke vindbaarheid van rechts-terroristisch materiaal op specifieke socialemediaplatforms die door de ATKM zijn onderzocht (toelichting ATKM).

87 ATKM (2025), Jaarverslag 2024.

materiaal wordt niet één op één opnieuw verspreid maar wordt bijvoorbeeld met AI of andere *tooling* in een format gestoken. Ook kan het 'bekend' materiaal zijn waaraan kleine aanpassingen worden gedaan, zoals toevoeging van logo's of toepassing van vormen van '*blurring'*. Dit soort 'bekende' materiaal is het materiaal waarop de standaardisering van de werkprocessen binnen het primaire proces van de ATKM zich richt (zie ook paragraaf 2.2). Er wordt binnen de ATKM om die reden relatief veel 'bekend' materiaal verwerkt.[88]

Het aantal bevelen dat Nederland uitvaardigt, is internationaal niet rechtstreeks vergelijkbaar, mede omdat lidstaten verschillende instrumenten en rolverdelingen hanteren. Ter illustratie: Duitsland verstuurde in 2024 245 verwijderbevelen, daarnaast bijna 30.000 niet-bindende referrals of verwijderverzoeken.[89] De meeste lidstaten werken primair met referrals en grijpen pas naar een formeel bevel bij niet-naleving. De Europese Verordening geeft in haar preambule expliciet weer dat de Verordening de mogelijkheid voor het werken met verwijderverzoeken niet belemmert. Bij de oprichting van de ATKM is door het ministerie een bewuste beleidsmatige keuze gemaakt om enkel met bevelen te werken bij gekwalificeerde TOI-content. De ATKM geeft opvolging aan deze keuze. De Nederlandse Uitvoeringswet TOI specificeert de mogelijkheid om verzoeken uit te vaardigen niet expliciet, maar sluit die mogelijkheid ook niet uit (meer hierover in paragraaf 3.2).

Een van de voordelen van de inzet van een verwijderbevel is dat bij niet-naleving direct handhavend opgetreden kan worden. Gezien de ernst van het materiaal en het doel om (verdere) verspreiding tegen te gaan, beschouwt de ATKM een verwijderbevel als passend instrument. Een verwijderverzoek vereist een vergelijkbare onderbouwing als een verwijderbevel maar heeft als voordeel dat het minder tijdsinvestering vergt (er hoeft geen formeel verwijderbevel opgesteld te worden). De keuze om naast verwijderbevelen geen gebruik van de verwijderverzoeken te maken, drukt het totale output volume in Nederland.(zie ook paragraaf 3.2).[90]

Op Europees niveau houdt Europol data bij over het aantal uitgestuurde verwijderbevelen en verwijderverzoeken via PERCI op het gebied van 'terrorisme'.[91] Wanneer deze Europese cijfers afgezet worden tegen de cijfers van de ATKM valt op dat de ATKM verantwoordelijk is voor een aanzienlijk aandeel van de verwijderbevelen in 2024 en 2025; van de in totaal 1703 verstuurde verwijderbevelen door de bevoegde autoriteiten in de Europese lidstaten werden er ongeveer 330 verstuurd door de ATKM. Dit staat gelijk aan 20%. Daarnaast valt op dat het aantal verstuurde verwijderbevelen tussen 2024 en 2025 terugliep (een afname van 33%).[92] Tegelijkertijd neemt het aantal verstuurde verwijderverzoeken toe. Tussen 2024 en 2025 is sprake van een toename van bijna 100%. In de eerste zes maanden van 2026 zijn bovendien al meer verwijderbevelen uitgegeven dan in het volledige jaar 2025. Zie voor een uitgebreidere analyse ten aanzien van de verwijderverzoeken ook paragraaf 3.2.

---

88 Schriftelijke toelichting ATKM, juli 2026.
89 Interview academici, april 2026.
90 Interview met ATKM, april 2026.
91 Schriftelijke informatie gedeeld door Europol, juli 2026.
92 De cijfers voor 2023 en 2026 omvatten slechts een half jaar en worden daarom niet meegenomen in deze afweging.

Tabel 3.1 Europol data van 3 juli 2023 – 30 juni 2026 ten aanzien van uitgestuurde verwijderbevelen en verwijderverzoeken via PERCI op gebied van terrorisme (EU gecombineerd)

	03/07/2023-31/12/2023	01/01/2024-31/12/2024	01/01/2025-31/12/2025	01/01/2026-30/06/2026
Verwijderbevelen	329	1022	681	372
Verwijderverzoeken	6623	22346	45734	47841
Totaal	**6952**	**23368**	**46415**	**48213**

Ook hier is een structureel aandachtspunt borderline content: content die extremistisch of zorgwekkend is, maar niet eenduidig als terroristische online inhoud kwalificeert. De ATKM signaleert dat haar detectieteam regelmatig materiaal aantreft dat schuurt aan de definitie van terroristische online inhoud, maar er net niet aan voldoet. Hierdoor kan de organisatie, gegeven het wettelijk mandaat dat strikt op terroristische content is gericht, geen actie ondernemen. De ATKM gaat graag het gesprek aan met (onder meer) de NCTV als onderdeel van het ministerie van Justitie en Veiligheid in bredere zin om de mogelijkheid om niet-bindende verwijderverzoeken ook te kunnen inzetten voor zorgwekkende extremistische content die niet als terroristische online inhoud gekwalificeerd kan worden.[93] Dit gesprek zou dan onderdeel zijn van een bredere discussie ten aanzien van de wenselijkheid van het uitbreiden van het mandaat/instrumentarium van de ATKM.

In het huidige kader werkt de ATKM samen met andere lidstaten aan een gemeenschappelijke taxonomie voor terroristische online inhoud, die moet bijdragen aan een uniformere interpretatie en toepassing van de definitie.[94]

3.1.3 In welke mate geven hostingdiensten en internetplatformen daadwerkelijk en tijdig opvolging aan verwijderbevelen (inclusief de één-uursregel)?

Het speelveld van HSPs waarop extremistische en terroristische content circuleert, is divers en gelaagd. Aan de ene kant zijn er grote, bekende sociale mediaplatforms, zoals Meta, TikTok, X, YouTube en Telegram, die beschikken over uitgebreide moderatiesystemen en geautomatiseerde detectietools. Naar schatting wordt een groot deel van de illegale en terroristische content op deze platformen al via geautomatiseerde AI-systemen gedetecteerd, voordat enige autoriteit in beeld komt.[95] Grote platforms hebben doorgaans gebruikersvoorwaarden die verder gaan dan wat de wet minimaal vereist, mede omdat zij de capaciteit en middelen hebben om deze actief te handhaven en omdat eigen, strikte gebruikersnormen doorgaans eenvoudiger te handhaven zijn dan de juridisch genuanceerde TOI-definitie.[96]

Aan de andere kant zijn er kleinere en zogenoemde *fringe*-platformen: nichesites, gamingomgevingen, alternatieve fora en sociale netwerken met beperkte of afwezige moderatie. Op deze platformen circuleert een aanzienlijk deel van extremistisch en terroristisch materiaal, juist omdat de drempel voor het plaatsen en handhaven van dit materiaal laag is.[97] Kleine

---

93 Interviews met ATKM, april en mei 2026.
94 Interview met ATKM, mei 2026; ATKM (2025), Jaarverslag 2024.
95 Interview met maatschappelijk middenveld, april 2026.
96 Interview met maatschappelijk middenveld, april 2026; Interview met ministerie Economische Zaken en Klimaat, maart 2026.
97 Peeters, T., van Wonderen, R., Burggraaff, D. & de Wit, N. (2022), Online extreemrechtse Radicalisering: Handvatten voor een preventieve aanpak; NCTV (2024), Fenomeenanalyse Memes als online wapen.

HSPs beschikken doorgaans over minder juridische kennis en minder technische capaciteit om bevelen snel te verwerken.

Daarnaast zijn er platformen met open of gesloten communicatietools. Bij terroristische online inhoud speelt ook besloten communicatie een toenemende rol: versleutelde kanalen via apps als WhatsApp en Telegram. Deze omgevingen vallen buiten de reikwijdte van de EU-verordening, die uitsluitend betrekking heeft op voor het publiek toegankelijke inhoud op hostingdiensten.

Tot slot vormen de zogenoemde 'dakloze' HSPs een bijzondere categorie platformen: aanbieders zonder een hoofdvestiging of wettelijke vertegenwoordiging in de EU. Voor deze partijen zijn de mogelijkheden tot handhaving beperkt. Zij zijn moeilijker te bereiken, minder responsief op bevelen en bieden feitelijk weinig aanknopingspunten voor toezicht of sanctionering. Er is geen bereikbaar correspondentieadres en boetes of dwangsommen zijn in de praktijk niet afdwingbaar buiten de EU-rechtsmacht.[98] Nederland denkt samen met Zweden na over mogelijkheden om dakloze HSPs beter te bereiken, maar concrete instrumenten ontbreken vooralsnog om in breder EU-verband te behandelen.[99]

Het is tegen deze achtergrond, een gefragmenteerd en deels ongrijpbaar online landschap, dat de ATKM haar werk doet. De kenmerken van het HSP-landschap bepalen in hoge mate hoe effectief de wet in de praktijk is. Desalniettemin zijn vrijwel alle verwijderbevelen die de ATKM uitvaardigde binnen de wettelijke termijn van 1 uur nagekomen.[100] De ATKM hanteerde tot voor kort een relatief pragmatische lijn: kleine overschrijdingen (van een paar minuten) werden niet formeel gesanctioneerd. Op het moment van schrijven hanteert de ATKM een strikt beleid ten aanzien van termijnoverschrijdingen. Er zijn tot op heden geen boetes of dwangsommen opgelegd wegens niet-naleving.[101]

Boetes en dwangsommen

In juni 2026 heeft de ATKM een dwangsom- en boetebeleid gepubliceerd (zie ook paragraaf 2.1).[102] Tot op heden zijn geen boetes of dwangsommen opgelegd wegens niet-naleving. Ten aanzien van dit proces en de passendheid van deze sancties kan in dit onderzoek daarom geen uitspraak worden gedaan.

Wat opvalt, is de hoogte van de boetes en dwangsommen. Boetes bedragen maximaal € 1.100.000 of, in een geval van systematische niet-naleving, maximaal 4% van de jaaromzet van de aanbieder. Eventueel kan daarnaast een dwangsom van € 20.000 op worden gelegd.

Ter illustratie, de jaarlijkse omzet van de twee beursgenoteerde HSPs met een hoofdvestiging of wettelijke vertegenwoordiging in Nederland bedroeg in 2025 ongeveer € 5 miljard.[103]

Grote platforms als TikTok, Discord en Telegram beschikken over gestructureerde processen voor het verwerken van bevelen en geven doorgaans snel opvolging. Europol signaleert dat

98 Rode draad sessie, januari 2026.
99 Rode draad sessie, januari 2026; Interview met ATKM, mei 2026.
100 ATKM (2025), Jaarverslag 2024.
101 Rode draad sessie, januari 2026.
102 ATKM (2026), Dwangsom- en boetebeleid Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM).
103 Snap Inc. (2025), Annual report 2025.

content bij grotere HSPs soms al verwijderd is op het moment dat een bevel arriveert. Platforms modereren intern sneller dan een toezichthouder formeel kan optreden.[104] Kleinere, HSPs met een hoofdvestiging of wettelijke vertegenwoordiging in de EU hebben minder technische capaciteit, maar waarderen de duidelijkheid van een bindend bevel: de inhoudelijke beslissingsverantwoordelijkheid ligt dan niet bij henzelf, wat juridische risico's voor de HSP vermindert.[105]

Tot slot ligt het werkelijke knelpunt in de keten niet bij de naleving na ontvangst door de HSP, maar bij de doorlooptijd van de detectie door de ATKM tot de verzending van het bevel. De Uitvoeringswet TOI legt geen wettelijke verplichtingen op aan de toezichthouder over de maximale doorlooptijd om bevelen uit te sturen, maar wel aan HSPs over het verwijderen van terroristische online inhoud binnen één uur. Er zijn daarbij enkele momenten die de tijdslijn van het proces beïnvloeden. Allereerst het deconflictieproces, waarbij de ATKM 48 uur wacht op de politie voordat een bevel wordt verstuurd. Dit verlengt de periode waarin terroristische online inhoud online blijft en toegankelijk is.

Een tweede moment is dat sommige platforms hun eigen systemen hebben voor het ontvangen van bevelen, wat betekent dat een bevel in de praktijk via meerdere kanalen tegelijk moet worden verstuurd. Het gehele administratieve proces (van het opstellen en aftekenen van het bevel tot en met de invoer in PERCI en de feitelijke verzending) kost aanzienlijk meer tijd dan de wettelijke één-uursregel (voor HSPs) doet vermoeden. In het snelste geval, bij gestandaardiseerde content, kan een bevel theoretisch binnen een uur worden verstuurd; in de praktijk vergt het volledige traject van detectie tot verzending aanzienlijk meer tijd.[106] Hoeveel tijd precies is niet met zekerheid te zeggen. Dit wordt ook niet systematisch door de ATKM bijgehouden. Wel wordt er door de organisatie actief gekeken naar manieren om de doorlooptijd te verkorten. Bijvoorbeeld, tijdens het deconflictieproces worden al andere taken rondom de voorbereiding van een bevel uitgevoerd om zo tijd te besparen.

3.1.4 Wat zijn de ervaringen van hostingdiensten en internetplatformen met het proces rondom bevelen en rondom bezwaar- en beroepsprocedures?

Het directe perspectief van individuele HSPs is in dit onderzoek beperkt beschikbaar gebleven. Ondanks gerichte pogingen hebben slechts twee van de aangeschreven grote platforms een interview toegekend. Op basis van de transparantierapporten van platforms, gesprekken met het maatschappelijk middenveld, het ministerie van Economische Zaken en Klimaat en twee HSPs ontstaat het volgende beeld.[107]

Vanuit de sector zijn er weinig klachten over verwijderbevelen. De duidelijke illegaliteit van terroristische online inhoud zorgt er vermoedelijk voor dat zowel platforms als gebruikers weinig aanleiding zien tot bezwaar of beroep; beide partijen weten doorgaans dat het om illegale content gaat.[108] Voor kleinere HSPs met beperkte juridische slagkracht geldt bovendien dat een bindend bevel juist duidelijkheid verschaft: de verantwoordelijkheid voor de

---

[104] Interview met opsporingsdienst, maart 2026.
[105] Interview met maatschappelijk middenveld, april 2026.
[106] Interview met ATKM, mei 2026; Rode draad sessie, januari 2026.
[107] Interview met HSP, april 2026; Interview met HSP, juni 2026; Interview met maatschappelijk middenveld, april 2026; Interview met ministerie Economische Zaken en Klimaat, maart 2026.
[108] Interview met ministerie Economische Zaken en Klimaat, maart 2026.

inhoudelijke beoordeling ligt dan bij de ATKM, niet bij henzelf, wat juridische risico's voor het platform vermindert.[109]

Een punt van aandacht is de eventuele onduidelijkheid voor HSPs over het verschil tussen verwijderverzoeken versus bevelen. Hoewel de ATKM alleen bindende bevelen uitstuurt, kunnen HSPs van bevoegde autoriteiten uit andere lidstaten mogelijk wél verwijderverzoeken ontvangen.[110] HSPs ervaren een verzoek van een overheidsinstantie niet als vrijblijvend en voelen informele druk om hierop te acteren, ook zonder dat de rechtswaarborgen van een formeel bevel van toepassing zijn. Dit brengt het risico met zich mee dat content wordt verwijderd zonder de zorgvuldigheidstoets die een bevel vereist, terwijl bij twijfel over de kwalificatie juist die toets het meest noodzakelijk is. Dit risico wordt expliciet benoemd: de verantwoordelijkheid om te beoordelen of content verwijderd moet worden, ligt bij de bevoegde autoriteit, niet bij het platform.[111] HSPs geven aan behoefte te hebben aan een gestandaardiseerd format dat het onderscheid tussen een verwijderverzoek en een verwijderbevel verduidelijkt. Hierbij spelen ook verschillen in aanpak tussen verschillende (bevoegde autoriteiten in) lidstaten een rol. Kleine HSPs hebben weinig zicht op welke bevoegde autoriteiten in de EU bestaan en over welke bevoegdheden zij beschikken. Een overzicht hiervan zou hun rechtspositie versterken.[112]

De uitvoerbaarheid van de één-uursregel wordt door geïnterviewde platforms als een aandachtspunt beschouwd. Grotere platforms beschikken doorgaans over geautomatiseerde systemen voor het verwerken van bevelen, al blijft menselijke eindtoetsing vereist.[113] Voor de uitwisseling van informatie met toezichthouders adviseren platforms gespecialiseerde tools (zoals Kodex Global) die overheidsinstanties en platforms in staat stellen data gestandaardiseerd en veilig uit te wisselen, als alternatief voor de huidige gefragmenteerde communicatiekanalen.[114] Open-source tools zoals AbuseIO bieden kleinere HSPs een laagdrempelige oplossing om het afhandelingsproces te ondersteunen, maar het is onduidelijk in hoeverre Nederlandse HSPs hiervan in de praktijk gebruikmaken of wat de veiligheids- en privacy implicaties zijn.[115]

Een geïnterviewd platform illustreert een bredere spanning rondom de één-uursregel. Om te kunnen voldoen aan de verplichting om bevelen te allen tijde binnen één uur op te volgen, heeft dit platform een systeem ingericht waarbij medewerkers in verschillende tijdszones permanent beschikbaar zijn. Dit vergt een aanzienlijke organisatorische en personele investering vanuit de HSPs. In de praktijk blijkt deze investering echter moeilijk te rechtvaardigen: het platform heeft tot op heden slechts een handvol verwijderbevelen van EU-lidstaten ontvangen en vrijwel alle bevelen werden tijdens kantooruren verstuurd. De feitelijke last van 24/7-bereikbaarheid staat daarmee in geen verhouding tot het werkelijke volume aan bevelen. Dit platform stelt dat een heroverweging van de één-uursregel, of ten minste een normering die rekening houdt met het verzendmoment, wenselijk zou zijn.[116]

---

109 Interview met maatschappelijk middenveld, april 2026.
110 Zie voor reflecties ten aanzien van mogelijkheden voor de ATKM om verwijderverzoeken te versturen paragraaf 3.2.
111 Interview met ministerie Economische Zaken en Klimaat, maart 2026.
112 Interview met maatschappelijk middenveld, april 2026.
113 Interview met HSP, juni 2026.
114 Interview met HSP, april 2026.
115 Interview met maatschappelijk middenveld, april 2026.
116 Interview met HSP, april 2026.

HSPs zijn naar eigen zeggen in de praktijk aanzienlijke tijd en capaciteit kwijt om te voldoen aan de verplichtingen die de EU-verordening en aanverwante wetgeving hen opleggen. De samenloop van TOI-verplichtingen, DSA-verplichtingen en andere nationale en Europese regelgeving maakt het voor met name kleinere HSPs complex om het juridische kader te overzien. Dit laat zien dat coördinatie tussen verschillende Europese regelgevingskaders een aandachtspunt is voor de uitvoerbaarheid van de verplichtingen in de praktijk.[117]

3.1.5 Wordt er in de praktijk gebruikgemaakt van bezwaar of beroep? Hoe vaak en met welk resultaat?

Tot op heden zijn er geen bezwaar- of beroepsprocedures gestart tegen een verwijderbevel van de ATKM.[118] Dit hoeft niet te betekenen dat er geen spanning bestaat rondom de bevelen. Een waarschijnlijke verklaring is dat de duidelijke illegaliteit van terroristische online inhoud weinig aanleiding geeft tot betwisting.[119] Daarnaast is het denkbaar dat de lage prikkel tot bezwaar- en beroep samenhangt met vertrouwen in het oordeel van de ATKM, onbekendheid met de beschikbare procedures of een kosten-batenafweging.

Dat er tot op heden geen gebruik is gemaakt van bezwaar- en beroepsprocedures heeft één belangrijke implicatie: de inhoudelijke beoordelingscriteria van de ATKM zijn tot op heden niet onafhankelijk door een rechter getoetst. Als de ATKM in de toekomst gaat opschalen en wellicht vaker borderline content betrekt, neemt de kans op procedures toe. Verschillende gesprekspartners verwachten dat dit in de toekomst een relevanter vraagstuk zal worden.[120]

3.1.6 Wordt er in de praktijk door de ATKM gebruikgemaakt van de mogelijkheid tot een blootstellingsbesluit en wat zijn de verklarende factoren?

De ATKM heeft tot op heden geen blootstellingsbesluiten uitgevaardigd, hoewel zij dit instrument inhoudelijk waardevol acht en bezig is met het opstellen van een concept-procedure.[121] Voor het uitblijven van toepassing door de ATKM zijn meerdere verklarende factoren aan te wijzen.

Ten eerste ontbreekt een helder en uniform (Europees) kader voor de inzet van het instrumentarium. De EU-verordening laat het aan lidstaten zelf om invulling te geven aan de procedure, wat internationaal heeft geleid tot aanzienlijke onderlinge verschillen. Van de lidstaten die al blootstellingsbesluiten hebben uitgevaardigd (met name Ierland en Duitsland), zijn de procedures onderling niet vergelijkbaar. De ATKM wacht op de uitkomsten van een EU-werkgroep, die zich over harmonisering buigt.[122]

Ten tweede beperkt de inrichting van de Nederlandse wet in de ogen van de ATKM de werkbaarheid ervan. De combinatie van het blootstellingsbesluit met de geschilbeslechtings-procedure van artikel 16 Uitvoeringswet TOI maakt de procedure in Nederland complexer dan in andere lidstaten: een HSP die na een blootstellingsbesluit maatregelen neemt die

---

117 Interview met maatschappelijk middenveld, april 2026; Interview met ministerie Economische Zaken en Klimaat, maart 2026.
118 Interview met ATKM, april 2026; Interview met ministerie Economische Zaken en Klimaat, maart 2026.
119 Interview met ministerie Economische Zaken en Klimaat, maart 2026.
120 Interview met maatschappelijk middenveld, maart 2026; Interview met academici, april 2026.
121 Interview met ATKM, april 2026.
122 Interviews met ATKM, april 2026.

vervolgens door een gebruiker worden betwist, legt die klacht neer bij diezelfde HSP en uiteindelijk bij de ATKM. Die laatste treedt daarmee op als geschilbeslechter over maatregelen die zij zelf heeft afgedwongen.[123] Deze constructie wordt door de ATKM als ongemakkelijk ervaren.[124]

Ten derde is de effectiviteit van het instrument beperkt. De EU-verordening legt de HSP uitsluitend een inspanningsverplichting op, geen resultaatverplichting. Dit maakt het voor de ATKM moeilijk te beoordelen of een aanbieder voldoende preventieve maatregelen heeft genomen en daarmee ook moeilijk om handhavend op te treden bij onvoldoende naleving.[125]

Ten vierde speelt een capaciteitsoverweging. De beperkte bezetting op het primaire proces, in het bijzonder het ontbreken van voldoende juridische capaciteit, maakt dat de ATKM haar beschikbare menskracht noodgedwongen concentreert op het primaire instrument: het verwijderbevel. Het voorbereiden en begeleiden van een blootstellingsprocedure, inclusief eventuele geschilbeslechting, legt naar verwachting een beslag op de beschikbare juridische capaciteit.[126]

3.1.7 Hoe wordt de mogelijkheid tot geschilbeslechting ervaren?

De geschilbeslechtingsprocedure van artikel 16 Uitvoeringswet TOI is tot op heden evenmin benut. Nederland is de enige EU-lidstaat die een dergelijke procedure heeft opgenomen in de implementatiewet: een directe uitkomst van het politieke debat in de Tweede Kamer, dat bij de totstandkoming van de wet sterk gericht was op rechtsbescherming en het voorkomen van overmoderatie.[127] De procedure biedt gebruikers van internetinhoud een extra mogelijkheid om een verwijderd stuk content ter beoordeling voor te leggen: zij kunnen eerst een klacht indienen bij de HSP, en het geschil voorleggen aan de ATKM als die klacht niet naar tevredenheid wordt afgehandeld.

De ATKM heeft aangegeven deze rol als capaciteitsintensief te ervaren en vraagt zich af of de geschilbeslechtingsprocedure doeltreffend is. Ze noemt met name het ontbreken van heldere kaders omtrent de beoordeling van de klachtafhandeling als problematisch. Bovendien beschouwt de ATKM de dubbele rol die zij heeft als complex: als autoriteit neemt zij blootstellingsbesluiten en als geschillenbeslechter bestaat de kans dat zij (de acties die voortvloeien uit) de besluiten moet toetsen. De ATKM beschouwt de rechtsbescherming op grond van de Europese Verordening en de DSA bovendien als afdoende en ziet, vanwege bovenstaande, de procedure het liefst uit de wetgeving verdwijnen.[128]

Tussenbalans: een instrumentarium dat grotendeels onbenut blijft

De bevindingen over bezwaar- en beroepsprocedures, blootstellingsbesluit en geschilbeslechting laten samen een opvallend patroon zien. De Uitvoeringswet TOI heeft de ATKM in theorie een breed instrumentarium meegegeven: naast het verwijderbevel beschikt zij over het blootstellingsbesluit, de last onder dwangsom, de bestuurlijke boete en de

---

[123] De ATKM neemt een besluit over het nemen van specifieke maatregelen. De HSP bepaalt vervolgens welke maatregelen dit zijn (zie artikel 5 van de verordening onder lid 2: "Het besluit over de keuze van de specifieke maatregelen blijft bij de aanbieder van hostingdiensten berusten").

[124] Interview met ATKM, april 2026; Artikel 16, Uitvoeringswet TOI.

[125] Interviews met ATKM, april 2026.

[126] Interview met ATKM, april 2026; Interview met ATKM, mei 2026.

[127] Interview met ATKM, april 2026; Artikel 16, Uitvoeringswet TOI.

[128] Interview met ATKM, april 2026; Rode draad sessie, januari 2026 en schriftelijke toevoeging augustus 2026.

geschilbeslechtingsprocedure. In de praktijk maakt de ATKM uitsluitend gebruik van het verwijderbevel.

Dit is deels het gevolg van bewuste strategische keuzes. De ATKM hecht aan een constructieve relatie met platforms en kiest voor een pragmatische, samenwerkingsgerichte opstelling ter verwijdering van TOI. Deels is het een gevolg van externe factoren die buiten de invloedssfeer van de ATKM liggen: het ontbreken van een uniforme Europese werkwijze voor het blootstellingsbesluit en de spanning tussen de geschilbeslechtingsprocedure en de uitvoering van bevelen. Deels is het een gevolg van capaciteitsbeperkingen: de ATKM heeft naar eigen zeggen onvoldoende juridische en operationele ruimte om haar volledige instrumentarium te benutten.

De vraag die hieruit volgt voor deze evaluatie is of de wet in haar huidige vormgeving, en met de huidige capaciteit van de ATKM, voldoende slagkracht biedt voor de lange termijn, of dat

de structurele onderbenutting van het instrumentarium een fundamenteler probleem weerspiegelt dat zowel in de wetgeving als in de uitvoering om adressering vraagt.[129]

Juiste toepassing en naleving van verwijderbevelen in andere lidstaten
De wijze waarop lidstaten verwijderbevelen inzetten, verschilt aanzienlijk. Het meest in het oog springende verschil betreft de verhouding tussen bindende bevelen en niet-bindende verwijderverzoeken. In Duitsland verstuurde het Bundeskriminalamt (BKA) in 2024 ruim 17.000 verwijderverzoeken, naast 482 verwijderbevelen; een verhouding van circa 35:1. Het nalevingspercentage op verzoeken lag op 87%, op bevelen op 96%. Het BKA grijpt primair naar een verzoek en zet een formeel bevel alleen in bij niet-naleving of hoge urgentie.[130] Nederland hanteert een fundamenteel andere aanpak: uitsluitend bindende bevelen, geen verzoeken. Onze indruk is dat dit impact heeft op het outputvolume, maar wel garantie geeft voor een hoge gemiddelde zorgvuldigheid per beslissing.

In Ierland ontvangt Coimisiún na Meán (CNAM) als bevoegde autoriteit een relatief hoog volume aan grensoverschrijdende bevelen, omdat veel grote platforms (waaronder Meta, TikTok en Google) een hoofdvestiging of wettelijke vertegenwoordiging in Ierland hebben. Daarmee is Ierland primair verantwoordelijk voor het toezicht op naleving door deze partijen wanneer andere lidstaten bevelen uitvaardigen. Dit levert een specifiek type druk op: niet zozeer het uitvaardigen van bevelen, maar het monitoren van de naleving ervan door de grootste platforms ter wereld.[131] In Zweden is Spotify AB de meest bekende ontvanger van nationale verwijderbevelen en heeft daarnaast ook een blootstellingbesluit op haar naam staan. Dit is een mechanisme dat de ATKM tot op heden nog niet heeft hoeven hanteren, maar dat wel illustreert hoe de vestigingsplaats van een HSP de rolverdeling tussen lidstaten bepaalt.[132]

Bezwaar- en beroepsprocedures zijn ook in andere lidstaten nauwelijks ingezet. In Duitsland heeft het BNetzA (*Bundesnetzagentur*) tot op heden geen bezwaren ontvangen tegen de door haar opgelegde sancties. Dit patroon bevestigt dat het uitblijven van bezwaren geen Nederlands fenomeen is, maar vermoedelijk samenhangt met de duidelijke illegaliteit van terroristische online inhoud en de lage prikkel tot betwisting voor zowel platforms als inhoudsaanbieders.[133]

---

129 Interview met ATKM, april 2026; Interview met ATKM, mei 2026; Interview met ministerie Economische Zaken en Klimaat, maart 2026.
130 Interview met bevoegde autoriteit Duitsland, maart 2026; Interview met bevoegde autoriteit Duitsland april 2026.
131 Interview met bevoegde autoriteit Ierland, mei 2026.
132 Interview met bevoegde autoriteit Zweden, mei 2026.
133 Interview met bevoegde autoriteit Duitsland, maart 2026.

3.2 Juridische aspecten van verwijderbevelen

Bevindingen in het kort

- De verwijderbevelen van de ATKM vallen binnen de kaders van de vrijheid van meningsuiting (artikel 7 Grondwet, artikel 10 Europees Verdrag voor de Rechten van de Mens).
- De ATKM hanteert een handmatige, meerlaagse beoordelingsprocedure met expliciete grondrechtelijke weging; er zijn geen aanwijzingen voor *chilling effects* of overblokkering.
- Externe rechterlijke validatie heeft tot op heden niet plaatsgevonden: er zijn geen bezwaar- of beroepsprocedures gestart.
- De Uitvoeringswet TOI sluit verwijderverzoeken niet expliciet uit; de meningen over wenselijkheid van het gebruik van verwijderverzoeken zijn verdeeld.
- Een helder mandaat om tevens op te treden tegen *borderline content* ontbreekt.
- De balans tussen effectiviteit en rechtsstatelijke bescherming is in de huidige praktijk voldoende geborgd, maar wordt bij verdere opschaling en inzet van zwaardere instrumenten kwetsbaarder.

3.2.1 In hoeverre valt de reikwijdte van verwijderbevelen binnen de kaders van de in Nederland beschermde grondrechten, met name de vrijheid van meningsuiting?

Artikel 7 van de Grondwet stelt dat niemand voorafgaande toestemming van de overheid nodig heeft om iets in het openbaar te zeggen of te schrijven. Het grondrecht heeft ook betrekking op het recht van eenieder om te lezen, luisteren of kijken wat men wil, zonder dat daarvoor toestemming nodig is. Deze rechten gelden ook voor de online dimensie. Het recht op vrijheid van meningsuiting is echter niet onbeperkt. Uitingen die verboden zijn op grond van het strafrecht vallen niet onder de vrijheid van meningsuiting. Met andere woorden, de vrijheid van meningsuiting kan worden beperkt, mits aan strikte voorwaarden is voldaan. Aangezien het internationaal recht boven het nationaal recht gaat, is het van belang om ook het Europees Verdrag voor de Rechten van de Mens (EVRM) in dit kader te beschouwen. Het EVRM is bovendien rechtstreeks toepasselijk in de Nederlandse jurisdictie en individuen kunnen daar rechten aan ontlenen. Er is een zekere overlap tussen de Grondwet en het EVRM, maar aangezien het EVRM de voorwaarden in artikel 10 EVRM ten aanzien van beperking van de vrijheid van meningsuiting gedetailleerd heeft uitgewerkt, dienen deze hier als leidraad:

- De beperking moet bij wet zijn, zoals het Wetboek van Strafrecht of in dit geval (ook) een EU-Verordening.
- De beperking moet een legitiem doel dienen dat genoemd wordt in artikel 10 van het EVRM. Een legitiem doel kan zijn de bescherming van de nationale veiligheid, de preventie van het plegen van misdrijven of het beschermen van de reputatie en goede naam van anderen.
- De beperking moet bovendien noodzakelijk zijn in een democratische samenleving. Dit vertaalt zich naar een proportionaliteitstoets en een noodzakelijkheidstoets. Met andere woorden: zijn er geen andere manieren om hetzelfde doel te bereiken en is de inbreuk proportioneel aan het te beschermen belang.

De uiteindelijke beoordeling van de vraag of er wel of niet sprake is van een schending van grondrechten is voorbehouden aan de rechter.

Een verwijderbevel is een beperking van de vrijheid van meningsuiting, maar - indien correct uitgevoerd - geen schending van het recht op vrijheid van meningsuiting. De vraag die hieronder wordt beantwoord, is of de wijze waarop de Uitvoeringswet TOI de ATKM mandateert om verwijderbevelen uit te vaardigen, in de praktijk valt binnen de kaders van de rechten zoals beschermd door de Grondwet.

De opdracht van de ATKM is om ervoor te zorgen dat content die kwalificeert als TOI van het internet wordt verwijderd. Dit doet de ATKM door middel van het uitvaardigen van een verwijderbevel. Bij de beoordeling van content en om zorgvuldig af te wegen of een verwijdering plaatsvindt conform de vereisten die gesteld worden aan een beperking op het recht op vrijheid van meningsuiting, kijkt de ATKM daarom in eerste instantie of de betreffende content valt binnen wat volgens de EU-verordening en de Uitvoeringswet TOI is gekwalificeerd als terroristische online inhoud. Enkel als de content binnen deze reikwijdte valt, wordt overwogen of een verwijderbevel noodzakelijk is.

Om vast te stellen of er sprake is van terroristische online inhoud moet echter voor de definitie van wat als terroristische inhoud te kwalificeren is een beoordeling in twee stappen plaatsvinden. In de eerste instantie moet worden gekeken naar de definitie van terroristische online inhoud zoals verwoord in artikel 2(7) van de EU-verordening 2021/748. Voor wat te kwalificeren is als ‘terrorisme’ dient in tweede instantie gekeken te worden naar artikel 3 van de EU-richtlijn 2017/541 van het Europese Parlement en de Raad van 15 maart 2017. In deze Richtlijn wordt vastgelegd wat terroristische misdrijven zijn.

De kritiek in de literatuur op deze dubbelslag bij de beoordeling van terroristische online inhoud richt zich onder meer op het feit dat zowel bij de EU-verordening als bij de Uitvoeringswet TOI het uitgangspunt is dat er preventief gemodereerd wordt op vermeende terroristische online inhoud. Er komt dus geen onafhankelijk rechterlijk oordeel in een strafzaak aan te pas ten aanzien van de vraag of er inderdaad sprake is van een terroristisch oogmerk zoals bedoeld in artikel 3 van EU Richtlijn 2017/541.[134] De zorg gaat met name uit naar de onafhankelijkheid van private partijen bij het beoordelen van de TOI en de beperkte tijd die beschikbaar zou zijn om tot zo'n oordeel te komen. Nu de beoordeling echter is belegd bij de ATKM, die juist als onafhankelijke zbo (zie paragraaf 3.4.1 over de rol van de ATKM als zbo) handmatig (en niet op basis van geautomatiseerde systemen) beoordeelt, is het oordeel van de onderzoekers van deze evaluatie dat deze zorg ongegrond is.

Beoordeling vereisten voor inperking vrijheid van meningsuiting

Het eerste vereiste voor een gegronde inperking van het recht op vrijheid van meningsuiting door middel van het uitvaardigen van een verwijderbevel, namelijk dat deze actie een grond vindt in de wet, is daarmee in de ogen van de onderzoekers in voldoende mate vervuld.

Het tweede vereiste, namelijk dat de inperking een legitiem doel dient, roept minder vragen op dan bij de toetsing aan het eerste vereiste. In dit geval is immers sprake van de bescherming van de nationale veiligheid en eventueel ook van de preventie van verdere strafbare feiten. Naar het oordeel van de onderzoekers is ook aan die eis voldaan.

---

[134] Gherbaoui, T. & Scheinin, M. (2022), A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it.

Conform het derde vereiste moet er echter een belangenafweging plaatsvinden, namelijk tussen het dienen van het legitieme doel, zoals bescherming van de nationale veiligheid of bescherming van het recht op leven, en het fundamentele recht dat door het nemen van een verwijderingsbesluit in het geding komt. In dit geval gaat het dus om de vrijheid van meningsuiting. Volgens de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) gaat die bescherming van het recht op vrijheid van meningsuiting verder. Dit heeft alles te maken met de rol die dit recht speelt in een democratische pluriforme samenleving.

Zo stelde het EHRM in de zaak *Handyside v. UK,* waarin het ging om de reikwijdte van het recht op vrijheid van meningsuiting, dat er juist in een tolerante, pluriforme democratie ook ruimte moet zijn voor ideeën en uitspraken die beledigen, choqueren of ontregelen.[135] Kortom, bij deze afweging van de noodzakelijkheid van de beperking door middel van een verwijderingsbesluit en de proportionaliteit van de impact van dat besluit ten opzichte van de inperking van de vrijheid van meningsuiting, moet grote zorgvuldigheid betracht worden. Bij de beoordeling van de proportionaliteit van de maatregelen speelt met name de vraag of verwijdering strikt noodzakelijk is of dat bijvoorbeeld ook met een minder ingrijpende maatregel hetzelfde effect bereikt kan worden. Er zou in dit geval immers ook overwogen kunnen worden om materiaal van een account tijdelijk onbereikbaar te maken. Het mandaat van de ATKM is echter gelimiteerd, want het bevel aan de HSPs betreft strikt genomen het ontoegankelijk maken van de inhoud. De HSPs neemt daarop op basis van een eigen afweging een besluit ten aanzien van verwijdering, of - minder ingrijpend - een zichtbaarheidsbeperking. Dat is een maatregel waarbij het algoritme ervoor zorgt dat het materiaal veel minder opduikt in de 'feed‘ of ‘timeline‘ van gebruikers van sociale mediaplatforms. De meest ingrijpende maatregel die een HSP kan nemen, betreft het verwijderen van een account. Dit laatste zou ook het gevolg kunnen zijn van een blootstellingsbesluit van de ATKM.

Deze evaluatie wijst erop dat er geen aanleiding is om zorgen te hebben over de zorgvuldigheid van het proces, zoals door de ATKM is uitgevoerd. De beoordeling van het bedrijfsproces wijst uit dat de ATKM - vooralsnog - handmatig te werk gaat bij het detecteren en beoordelen van content. Hierdoor blijft men de nuance in de gaten houden. Bovendien wordt pas geconcludeerd dat er sprake is van terroristische online inhoud als ófwel inhoud wordt aangetroffen die al eerder als zodanig is bestempeld, of dat dit geconstateerd wordt door meerdere beoordelaars in verschillende stappen. In de laatste fase van het constaterings- en beoordelingsproces vindt de belangenafweging plaats. In onze ogen wordt deze werkwijze derhalve zorgvuldig uitgevoerd en niet gehaast.

Vooruitlopend op de aanpassing in de bedrijfsvoering van de ATKM, waarbij deels zal worden overgegaan op geautomatiseerde detectie, is het belangrijk te benadrukken dat ook bij een geautomatiseerde detectie de zorgvuldige belangenafweging van het grootste belang blijft. Een geautomatiseerde schifting van online inhoud, waarbij onderscheid gemaakt wordt tussen inhoud die eerder zorgvuldig is beoordeeld maar die bij herhaling in de detectie voorkomt, en 'nieuwe’ online inhoud die nog voor de eerste keer beoordeeld moet worden, zou volgens ons echter geen probleem moeten opleveren ten aan zien van de zorgvuldige belangenafweging.

Een uiteindelijk eindoordeel over de vraag of er rechtmatig een beperking opgelegd is op de vrijheid van meningsuiting zal, indien dit besluit betwist wordt, altijd vastgesteld worden door

[135] European Court of Human Rights (1976), Handyside v United Kingdom, Appl No 5493/72, par. 49.

een onafhankelijke rechter. Daarvoor is de geschilbeslechtingsprocedure ingericht. Hoewel de Autoriteit Consument & Markt (ACM), de officiële toezichthouder op de uitvoering van de DSA, sinds februari 2025 een reeks aan klachten heeft ontvangen die ook betrekking hebben op account- en inhoudsbeperkingen, is niet vast te stellen of daar klachten tussen zitten die voortvloeien uit een verwijderbevel van de ATKM.[136]

Uit dit onderzoek blijkt in ieder geval dat er geen klachten over overblokkering zijn ontvangen door de ATKM zelf en dat er ook geen bezwaar- of beroepsprocedures zijn gestart. Het ontbreken van deze rechtelijke toetsing tot nu toe betekent overigens wel dat de grondrechtelijke houdbaarheid van de ATKM-besluiten nog niet onafhankelijk is vastgesteld. Echter, ook op basis van de interviews heeft dit onderzoek geen concrete aanwijzingen opgeleverd dat de verwijderbevel van de ATKM buiten de grondrechtelijke kaders zouden vallen.

3.2.2 Zijn er aanwijzingen voor chilling effects of andere onbedoelde neveneffecten op legitieme online inhoud?

Bij een *chilling effect* bestaat de kans dat individuen al bij voorbaat besluiten geen openbare online uitspraken te doen of materiaal te posten, uit angst dat dit als materiaal binnen de reikwijdte van de Uitvoeringswet TOI kan worden gezien. Ook HSPs kunnen, zonder dat daar een juridische aanleiding voor is, al bij voorbaat besluiten bepaald soort materiaal van hun platforms te weren of minder zichtbaar te maken. Er zou dan een vorm van (zelf-)censuur ontstaan. In dat laatste geval zou er sprake zijn van een ongewenste beperking van de vrijheid van meningsuiting.

Hoewel dit punt met name door mensenrechtenorganisaties, experts en het maatschappelijk middenveld als punt van zorg of aandacht wordt opgeworpen tijdens de interviews, kunnen diezelfde geïnterviewden geen concrete bewijzen aanleveren dat hier (in Nederland) sprake van zou zijn.[137] Er zijn voor deze evaluatie geen onderzoeken gevonden die empirisch bewijs leveren voor een *chilling effect* in de Nederlandse samenleving. Wel geeft een van de geïnterviewden aan dat er signalen zijn dat journalisten en academici voorzichtiger zijn geworden in het gebruik van schokkende beelden of een bepaald soort terroristisch materiaal.[138] Het valt te betwisten of dit als een ongewenst *chilling effect* kan worden aangemerkt, aangezien de argumentatie achter deze terughoudendheid zich vooral richt op het niet bijdragen aan het verspreiden van angst en dus aan het uitvoeren van de terroristische agenda. Belangrijke afweging in dezen is dan ook of de journalistieke taak of onafhankelijk onderzoek niet beperkt worden.

Een expert geeft aan dat het belangrijk blijft dat historische archieven met terroristisch materiaal openbaar toegankelijk blijven voor onderzoek.[139] Dezelfde expert geeft echter ook aan dat een beperking door versleuteling of beperkte toegang via een speciaal account begrijpelijk zou zijn. Dit zou te verantwoorden zijn op dezelfde manier dat journalisten, media en academici voorzichtig afwegen wanneer ze expliciet jihadistisch of *gore* materiaal tonen, aangezien dit immers kan bijdragen aan verspreiding van terroristisch of schadelijk materiaal.

---

136 ACM (2025), Veel gebruikers onbekend met hun rechten op online platforms, ACM start voorlichtingscampagne.
137 Interview met maatschappelijk middenveld, maart 2026; Interviews met academici, april 2026.
138 Interview met academici, april 2026.
139 Interview met academici, april 2026.

Bij gebrek aan empirisch onderzoek naar de percepties rond beperkingen van de vrijheid van meningsuiting in Nederland is het interessant om naar buurland Duitsland te kijken.
Een onderzoek uit 2025, uitgevoerd onder 1.490 inwoners in Duitsland, biedt enig inzicht in hoe ondervraagden aankijken tegen restricties op de vrijheid van meningsuiting. Uit het onderzoek blijkt dat bijna de helft van de ondervraagden van mening is dat er te veel restricties zijn op de vrijheid van meningsuiting.[140] Het onderzoek ging een stap verder door ook uit te zoeken waar die beperkingen in de visie van de ondervraagden vandaan kwamen. Er bleek een onderscheid te zijn tussen percepties in relatie tot juridische restricties en sociaal-normatieve restricties en er werd bovendien gekeken welke instanties geacht werden verantwoordelijk te zijn voor de restrictie. In dat laatste geval keek men zelfs of kennis van wie verantwoordelijk was voor de gepercipieerde restrictie invloed had op de mate waarin dit de percepties van de ondervraagden beïnvloedde. Hoewel zeker een deel van de ondervraagden van mening was dat juridische restricties te paternalistisch waren, meende evengoed een deel dat de juridische normen te weinig deden om bijvoorbeeld *hate speech* tegen te gaan.

Een belangrijke bevinding in dit onderzoek is dat de perceptie dat restricties op de vrijheid van meningsuiting die leiden tot politieke correctheid of die bijdragen aan een cancelcultuur vooral toegeschreven werden aan sociaal-normatieve restricties. Met name bepaalde groepen, zoals rechtse populistische bewegingen en extremistische groepen, wijzen graag een schuldige aan voor de gepercipieerde restrictie op de vrijheid van meningsuiting.[141]

Het bovenstaande onderzoek schetst in eerste instantie een beeld van de percepties over de beperkingen op de vrijheid van meningsuiting in Duitsland. Wat evenwel relevant is voor de Nederlandse context is dat volgens het Duitse onderzoek zelden een direct causaal verband te leggen is tussen enerzijds een perceptie van een beperking van de vrijheid van meningsuiting en anderzijds een juridische norm of een sociaal-normatieve restrictie. Met andere woorden, zelfs als er sprake zou zijn van een empirisch waarneembaar *chilling effect* als gevolg van de handhaving de Uitvoeringswet TOI, valt te betwijfelen of dit effect daadwerkelijk voortkomt uit gepercipieerde sociaal-normatieve restricties.

Behalve de moderatie op basis van de Uitvoeringswet TOI hebben gebruikers bovendien te maken met platformmoderatie op basis van hun gebruikersvoorwaarden, die overigens mede vorm hebben gekregen in relatie tot de vereisten die de DSA stelt. Naast restricties op basis van juridische normen, en in het bijzonder de Uitvoeringswet TOI, kunnen gebruikers dus ook te maken krijgen met opgelegde restricties op basis van andere juridische normen en sociaal-normatieve normen. Welke norm de HSP hanteert, is voor gebruikers niet altijd duidelijk. Het gebrek aan transparantie kan daarom wel degelijk leiden tot terughoudendheid bij het plaatsen van informatie, politieke correctheid of een gepercipieerde cancelcultuur.

Zeker wanneer de wet vage termen hanteert om het soort online inhoud af te bakenen dat als illegaal wordt bestempeld, neemt het risico op chilling effecten, of zelfs ‘censorship creep’ toe.[142] Er bestaan momenteel wel zorgen over de vage termen die worden gehanteerd in het wetsvoorstel voor strafbaarstelling van verheerlijking van terrorisme en openbare

---

140 Sacher, A.-L., & Reinemann, C. (2025), What is Freedom of Speech? How Citizens Define and Perceive the “Bulwark of Liberty”, p. 15.

141 Sacher, A.-L., & Reinemann, C. (2025), What is Freedom of Speech? How Citizens Define and Perceive the “Bulwark of Liberty”, p. 15

142 Keats Citron, D. (2018), Extremist Speech, Compelled Conformity, and Censorship Creep, p. 1054.

steunbetuigingen aan terroristische organisaties.[143] De Raad van State was ook kritisch over het gebrek aan duidelijke instructie voor de interpretatie van de factoren die bij de beoordeling een rol spelen, wat tot ontoelaatbare toepassing van de wet in concrete gevallen kan leiden.144 Met name het criterium van opzet van de dader behoeft, in de ogen van de Raad van State, nadere duiding. Andere kritiek richt zich op de weinig omkaderde termen van steunbetuigingen aan terroristische organisaties, waarbij niet per se helder is of dit om steun aan gewelddadige activiteiten gaat.[145] Dit kan op den duur tot ongewenste beperking van de vrijheid van meningsuiting leiden.

Het is duidelijk dat het van belang blijft om scherp te monitoren of er een *chilling effect* kan ontstaan. Echter, zoals hierboven aangegeven, zijn er voor deze evaluatie geen concrete aanwijzingen gevonden dat een eventueel *chilling effect* toe te schrijven is aan de Uitvoeringswet TOI.

Juridische aspecten van verwijderbevelen in andere lidstaten
De spanning tussen effectief optreden tegen terroristische online inhoud en de bescherming van de vrijheid van meningsuiting is in alle onderzochte lidstaten herkenbaar, maar wordt op verschillende manieren aangepakt.

In Duitsland heeft de netwerkhandhavingswet (NetzDG), al vóór de EU-verordening is ingevoerd, geleid tot discussie over overblokkering. Platforms kozen er soms voor content preventief te verwijderen om boetes te vermijden, ook wanneer de kwalificatie als illegale inhoud onzeker was. Juist dit risico heeft bijgedragen aan de keuze in de EU-verordening voor een aanpak waarbij de beslissing tot verwijdering bij de bevoegde autoriteit ligt en niet bij het platform.[146]

In Ierland speelt de bijzondere positie van grote platforms een rol in de juridische dynamiek. Coimisiún na Meán rapporteert dat Google regelmatig klachten indient over verwijderbevelen van andere lidstaten die gericht zijn aan in Ierland gevestigde diensten. Dit heeft ertoe geleid dat Ierland als een van de weinig lidstaten al enige ervaring heeft opgebouwd met het toetsen van grensoverschrijdende bevelen, zij het primair in de rol van ontvangende autoriteit.[147]

3.2.3 Is er juridische ruimte voor de ATKM om ook verwijderverzoeken in te dienen?

Verwijderverzoeken zijn een vrijwillig instrument dat EU-lidstaten en Europol reeds vóór de adoptie van de EU-verordening konden hanteren om HSPs te waarschuwen voor informatie die als terroristische inhoud kan worden beschouwd. De EU-verordening heeft geen specifiek mandaat opgenomen voor verwijderverzoeken, maar stelt in overweging 40 van de preambule dat “niets in deze verordening [mag] worden uitgelegd als een beletsel voor de lidstaten en

---

143 Rijksoverheid (2025), Wetsvoorstel om verheerlijken van terrorisme strafbaar te stellen naar Raad van State. Zie voor een kritische reflectie op het wetsvoorstel Van Noorloos, L. A. (2025), Strafbaarstelling van het verheerlijken van terrorisme en openbare steunbetuiging aan terroristische organisaties.

144 Raad van State, Advies over wetsvoorstel verheerlijken van terrorisme, 30 maart 2026, Strafbaarstelling verheerlijken van terrorisme en openbare steunbetuiging aan terroristische organisaties. | Raad van State

145 Van Noorloos, L. A. (2025), Strafbaarstelling van het verheerlijken van terrorisme en openbare steunbetuiging aan terroristische organisaties.

146 Europese Commissie (2024), Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online.

147 Interview met bevoegde autoriteit Ierland, mei 2026; Interview met ATKM, april 2026.

Europol om [verzoeken] te gebruiken als instrument om terroristische online inhoud tegen te gaan". In overweging 40 wordt tevens gesteld dat dergelijke verwijderverzoeken een doeltreffend en snel middel zijn gebleken om HSPs te wijzen op specifieke inhoud en om ze in staat te stellen daar actie op te nemen.

In rapporten van de Commissie aan het Europees Parlement en de Raad wordt gesteld dat door verschillende EU-lidstaten het instrument van verwijderverzoeken nog steeds gebruikt wordt ten aanzien van bepaalde HSPs, terwijl het instrument van verwijderbevelen enkel wordt gebruikt ten aanzien van HSPs die niet reageren op verzoeken of wanneer de urgentie groot is.[148] Europol stelt zelfs dat er in de afgelopen jaren meer dan 130.000 verwijderverzoeken zijn ingediend bij 200 verschillende HSPs, terwijl tegelijkertijd slechts 2.200 verwijderbevelen zijn verstuurd naar 35 HSPs.[149]

Noch in de Uitvoeringswet TOI, noch in de memorie van toelichting op de wet wordt specifiek gerefereerd aan de mogelijkheid om verwijderverzoeken in te dienen. In artikel 2 (3) (a) wordt echter wel als doelstelling van de ATKM gesteld dat die het ontoegankelijk maken van terroristische online inhoud bevordert. Op basis van die laatste zin zou de ATKM ook verwijderverzoeken kunnen uitsturen, mits deze gericht zijn op het tegengaan van de verspreiding van terroristische online inhoud. Tot op heden heeft de ATKM echter nog geen verwijderverzoeken ingediend.[150]

Op de vraag tijdens de interviews of het zinvol zou zijn als de ATKM ook verwijderverzoeken zou doen, bleken de meningen verdeeld. Voorstanders van verwijderverzoeken zien het als een nuttige eerste stap vóór formeel optreden, die de doorlooptijd verkort en HSPs de gelegenheid biedt zelf actie te ondernemen.[151] Tegenstanders benadrukken dat de ATKM als expertinstantie verantwoordelijkheid draagt voor de inhoudelijke beoordeling en dat het overdragen van deze afweging aan HSPs risico's op overblokkering met zich meebrengt. Bovendien is de vraag of een 'verzoek' vanuit een overheidsinstantie in de praktijk ook echt als vrijwillig wordt ervaren.[152] Deze aanname wordt niet onderschreven door HSPs die geïnterviewd zijn voor dit onderzoek. Zij benadrukken eerder dat ze een voordeel zien in het gebruik van verzoeken boven bevelen, omdat dat meer tijd geeft (dan één uur in geval van een bevel) om het verzoek zorgvuldig te behandelen.[153]

Verwijderverzoeken ten aanzien van borderline content

Bij de afweging of het huidige juridisch kader ruimte laat aan de ATKM om verzoeken tot verwijdering uit te sturen, speelt tevens de vraag of het opportuun is de ATKM ook een rol te laten spelen bij het doen van verzoeken over online inhoud die niet valt onder de Uitvoeringswet TOI. Deze vraag dient zich steeds nadrukkelijker aan gezien de grote zorgen over de rol van borderline content en desinformatie bij radicalisering en ondermijning van de democratische rechtsstaat.

---

148 Europese Commissie (2024), Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, p. 10.

149 Interview met opsporingsdienst, maart 2026.

150 Interviews met ATKM, mei 2026.

151 Interview met opsporingsdienst, maart 2026; Interviews met opsporingsdienst, april 2026.

152 Interview met maatschappelijk middenveld, maart 2026, Interview met ministerie van Economische Zaken en Klimaat, maart 2026; Interview met maatschappelijk middenveld, april 2026.

153 Interview met HSP, april 2026; Interview met HSP, juni 2026.

De Uitvoeringswet TOI en de EU-verordening staan niet in de weg voor het indienen van verwijderverzoeken, naast het gebruik van het instrument van verwijderbevelen. De Uitvoeringswet TOI koppelt iedere actie van de ATKM echter wel aan het tegengaan van de verspreiding van terroristische online inhoud. Het huidige mandaat van de ATKM biedt dan ook geen houvast voor het uitvaardigen van verwijderverzoeken ten aanzien van borderline content. Voor bepaalde vormen van borderline content, zoals *hate speech* en desinformatie, biedt de DSA overigens wel houvast aan HSPs om te modereren. Een uitzondering zou zich kunnen aandienen in het geval dat op het eerste oog borderline content na nadere bestudering toch valt onder de categorie terroristische online inhoud en daarmee binnen de reikwijdte van het mandaat van de ATKM valt.[154] Voor die uitzonderingscategorie online inhoud zou het derhalve juridisch mogelijk zijn om verwijderverzoeken uit te vaardigen. Overigens worden verwijderverzoeken door andere lidstaten wel gebruikt om de HSPs te wijzen op bijvoorbeeld online inhoud die als desinformatie of '*hate speech'* wordt geduid'.

Hieronder worden de argumenten opgesomd voor en tegen het gebruik door de ATKM van de mogelijkheid verwijderverzoeken uit te vaardigen, alsmede de argumenten voor en tegen uitbreiding van het juridisch mandaat:
Argumenten voor:

- De doorlooptijd voordat er tot een verwijderverzoek wordt besloten, zal korter zijn dan bij verwijderbevelen. Dit heeft te maken met het feit dat er voor een verzoek geen juridisch waterdichte argumentatie hoeft te worden opgesteld en opgeslagen om te beargumenteren dat er sprake is van terroristische online inhoud.[155]
- Hoewel er geen juridisch dwangmiddel aan een verwijderverzoek is gekoppeld, blijkt dat (enkele) grotere platforms vergelijkbaar scoren wat betreft de opvolging na een verzoek of bevel.
- De onafhankelijke rol van de ATKM als zbo stelt haar beter in staat een goede verstandhouding op te bouwen met de HSPs, wat het gebruik van verzoeken ten opzichte van bevelen ten goede zou komen, zoals ook blijkt uit de ervaringen van andere lidstaten.[156]
- Bij moderatie van online content die niet duidelijk is omschreven in de TOI-wetgeving bestaat eerder het gevaar dat inmenging door de overheid wordt gezien als een ongewenste inmenging in het publieke debat of zelfs in de vrijheid van meningsuiting. Door echter de ATKM, in plaats van de politie die een opsporingstaak heeft, een rol te geven bij het tegengaan van ongewenste en schadelijke borderline content, is het risico minder groot op een gepercipieerde ongewenste inmenging van de overheid in het publieke debat.

Argumenten tegen:

- Bij het uitsturen van een verwijderverzoek is er geen sprake van een juridisch dwangmiddel. Behalve bij enkele grotere HSPs is de opvolging na een verzoek tot verwijdering volgens Europol 60%, terwijl dat bij verwijderbevelen 90% is.

---

154 Van Ginkel, B., Mehra, T., Herbach, M. Lanchès, J. & Boerma, Y. (2025). Blurred Boundaries: Legal, Ethical and Practical limits in Detecting and Moderating Terrorist, Illegal, and Implicit Extremist Content Online While Respecting Freedom of Expression.

155 Hiermee wordt gedoeld op de administratieve last die samenhangt met het opstellen van een verwijderbevel.

156 Interview bevoegde autoriteit Duitsland, maart 2026; Interview bevoegde autoriteit Duitsland, april 2026; Interview bevoegde autoriteit Ierland, mei 2026.

- Voordat er tot een verwijderverzoek wordt besloten, zal een minder zorgvuldige afweging plaatsvinden van de noodzakelijkheid en de proportionaliteit van het verzoek tot verwijdering.
- Bij uitbreiding van het mandaat van de ATKM om ook te ageren op ongewenste en schadelijke borderline content ontstaat er een groter zorgpunt ten aanzien van de zorgvuldige afweging van de noodzakelijkheid en proportionaliteit van een verwijderverzoek.

3.2.4 Wordt de balans tussen effectiviteit en rechtsstatelijke bescherming voldoende geborgd?

Bij de beoordeling van deze vraag wordt effectiviteit begrepen als de output van de uitvoering van de wet: de mate waarin de ATKM er daadwerkelijk in slaagt terroristische online inhoud te identificeren, te kwalificeren en te doen verwijderen. Rechtsstatelijke bescherming omvat de waarborgen die ervoor zorgen dat deze uitvoering plaatsvindt binnen de grenzen van grondrechten, in het bijzonder de vrijheid van meningsuiting, en dat betrokkenen toegang hebben tot adequate rechtsbescherming.

Op basis van het onderzoek is het oordeel van de onderzoekers dat de ATKM deze balans in de huidige praktijk in voldoende mate borgt, zij het met een aantal kanttekeningen die aan belang winnen bij uitbreiding met geautomatiseerde detectiesystemen, de inwerkingtreding van de wet strafbaarheid verheerlijking terrorisme en de uitbreiding van het mandaat van de ATKM.

Interne waarborgen zijn stevig

De ATKM hanteert een meerlaagse beoordelingsprocedure waarin grondrechtelijke overwegingen een expliciete en structurele rol spelen. Elke casus doorloopt achtereenvolgens een inhoudelijke kwalificatie, een grondrechtelijke weging waarbij context, intentie, doelgroep en herkomst worden meegewogen, en een proportionaliteitsbeslissing. Daarbij is de interne norm bewust streng: de ATKM geeft aan dat de vrees om onterecht een legitieme uiting te verwijderen zwaarder weegt dan de vrees dat zorgwekkende content online blijft.[157] Dit duidt op een organisatiecultuur die gepaste terughoudendheid in de uitoefening van bevoegdheden als norm hanteert, wat bijdraagt aan de bescherming van de vrijheid van meningsuiting.

De ATKM is ingericht als zelfstandig bestuursorgaan zonder rechtspersoonlijkheid, onafhankelijk van politieke aansturing. Dit institutionele ontwerp is mede gekozen om de onafhankelijkheid van de oordeelsvorming te waarborgen en de schijn van politieke beïnvloeding te vermijden.[158] De combinatie van onafhankelijke status, handmatige beoordeling door gespecialiseerde medewerkers en dubbele interne toetsing biedt stevige procedurele garanties.

Externe validatie ontbreekt nog

Een lacune in de beoordeling van de rechtsstatelijke borging is het uitblijven van een onafhankelijk oordeel in een bezwaar- of beroepsprocedure. Tot op heden zijn er geen bezwaar- of beroepsprocedures gestart, wat betekent dat de inhoudelijke beoordelingscriteria van de ATKM nog nooit rechterlijk zijn gevalideerd.[159] Dit is op zichzelf geen bewijs van een

---

157 Interview met ATKM, april 2026; Interview met ATKM, mei 2026.
158 Kwartiermaker ATKM (2022), Organisatie- en Formatie rapport ATKM.
159 Interview met ATKM, april 2026; Interview met ministerie Economische Zaken en Klimaat, maart 2026.

probleem; de lage prikkel tot bezwaar- en beroep is mogelijk mede een teken dat de bevelen inhoudelijk niet worden betwist. Overigens zou - gezien een zekere selectiebias - bij dergelijke procedure een onafhankelijke rechter ook nooit een volledig oordeel kunnen vellen over de rechtsstatelijke borging van het afwegingsproces als geheel. Onze beoordeling van de rechtsstatelijke borging is daarom, bij afwezigheid van externe validatie, dat het aannemelijk is dat er interne zorgvuldigheid wordt betracht.

Naarmate de ATKM ook andere instrumenten inzet, zoals blootstellingsbesluiten, neemt de kans op procedures toe; en daarmee de kans op rechterlijke toetsing. Indien de ATKM zich in de toekomst eventueel meer op *borderline content* richt dan is aan te raden om deze beoordelingscriteria intern consistent te documenteren, zodat de ATKM goed is voorbereid op eventuele externe toetsing hierop.[160]

3.3 Capaciteit, uitvoerbaarheid en administratieve lasten

Bevindingen in het kort

- De ATKM telt 37 fte en heeft een jaarbudget van circa 8 miljoen euro; structurele capaciteitsknelpunten zijn breed erkend.
- Slechts twee detectiemedewerkers en drie beoordelaars zijn direct operationeel op detectie van terroristische online inhoud. Uitval van één medewerker raakt direct de continuïteit.
- Geautomatiseerde detectietooling is niet beschikbaar; een maatwerkoplossing is in ontwikkeling.
- De huisvesting is te krap en biedt onvoldoende ruimte voor herstel van medewerkers die dagelijks worden blootgesteld aan schokkend materiaal.
- Administratieve lasten rondom bevelen zijn hoog; de afhankelijkheid van de politie voor deconflictie en beperkte Europol-toegang begrenzen snelheid en informatiepositie.
- Voor HSPs zijn uitvoeringslasten relatief beperkt, maar kleinere platforms signaleren onduidelijkheid over de veelheid aan verplichtingen en het ontbreken van gestandaardiseerde processen.

3.3.1 Zijn de personele, juridische en technische middelen van de ATKM toereikend voor een effectieve uitvoering van haar taken en bevoegdheden?

De organisatiestructuur van de ATKM is vastgelegd in het Organisatie- en Formatieplan (OFP) dat in mei 2022 is opgesteld. Daarin was voorzien in een bezetting van 35 fte. Eind 2025 had de ATKM 37 fte in dienst, iets meer dan het plan voorzag, mede omdat de organisatie veel extra ICT-capaciteit heeft geworven voor de doorontwikkeling van haar informatievoorziening en systemen.[161]

Ongeveer de helft van het personeel zit op het primaire proces (~15 fte). Capaciteit binnen de afdeling primair proces van de ATKM onderverdeeld naar capaciteit voor TOI en capaciteit voor kinderpornografisch materiaal. Voor TOI zijn 1 lead (meewerkend voorman/-vrouw), 3 beoordelaars (inhoudelijk en juridisch), 2 detectiemedewerkers en 2x 0,5 fte senior beoordelaar (juridisch) beschikbaar. Voor kinderpornografisch materiaal bestaat de afdeling primair proces uit 1 lead (meewerkend voorman/-vrouw), 3 beoordelaars (inhoudelijk en

[160] Interview met maatschappelijk middenveld, maart 2026; Interview met academici, april 2026.
[161] Kwartiermaker ATKM (2022), Organisatie- en Formatie rapport ATKM; ATKM (2026), Jaarverslag 2025.

juridisch) en 2x 0,5 fte senior beoordelaar (juridisch). Daarnaast zijn 1 data-analist en 1 data-scientist werkzaam, zij bedienen zowel de TOI als kinderpornografisch materiaal vleugel van de ATKM.[162]

De overige fte bestaat uit ondersteunend en leidinggevend personeel (zoals bestuur, informatietechnologie, financiële afdeling, of human resources). Deze capaciteit wordt ten behoeve van de gehele organisatie ingezet. Dit heeft er mee te maken dat de organisatie in ontwikkeling is en dat voor beide onderwerpen min of meer in dezelfde mate flankerende inspanningen dienen te worden verricht. Het kan hier gaan om de uitwerking van beleids-regels, communicatieinspanningen, (inter)nationale netwerkopbouw, beleidsontwikkeling, maar ook bedrijfsvoeringsinpanningen en ICT-ontwikkeling.[163]
Voorzien wordt dat in de loop van 2027 aanvullende detectiemiddelen worden geïmplemen-teerd die specifiek zijn toegesneden op de behoeften en functionele eisen van de ATKM.[164]

Financieel beschikte de ATKM in 2024 over een budget van € 7,6 miljoen, waarvan € 5,4 miljoen is benut. In 2025 steeg het totaalbudget naar € 8 miljoen, waarvan € 7,5 miljoen is uitgegeven. Het budget is samengesteld uit drie structurele financieringsstromen: financie-ring onder de EU-verordening, middelen overgeboekt vanuit de Internet Referral Unit-pilot en financiering voor de aanpak van kinderpornografisch materiaal vanuit het directoraat-generaal Rechtspleging en Rechtshandhaving van het ministerie van Justitie en Veiligheid. Aanvullend ontvangt de ATKM tijdelijke middelen uit het Internal Security Fund (ISF).[165] Vanuit dit fonds heeft de AKTM ongeveer € 2,7 miljoen euro toegekend gekregen. Het overkoepelende doel hiervan was ‘Strengthening capabilities through increased cooperation between public authorities and all relevant actors’. Deze middelen zijn door de ATKM voornamelijk ingezet voor de ontwikkeling van ICT middelen die zowel bijdragen aan de bestrijding van online terroristische content als aan de bestrijding van kinderpornografisch materiaal. Daarnaast is ook geïnvesteerd in de samenwerking tussen de competent authorities binnen Europa op het vlak van classificatie.[166]

De bestedingspatronen in 2025 wijken op een aantal punten af van het jaarplan: de externe inhuur lag ruim 50% boven de begrote € 1,5 miljoen en aan ICT werd ruim € 0,8 miljoen uitgegeven, terwijl daar slechts € 250.000 voor was aangemerkt. Aan bedrijfsvoering werd daarentegen minder dan de helft van het begrote bedrag besteed. De ATKM schrijft de onderuitputting deels toe aan vertraging bij de aanschaf van detectiesoftware en het uitblijven van de mediacampagne voor het meldpunt.[167]

Van de 37 fte is het merendeel ondersteunend en leidinggevend personeel. Dit heeft enerzijds te maken met de recente oprichting van de zbo, en anderzijds met de noodzaak om voldoende IT-support te geven aan het primaire proces. De recente oprichting van de organisatie heeft ervoor gezorgd dat extra aandacht moest worden besteed aan het vormgeven van de organisatie, processen en beleid. Daarnaast heeft de ATKM specifieke IT en veiligheids-behoeftes vanwege het soort werk dat het verricht. Er zijn geen signalen van over- of ondercapaciteit op ondersteunend en leidinggevend personeel. Wel wordt er

---

162 Schriftelijke toelichting ATKM, juli 2026.
163 Schriftelijke toelichting ATKM, juli 2026.
164 Schriftelijke toelichting ATKM, juli 2026.
165 ATKM (2026), Jaarverslag 2025; Interview met ATKM, mei 2026.
166 Schriftelijke toelichting ATKM, juli 2026.
167 ATKM (2026), Jaarverslag 2025.

aangegeven dat, met de ontwikkeling van de organisatie, de balans zou kunnen worden verschoven ten voordele van capaciteit op het primaire proces. Bovendien kan het zijn dat op termijn een verschil zichtbaar wordt tussen benodigde capaciteit voor kinderpornografisch materiaal en de benodigde capaciteit voor TOI, ook wat betreft de flankerende inzet. Vooralsnog is daar geen sprake van.[168]

Met slechts vijf direct operationele medewerkers in het TOI-primaire proces is die bezetting zo krap dat het wegvallen van één medewerker direct de continuïteit raakt. De ATKM zelf stelt dat uitbreiding van de menselijke capaciteit niet de primaire oplossing is: zodra geautomatiseerde *tooling* beschikbaar is, kunnen bestaande medewerkers een veelvoud van de huidige output genereren.[169]

De technische infrastructuur vormt een structurele kwetsbaarheid. De detectiesystemen die door het kwartiermakersteam waren geselecteerd, bleken niet geschikt voor het primaire proces van de ATKM. Ze konden slechts bestanden van beperkte omvang verwerken en waren niet toegesneden op de bestuursrechtelijke vereisten van de autoriteit. Alternatieve systemen op de markt zijn doorgaans ontworpen voor opsporingsinstanties en sluiten niet aan bij de bevoegdheden van de ATKM. Een aanbestedingsprocedure voor vervangende OSINT-software heeft geen geschikte oplossing opgeleverd; momenteel wordt een maatwerkoplossing *in house* ontwikkeld, mede gefinancierd via ISF-middelen.[170] Tot die tijd werkt de ATKM handmatig en besteedt zij een deel van de detectie uit aan externe OSINT-bureaus. Dit laatste heeft ook financiële implicaties omdat aanbesteding doorgaans hogere kosten met zich meebrengt.

De juridische capaciteit was in de opstartfase ernstig ondermaats: aanvankelijk was slechts één persoon verantwoordelijk voor alle juridische taken van de organisatie. Dit leidde tot vertragingen en kwetsbaarheid. De situatie is verbeterd maar blijft beperkt ten opzichte van het takenpakket, met name wanneer het bredere instrumentarium (blootstellingsbesluiten en geschilbeslechting) in de toekomst volledig zou worden benut.[171]

Een aanverwant knelpunt is de huisvesting. Het kantoor van de ATKM biedt volgens de organisatie onvoldoende ruimte voor de huidige bezetting. Vanwege de werkzaamheden bestaat weinig flexibiliteit; medewerkers die zich bezighouden met de detectie en beoordeling van terroristisch en kinderpornografisch materiaal kunnen dit werk vanwege de aard van het materiaal niet thuis verrichten. Dit betekent dat zij altijd op kantoor aanwezig moeten zijn en dat andere medewerkers de werkruimte van het primaire proces niet kunnen benutten. De rijksbrede norm voor het aantal werkplekken per vierkante meter volstaat daardoor niet voor de specifieke situatie van de ATKM. Bovendien beschikt het huidige pand niet over adequate ruimte voor ontspanning en herstel, wat juist voor medewerkers die dagelijks worden blootgesteld aan zwaar beeldmateriaal een wezenlijk onderdeel is van een verantwoord arbeidsomstandighedenbeleid. De ATKM heeft in 2025 een visie op huisvesting opgesteld met een programma van eisen en verkent in overleg met het ministerie van Justitie en Veiligheid en het Rijksvastgoedbedrijf de mogelijkheden voor alternatieve huisvesting.[172]

---

168 Schriftelijke toelichting ATKM, juli 2026.
169 Interview met ATKM, mei 2026.
170 ATKM (2025), Jaarverslag 2024; Interview met ATKM, april 2026; Interview met ATKM, mei 2026.
171 Interview met ATKM, april 2026; Interview met ATKM, mei 2026.
172 ATKM (2026), Jaarverslag 2025.

3.3.2 *In hoeverre ervaren de ATKM of ketenpartners knelpunten met betrekking tot capaciteit, uitvoerbaarheid of administratieve lasten (of anderszins) bij de Uitvoeringswet TOI?*

De voornaamste knelpunten die uit de interviews naar voren komen, kunnen worden verdeeld in vier categorieën.

De eerste categorie betreft de handmatige detectie en het ontbreken van geautomatiseerde *tooling*. Omdat de ATKM nog uitsluitend handmatig detecteert, is groei van geïdentificeerde content direct begrensd door de beschikbare menselijke capaciteit. Dit knelpunt wordt versterkt door de lange doorlooptijd van aanbestedingsprocedures voor maatwerksoftware.[173]

De tweede categorie betreft de administratieve lasten rondom het opstellen en verzenden van verwijderbevelen. Een bevel is een juridisch document dat aan bestuursrechtelijke standaarden moet voldoen: het vergt motivering, aftekening, invoer in PERCI en, voor platforms die niet op PERCI zijn aangesloten, aanvullende verzending via eigen kanalen van het platform. Dit administratieve traject kost aanzienlijk meer tijd dan de wettelijke één-uursregel doet vermoeden. De ATKM werkt aan de stroomlijning van dit proces, onder andere via CSV-exports die automatisch in PERCI kunnen worden ingevoerd.[174]

De derde categorie betreft de informatiedeling met de politie en de afhankelijkheid van het deconflictieproces. Zoals beschreven in paragraaf 3.2 kan de ATKM het deconflictieproces niet zelfstandig uitvoeren en is zij hiervoor afhankelijk van de politie. Hoewel de samenwerking goed verloopt en de politie doorgaans snel reageert, vormt de 48-uursperiode een structurele vertraging in het proces.[175] Specifieke Europol-informatie, zoals hashlists en het Check the Web-systeem, bereikt de ATKM bovendien niet automatisch en tijdig, wat de informatiepositie van de organisatie beperkt.[176]

De vierde categorie betreft de zogenoemde *lawful but awful*-problematiek: een aanzienlijk deel van de content die de ATKM signaleert, valt buiten het TOI-kader, maar is wel zorgwekkend. Omdat de ATKM geen verwijderverzoek gebruikt en beperkt blijft tot aantoonbare TOI, wordt een deel van de problematische content niet aangepakt.

3.3.3 *Wordt de uitvoerbaarheid van de verplichtingen als werkbaar ervaren door hostingdiensten en internetplatformen?*

Het directe perspectief van individuele HSPs op de uitvoerbaarheid van de Uitvoeringswet TOI is in dit onderzoek beperkt vertegenwoordigd. Er zijn weinig signalen ontvangen over structurele uitvoerbaarheidsproblemen bij platforms.[177]

Voor kleinere HSPs geldt dat zij minder juridische capaciteit hebben om bevelen snel te verwerken, maar tegelijkertijd doorgaans minder TOI-content hebben. De één-uursregel wordt voor kleinere partijen als potentieel uitdagend beschouwd, al zijn er geen concrete klachten over geregistreerd.[178] Grotere platforms beschikken over geautomatiseerde systemen voor het

---

173 Interview met ATKM, mei 2026; ATKM (2025), Jaarverslag 2024.

174 CSV is bestandstype dat geëxporteerd (en geïmporteerd) kan worden vanuit programma's zoals Excel. Interview met ATKM, mei 2026.

175 Interview met opsporingsdienst, april 2026; Interview met ATKM, mei 2026.

176 Interview met opsporingsdienst, april 2026; Interview met opsporingsdienst, maart 2026.

177 Interview met ministerie van Economische Zaken en Klimaat, maart 2026; Interview met maatschappelijk middenveld, april 2026.

178 Interview met maatschappelijk middenveld, april 2026.

verwerken van bevelen en ervaren de termijn als werkbaar. Open-source tools zoals AbuseIO kunnen kleinere HSPs ondersteunen bij het verwerken van bevelen, maar het is onduidelijk in hoeverre Nederlandse HSPs hier in de praktijk gebruik van maken.[179]

Een punt van aandacht vanuit de sector is de onduidelijkheid over de betekenis van een verwijderverzoek wanneer een toezichthoudende autoriteit tegelijkertijd bevoegd is om bindende bevelen uit te vaardigen. HSPs geven aan behoefte te hebben aan gestandaardiseerde communicatie die het onderscheid tussen beide instrumenten verduidelijkt en aan meer transparantie over welke autoriteit in welke lidstaat welke bevoegdheden heeft.[180]

Tot slot blijkt uit de bevindingen dat met name kleinere HSPs moeite hebben om te voldoen aan verschillende verplichtingen en initiatieven die op nationaal en EU-niveau bestaan.[181] De veelheid aan initiatieven en het ontbreken van gestroomlijnde processen maken het voor deze partijen lastig om effectief te opereren, mede vanwege beperkte capaciteit en middelen. In dit kader wordt ook gewezen op het belang van verdere standaardisatie van technologische oplossingen, zodat met name kleinere platforms beter in staat worden gesteld om aan de vereisten te voldoen.

Capaciteit en uitvoerbaarheid in andere lidstaten

De capaciteitsuitdagingen waarmee de ATKM kampt, zijn niet uniek. In Duitsland zijn het BKA en het BNetzA samen verantwoordelijk voor de uitvoering van de EU-verordening, met in totaal zeventien medewerkers verspreid over beide organisaties. De meeste hiervan vervullen ook andere taken. Capaciteitstekorten bij het BKA zorgen ervoor dat verzoeken van het BNetzA niet altijd tijdig worden verwerkt, wat de interne samenwerking bemoeilijkt.[182] In Ierland beschikt Coimisiún na Meán over een bredere toezichtstaak en meer operationele capaciteit, maar ook daar wordt de combinatie van taken onder de EU-verordening, de DSA en nationale regelgeving als intensief ervaren. Het Ierse model (waarbij één autoriteit verantwoordelijk is voor een groot aantal in Ierland gevestigde grote platforms) levert een hoog volume aan grensoverschrijdende bevelen op, wat niet proportioneel is aan de beschikbare capaciteit.[183]

Een opvallend verschil is dat het merendeel van de lidstaten de implementatietaken heeft ondergebracht bij bestaande organisaties, waardoor opstartproblemen rond ICT-systemen en personeelsopbouw minder prominent speelden dan bij de ATKM. Het nadeel van die keuze is echter dat de TOI-taak daardoor vaak een bijrol speelt binnen een grotere organisatie, wat ten koste kan gaan van de focus en expertise. De ATKM heeft, als volledig nieuwe en zelfstandige autoriteit, meer investeringstijd nodig gehad, maar beschikt nu over geconcentreerde expertise wat andere lidstaten als een voordeel beschouwen.[184]

---

179 Ibid.
180 Interview met maatschappelijke middenveld, april 2026; Interview met HSP, april 2026.
181 Interview met HSP, april 2026.
182 Interview met bevoegde autoriteit Duitsland, maart 2026.
183 Interview met bevoegde autoriteit Ierland, mei 2026.
184 Interview met ATKM, april 2026; Interview met opsporingsdienst, maart 2026.

3.4 Governance en samenwerking

Bevindingen in het kort

- De ATKM wordt internationaal gezien als een proactieve en constructieve partner die relatief succesvol is in samenwerking met de private sector. Internationaal vervult de ATKM een voortrekkersrol, onder meer als covoorzitter van de EU-werkgroep voor een gemeenschappelijke TOI-taxonomie.
- De constructie van ATKM als zbo levert aantoonbare voordelen op, waaronder onafhankelijkheid, legitimiteit en meer ruimte (ten opzichte van opsporingsdiensten) om een vertrouwensrelatie met Hosting Service Providers op te bouwen.
- Structurele nadelen van de keuze voor ATKM als zbo zijn het ontbreken van directe toegang tot Europol-systemen zoals SIENA en de afhankelijkheid van de politie als intermediair voor deconflictie en informatiedeling. Dit drukt op de efficiëntie van de organisatie.
- Samenwerking tussen ATKM en politie is goed maar beperkt en wordt steeds verder ingebed (onder andere reguliere overleggen en delen van informatie). Momenteel wordt onderzocht of en hoe aanvullende relevante informatie gedeeld kan worden, conform de Wet politiegegevens. De waardevolle kennis die de ATKM opbouwt, bereikt de politie en de NCTV op dit moment nog onvoldoende.
- De combinatie van taken op het gebied van de bestrijding van terroristische online inhoud en kinderpornografisch materiaal biedt synergievoordelen.

3.4.1 Hoe werkt de keuze voor de ATKM als zelfstandig bestuursorgaan door in een effectieve en efficiënte uitvoering van de TOI? In hoeverre zou de ATKM haar wettelijke taken en bevoegdheden (met name ten aanzien van internationale politiesamenwerking en toegang tot informatie) anders kunnen uitvoeren als ze een opsporingsinstantie zou zijn?

Om de doorwerking van de keuze voor de ATKM als zelfstandig bestuursorgaan te kunnen overzien, is het van belang om de overwegingen voor deze keuze voor het voetlicht te brengen. Vervolgens kunnen de voor- en nadelen van deze keuze, alsook hun effect op de effectiviteit en efficiëntie van de uitvoering van de Uitvoeringswet TOI, worden uiteengezet.

Beweegredenen en overwegingen voor de keuze voor de ATKM als zbo

De keuze om de ATKM als zbo in te richten, is gebaseerd op juridische, bestuurlijke en inhoudelijke overwegingen, welke zijn toegelicht in de memorie van toelichting.[185] In de eerste plaats is gekozen voor een bestuursrechtelijke in plaats van strafrechtelijke uitvoering van de taken die voortvloeien uit de EU-verordening. De kern van de Uitvoeringswet TOI ligt bij het verwijderen van terroristische online inhoud en niet bij het opsporen en vervolgen van daders. Bovendien heeft de Uitvoeringswet TOI geen punitief karakter. In dit kader werd de bestuursrechtelijke aanpak passender geacht dan een strafrechtelijke insteek.[186] [187]

Met deze keuze wordt bovendien een duidelijke scheiding tussen toezicht en opsporing nagestreefd. De ATKM richt zich op het beëindigen van de beschikbaarheid van content, terwijl opsporing en vervolging zijn belegd bij politie en Openbaar Ministerie. Deze functiescheiding sluit aan bij bestaande institutionele verhoudingen binnen het Nederlandse

[185] Tweede Kamer (2022), Memorie van toelichting: Uitvoeringswet verordening terroristische online-inhoud. 36 138, nr. 3.
[186] Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM.
[187] Interview met ATKM, februari 2026; Interviews met ministerie van Justitie en Veiligheid, februari en maart 2026.

veiligheidsdomein en voorkomt de vermenging van bestuursrechtelijke en strafrechtelijke rollen.[188]

Op basis van de keuze voor de bestuursrechtelijke benadering is gekeken naar een mogelijke organisatorische inbedding van de uitvoering van de Uitvoeringswet TOI. Een centrale overweging hierbij was het belang van onafhankelijke oordeelsvorming. De besluiten van de ATKM, met name het uitvaardigen van verwijderbevelen, raken fundamentele rechten zoals de vrijheid van meningsuiting. Daarom werd het noodzakelijk geacht de besluitvorming op afstand van politieke aansturing te positioneren, zodat deze plaatsvindt zonder (de schijn van) politieke beïnvloeding.[189] [190]

Hieraan gerelateerd speelde ook de wens om de ATKM duidelijk te positioneren als een neutrale toezichthouder op het snijvlak van overheid en private sector.[191] De gedachte was (en is) dat een neutrale autoriteit zoals de ATKM beter in staat zou zijn om een werkrelatie op te bouwen met HSPs en de private sector dan, bijvoorbeeld, de nationale politie.[192]

Daarnaast speelden praktijkervaringen een rol bij de totstandkoming van de organisatorische constructie. Zo wordt verwezen naar eerdere ervaringen met de Internet Referral Unit (IRU) bij de politie, die volgens betrokkenen minder goed aansloot bij de rol en werkwijze van een opsporingsdienst.[193] De politie opereert primair binnen het strafrechtelijke domein, met bijbehorende bevoegdheden, procedures en prioriteiten, en ze richt zich op opsporing. Het monitoren van het internet (en het in dat verband versturen van verwijderverzoeken) paste niet goed in de taakomschrijving van de politie.[194] Bovendien vormde beperkte capaciteit binnen de politie een belemmerende factor om de unit effectief in te zetten.[195]

Daarnaast wordt benadrukt dat een zbo beter ruimte biedt voor proactief OSINT-onderzoek zonder dat sprake hoeft te zijn van een concrete verdenking, terwijl opsporingsdiensten hier juridisch gezien sterker in worden beperkt. Een aanvullende overweging betreft de inrichting van de informatiepositie. In de gekozen constructie is expliciet rekening gehouden met de wens om informatie te kunnen verwerken en delen buiten het kader van de Wet politiegegevens (Wpg). Door de ATKM buiten dit kader te positioneren, wordt ruimte gecreëerd voor een bredere informatiepositie, met name op het gebied van open bronnenonderzoek en samenwerking met private partijen.[196]

In de overwegingen rondom het beleggen van de verantwoordelijkheden die voortvloeien uit de Uitvoeringswet TOI zijn verschillende opties overwogen, waaronder ook onderbrenging bij bestaande organisaties zoals de politie, de ACM of het kerndepartement van Justitie en Veiligheid.[197] Geen van deze opties werd echter passend geacht, vanwege de specifieke combinatie van taken die vraagt om snelle besluitvorming, specialistische beoordeling en

---

188 Interview met opsporingsdienst, maart 2026.
189 Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM; Tweede Kamer (2022), Memorie van toelichting: Uitvoeringswet verordening terroristische online-inhoud. 36 138, nr. 3.
190 Interview met ATKM, februari 2026; Interview met ministerie van Justitie en Veiligheid, maart 2026.
191 Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM.
192 Interview met ATKM, februari 2026; Interview met ministerie van Justitie en Veiligheid, maart 2026.
193 Interview met opsporingsdienst, maart 2026.
194 Ibid.
195 Ibid.
196 Interviews met opsporingsdienst, maart en april 2026.
197 Interview met ministerie van Justitie en Veiligheid, maart 2026.

intensieve samenwerking met private partijen.[198] Daarmee bleef de optie over om een nieuwe organisatievorm in te richten, die specifiek toegesneden is op deze taak.

Bovendien is de keuze voor de ATKM als zbo beïnvloed door ontwikkelingen op het gebied van het tegengaan van online illegale content in den brede. De ATKM als zbo kan de TOI-taak combineren met de aanpak van kinderpornografisch materiaal (zie ook paragraaf 3.4.5).[199]

Nederland is de enige lidstaat die als bevoegde autoriteit een organisatie zonder opsporingsbevoegdheden heeft aangewezen. In alle andere lidstaten is (in ieder geval) een deel van de taken belegd bij een opsporingsorganisatie. Nu, midden 2026, met enkele jaren uitvoeringservaring achter de rug, kan de balans worden opgemaakt ten aanzien van de voor- en nadelen van deze keuze, alsook de praktische implicaties.

Voordelen van de keuze voor een zbo

De keuze voor een zbo-constructie brengt verschillende voordelen met zich mee voor zowel de effectiviteit als de efficiëntie van de uitvoering van de Uitvoeringswet TOI. Allereerst draagt de zbo-status bij aan onafhankelijkheid en legitimiteit van besluitvorming. Deze onafhankelijkheid wordt in den brede gezien als essentieel voor het zorgvuldig omgaan met grondrechten en voor het creëren van vertrouwen bij stakeholders, waaronder burgers en HSPs.[200]

Daarnaast faciliteert de zbo-positie de opbouw van een vertrouwensrelatie met HSPs. In interviews wordt benadrukt dat de ATKM hierdoor kan opereren als een relatief neutrale en deskundige autoriteit, wat de bereidheid van HSPs tot samenwerking kan vergroten. Deze relatie is van belang, omdat effectieve uitvoering in belangrijke mate afhankelijk is van de medewerking van private partijen. Opsporingsinstanties hebben mogelijk meer moeite met het opbouwen van een dergelijke vertrouwensrelatie en hebben hier doorgaans minder tijd en middelen voor beschikbaar. Een vertegenwoordiger vanuit een opsporingsinstantie benadrukt bijvoorbeeld dat de ATKM, in vergelijking met de bevoegde autoriteiten in andere lidstaten, relatief succesvol is in het opbouwen van een relatie en samenwerking met HSPs.[201]

Een derde voordeel is de mogelijkheid om gespecialiseerde kennis en expertise op te bouwen. Omdat de ATKM zich vrijwel exclusief (naast kinderpornografisch materiaal) richt op de beoordeling en handhaving van online illegale terroristische content, kan zij expertise ontwikkelen op het gebied van de interpretatie van terroristisch materiaal, platformdynamieken en juridische afwegingen. Dit draagt bij aan de kennis en kunde van de autoriteit om materiaal op te sporen en te interpreteren. Specialistische expertise en een diepgaand begrip van hoe materiaal online wordt geuit en gedeeld, zijn essentieel om het effectief op te sporen.[202]

Het volgende tekstvak illustreert waarom gespecialiseerde kennis en expertise van belang zijn om terroristisch materiaal als zodanig te kunnen herkennen.

---

198 Kwartiermaker ATKM (2022), Organisatie & Formatierapport ATKM.
199 Interview met ministerie van Justitie en Veiligheid, maart 2026.
200 Onder andere interview met ministerie van Justitie en Veiligheid, maart 2026; Interviews met ATKM, februari – mei 2026.
201 Interview met opsporingsdienst, maart 2026.
202 Interview met academici, april 2026.

Extremistische en terroristische *dog whistles*
Extremistische en terroristische actoren maken in hun communicatie op het internet steeds vaker gebruik van *dog whistles* en gecodeerde taal en symbolen. Om nieuwe gebruikers te radicaliseren, produceren groepen en individuen propaganda die grotendeels aansluit bij mainstream trends of *memes*, waarbij extremere ideeën met humor worden genormaliseerd.[203]

Rechtsextremistische groeperingen staan erom bekend dat ze uitgebreid gebruikmaken van onder andere numerieke codes (zoals 14 dat verwijst naar een populaire *White supremacist* slogan), handgebaren (zoals 88 dat symbool staat voor de achtste letter van het alfabet, de H, en daarmee Heil Hitler) en *emoijs* om minderheden aan te wijzen en dehumaniseren.[204] Jihadistische groepen introduceren vaak een tweede betekenis voor religieuze of historische uitdrukkingen en produceren veel videogamegerelateerde *memes* en video's die de esthetiek van *first person shooter games* kopiëren.[205] Deze gecodeerde communicatie wordt gebruikt om gelijkgestemden te vinden op openbare platforms, extremistische ideeën onbewust te normaliseren en contentmoderatie te beperken.

De politie ziet de ATKM bovendien als partnerorganisatie die op een andere wijze kan opereren dan de politie kan en mag. De politie richt zich voornamelijk op het vervolgen van strafbare feiten onder gezag van het OM. De ATKM richt zich op het identificeren en verwijderen van terroristische online inhoud en richt zich juist niet op de personen die materiaal plaatsen. De politie en de ATKM zijn complementair aan elkaar.

Tot slot wordt gewezen op de mogelijkheid om synergie te realiseren tussen verschillende taakdomeinen, met name tussen terroristische online inhoud en kinderpornografisch materiaal. De bundeling van taken binnen één organisatie maakt het mogelijk om patronen te herkennen en kennis te delen. Dit stelt de ATKM in staat om bepaalde trends en patronen vroegtijdig op te sporen (zie ook paragraaf 3.4.5).

Nadelen van de keuze voor een zbo

Tegenover deze voordelen staan verschillende nadelen. Het meest fundamentele nadeel is de beperkte toegang tot informatie en internationale systemen. Omdat de ATKM geen opsporingsinstantie is, heeft zij geen directe toegang tot Europol-informatie-uitwisselings-systemen zoals SIENA. Dit systeem wordt door opsporingsinstanties onderling gebruikt voor informatie-uitwisseling. In de praktijk betekent het ontbreken van SIENA-toegang dat de ATKM niet rechtstreeks kan communiceren met buitenlandse opsporingsdiensten of Europol-netwerken, maar hiervoor afhankelijk is van de Nederlandse politie als intermediair.[206] Dit zorgt concreet voor vertraging in het deconflictieproces (zie hieronder), alsook voor een beperktere informatiepositie.

---

203 NCTV (2024), Fenomeenanalyse 'Memes als online wapen'.

204 Anti-Defamation League (2019), Hate on display: hate symbols database; Gentile, F. & O'Keefe, I. G. (2025), Use of Coded Language by Far-Right Extremists Online: Emojis, Numbers, and Symbols Reinforce In-Group Identity.

205 Mehra, T. & van Ginkel, B. (2025), Boundaries to Borderline Content: Defining the scope of Implicit Extremist Content; Dauber, C. E., Robinson, M. D., Baslious, J. J. & Blair, A. G. (2019), Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos.

206 Interview met opsporingsdienst, maart 2026; Interview met opsporingsdienst, maart 2026; Interviews met ATKM, februari – mei 2026.

De ATKM zou in principe toegang kunnen krijgen tot SIENA, mits de Nederlandse politie en Europol daar toestemming voor geven.[207] De Nederlandse politie is terughoudend met het verstrekken van deze toegang aan de ATKM, temeer omdat in de keuze voor de bestuurlijke inrichting van de autoriteit expliciet is gekozen voor het scheiden van de toezichthouderstaak van de opsporingstaak.[208] Door de ATKM toegang te geven tot systemen als SIENA zou het risico bestaan dat de ATKM toegang krijgt tot opsporingsinformatie waar zij geen recht op heeft en zouden de toezicht- en opsporingstaken door elkaar gaan lopen, terwijl hier met de keuze voor de ATKM als zbo juíst voor gewaakt is.[209] De ATKM heeft daarnaast ook geen directe toegang tot Europol-tools, waaronder 'Check the Web' en hashlists.

In de beginfase van de ATKM bestonden er knelpunten rondom de toegang van de ATKM tot systemen en informatie.[210] Hierover zijn gedurende de looptijd van de ATKM steeds concretere afspraken gemaakt. Echter, Europol-informatie zoals 'Check the Web' en hashlists worden tot op heden niet automatisch doorgezet door de politie naar de ATKM en het is onbekend in hoeverre dit soort informatie de ATKM (tijdig) bereikt.[211]

Het gevolg van de beperkte of omslachtige toegang van de ATKM tot informatie en trendanalyses van Europol is dat de ATKM over minder contextuele en netwerkgerichte informatie beschikt dan de opsporingsdiensten. In hoeverre dit de effectiviteit van de beoordeling van materiaal en het uitsturen van verwijderbevelen beïnvloedt, is moeilijk vast te stellen. Belangrijk om te benadrukken, is dat de ATKM wél toegang heeft tot PERCI (zie ook paragraaf 3.3.2).

Daarnaast ontstaat er een structurele afhankelijkheid van de ATKM van de politie voor deconflictie en informatiedeling. Hierover zijn aan de start van de totstandkoming van de ATKM afspraken gemaakt. Concreet houdt dit in dat de ATKM links van geïdentificeerd materiaal deelt met de politie en dat de politie vervolgens de check uitvoert. De politie gaat na (binnen 48 uur) of het desbetreffende materiaal deel uitmaakt van een lopend opsporings-onderzoek. Indien dit het geval is, krijgt de ATKM (en de eenheid waarbinnen het opsporings-onderzoek loopt) hierover melding en wordt zij verzocht geen verwijderbevel uit te sturen. Indien het materiaal geen deel uitmaakt van een lopend opsporingsonderzoek, dan krijgt de ATKM groen licht om het proces tot het opstellen van het verwijderbevel voort te zetten.

In de praktijk deelt de ATKM ongeveer eens per week een mail met de politie met geïdentificeerde links. Dit kan variëren van enkele links tot 30 links. De politie geeft aan dat zij doorgaans binnen één uur reageert op het deconflictieverzoek.[212] Het kost de politie ongeveer één minuut om een link te deconflicteren.[213]

In de startfase van de ATKM bleek de deconflictie door de politie niet volledig uitgevoerd te worden en niet alle relevante systemen te worden bevraagd. De ATKM deelt het verzoek tot deconflictie sindsdien met twee verschillende onderdelen van de politie.[214] Daarnaast zijn

---

207 Interview met opsporingsdienst, maart 2026; Interview met opsporingsdienst, maart 2026.
208 Interview met opsporingsdienst, maart 2026.
209 Ibid.
210 Interview met ministerie van Justitie en Veiligheid, februari 2026; Interview met opsporingsdienst, maart 2026; Interviews met ATKM, februari – mei 2026.
211 Interview met opsporingsdienst, april 2026.
212 Ibid.
213 Ibid.
214 Interview met ATKM, mei 2026.

sinds de startperiode van de ATKM ook wijzigingen doorgevoerd in de timing van het deconflictieproces. Initieel voerde de ATKM de volledige beoordeling van potentieel terroristische online inhoud uit en werd dan het deconflictieverzoek met de politie gedeeld, waarna de politie nog 48 uur de tijd had om de deconflictie uit te voeren. Na verloop van tijd is dit proces anders ingericht, zodat er niet onnodig tijd wordt verloren zodra vaststaat dat het materiaal TOI betreft. De ATKM identificeert nu materiaal, doorloopt de beoordelingsprocedure, stuurt vervolgens een deconflictieverzoek uit naar de politie en geeft ondertussen (administratieve) opvolging (door het al dan niet klaarzetten en versturen van een verwijderverzoek).[215] Door de processen parallel aan elkaar in te richten en het verwijderverzoek al 'klaar te zetten' terwijl de deconflictie plaatsvindt, wordt getracht de efficiëntie van het deconflictieproces te vergroten. De ATKM geeft bovendien aan dat zij niet altijd reactie ontvangt op haar verzoek tot deconflictie; als men na 48 uur geen reactie heeft ontvangen van de politie, beschouwt de ATKM dit als voldoende grond om het verwijderbevel uit te sturen.[216]

Opvallend is dat deconflictie tussen de ATKM en nationale politie tot op heden nog nooit tot een 'hit' heeft geleid. De politie vindt dit opvallend, maar benoemt dat online een enorme hoeveelheid materiaal beschikbaar is en dat het daarom niet vreemd is dat de opsporings-onderzoeken en het materiaal dat de ATKM identificeert elkaar niet kruisen.[217]

In hoeverre de deconflictie op nationaal niveau volledig en effectief plaatsvindt, is moeilijk te beoordelen. Hoewel de politie dus geen formele rol speelt bij de uitvoering van de Uitvoeringswet TOI, vormt de politie wél een extra schakel in het proces. De samenwerking tussen de politie en de ATKM wordt als goed ervaren en wordt steeds verbeterd (zie ook paragraaf 3.4.2), maar deze afhankelijkheid zorgt wel voor vertraging in het proces. Dit raakt de efficiëntie van de uitvoering van de Uitvoeringswet TOI.

Deconflictie vindt bovendien niet alleen op nationaal, maar ook op EU-niveau plaats. Voor geïdentificeerd materiaal dient ook bij opsporingsinstanties in andere lidstaten nagegaan te worden of het materiaal aldaar deel uitmaakt van lopend opsporingsonderzoek. Wanneer materiaal onderdeel is van een lopend opsporingsonderzoek, kan het als zodanig worden aangemerkt in het Europol-systeem PERCI (zogenaamd *whitelisten)*. Wanneer een andere autoriteit materiaal invoert in PERCI om een verwijderbevel (of verzoek) uit te sturen, wordt men gealarmeerd via de *whitelist*. Er wordt echter slechts in beperkte mate gebruikgemaakt van de mogelijkheid om materiaal te w*hitelisten.* Een van de redenen die genoemd wordt voor het beperkte gebruik van de *whitelist* is dat dit nóg een extra (administratieve) stap is die tijd vereist in een omgeving waar tijd en capaciteit schaars zijn. Het beperkte gebruik van de *whitelist*, in combinatie met het gegeven dat de ATKM geen toegang heeft tot SIENA, zorgt ervoor dat materiaal dat door de ATKM wordt geïdentificeerd en waarop een verwijderbevel wordt gestuurd, niet (altijd) op EU-niveau wordt gedeconflicteerd. Concreet betekent dit dat de ATKM verwijderbevelen zou kunnen versturen op materiaal dat onderdeel is van lopende opsporingsonderzoeken in andere lidstaten. Het is onduidelijk in hoeverre dit is voorgekomen.

Het volgende tekstvak illustreert hoe de bevoegde toezichthoudende autoriteit in drie andere lidstaten is ingericht en welke voor- en nadelen verbonden zijn aan deze constructies.

---

215 Interview met ATKM, mei 2026.
216 Interview met ATKM, februari 2026.
217 Interview met opsporingsdienst, april 2026.

Governance en samenwerking in andere lidstaten
De governance-keuzes van lidstaten bij de implementatie van de EU-verordening lopen sterk uiteen en weerspiegelen nationale constitutionele tradities, bestaande institutionele capaciteit en politieke prioriteiten.

Duitsland heeft de taken gesplitst over twee bestaande autoriteiten: het BKA als bevoegde autoriteit voor het uitvaardigen en toetsen van verwijderbevelen, en het BNetzA als toezichthoudende autoriteit verantwoordelijk voor het opleggen van specifieke maatregelen en sancties aan HSPs. Deze keuze was grondwettelijk ingegeven: een opsporingsorganisatie als het BKA mag naar Duits constitutioneel recht geen bestuursrechtelijke sancties opleggen. De splitsing levert capaciteitsknelpunten op, met name vertraagde verwerking van verzoeken van het BNetzA door het BKA, maar ook synergievoordelen: het BNetzA benut haar bestaande vertrouwensrelaties met HSPs vanuit de DSA-toezicht rol en beide organisaties zijn in hetzelfde gebouw gehuisvest, wat informeel overleg faciliteert.[218]

In Ierland zijn de verantwoordelijkheden onder de Europese verordening verdeeld over twee bestaande autoriteiten. *An Guarda Síochána*, de nationale politie- en veiligheidsdienst, is aangewezen als bevoegde autoriteit voor operationele taken zoals het uitvaardigen van verwijderbevelen en de toetsing daarvan, terwijl *Coimisiún na Meán*, de onafhankelijke media- en onlineveiligheidstoezichthouder, verantwoordelijk is voor de toezichthoudende taken en het opleggen van sancties. Coimisiún na Meán vervult al een centrale rol bij de uitvoering van de DSA en deze taak sluit hierbij aan. De constructie maakt het mogelijk om de terrorisme-expertise en operationele bevoegdheden van de politie te combineren met de bestaande ervaring en relaties van Coimisiún na Meán met online platforms. Tot op heden heeft Ierland met name ingezet op het beoordelen en monitoren van bevelen die door andere lidstaten uitgestuurd worden naar HSPs die in Ierland gevestigd zijn (onder andere Snapchat, Meta, Google). Zelf heeft Ierland slechts één verwijderbevel uitgegeven in 2025.[219]

Zweden heeft ervoor gekozen om alle taken onder de Europese verordening onder te brengen bij één bestaande autoriteit: de nationale politie (Polismyndigheten, polisen). De polisen is zowel verantwoordelijk voor het uitvaardigen en toetsen van verwijderbevelen als voor de toezichthoudende taken, waaronder het opleggen van bestuursrechtelijke sancties. Bij de keuze voor deze governance-structuur werd expliciet afgewogen of deze taken bij de politie of de veiligheidsdienst (Säkerhetspolisen, SÄPO) moesten worden belegd. Uiteindelijk viel de keuze op de politie vanwege haar bestaande 24/7-operationele capaciteit, internationale samenwerkingsstructuren via Europol en ervaring met bestuursrechtelijke taken. Tegelijkertijd speelt SÄPO een belangrijke ondersteunende rol dankzij haar expertise op het gebied van terrorisme, radicalisering en dreigingsanalyse. Om deze samenwerking te faciliteren, bevat de Zweedse implementatiewet een expliciete informatie-uitwisselingsverplichting tussen beide organisaties. De gekozen structuur combineert daarmee operationele slagkracht met specialistische terrorisme-expertise, terwijl de exclusieve beslissingsbevoegdheid van de politie tevens moet waarborgen dat wordt voldaan aan de onafhankelijkheidsvereisten van de verordening.[220]

---

218 Interview met bevoegde autoriteit Duitsland, maart 2026; Interview met bevoegde autoriteit Duitsland, april 2026.
219 Interview met bevoegde autoriteit Ierland, mei 2026.
220 Interview met bevoegde autoriteit Zweden, mei 2026.

3.4.2 Hoe functioneert de samenwerking tussen de ATKM en nationale actoren (zoals politie, Openbaar Ministerie, toezichthouders)?

De ATKM werkt in de praktijk samen met verschillende ketenpartners, partijen in het maatschappelijk middenveld en HSPs. De ervaringen hiermee worden in volgende alinea's nader uiteengezet.[221]

Nationaal Coördinator Terrorismebestrijding en Veiligheid

De NCTV fungeert, naast de Directie Rechtshandhaving en Criminaliteitsbestrijding (DRC) bij het directoraat-generaal Rechtsbescherming en Rechtshandhaving van het ministerie van Justitie en Veiligheid, als opdrachtgever van de ATKM.[222] In deze rol is de NCTV verantwoordelijk voor het vaststellen van beleidskaders en prioriteiten waarbinnen de ATKM haar taken uitvoert.[223] Deze formele relatie vertaalt zich in de praktijk naar een frequente en gestructureerde samenwerking, waarbij regelmatig overleg plaatsvindt over trends, beleidsontwikkelingen op Nederlands en EU-niveau en de uitvoering van de TOI-taak.

Gesprekspartners beschrijven het gedeelde opdrachtgeverschap van de NCTV en DRC niet als problematisch. Wel wordt benoemd dat de opdrachtgevers elk hun eigen beleidsprioriteiten en verwachtingen hebben. Wanneer beide domeinen gelijktijdig een hoge prioriteit krijgen van de respectievelijke opdrachtgever dan kan dit leiden tot frictie in de aansturing en de noodzaak tot keuzes.[224]

De samenwerking tussen de NCTV en de ATKM wordt door de geïnterviewden als goed en constructief gekarakteriseerd.[225] De organisaties zijn inhoudelijk complementair aan elkaar: de NCTV richt zich op coördinatie en dreigingsbeeldvorming, terwijl de ATKM deze inzichten kan benutten bij haar operationele toezichtstaak. Daarmee draagt de samenwerking met de NCTV met name bij aan de strategische en contextuele onderbouwing van het optreden van de ATKM.

Nationale politie

Er zijn drie belangrijke raakvlakken tussen de ATKM en de politie bij de uitvoering van de TOI-taak. Dit betreft (1) strategische afstemming om te zorgen dat de bestuurlijke hoofdlijnen goed op elkaar aansluiten, zodat beide organisaties elkaar versterken, (2) deconflictie op operationeel niveau (zie hierboven) en (3) informatie-uitwisseling vanuit de politie richting de ATKM over trends en ontwikkelingen (zie hieronder).[226] Hoewel de politie geen formele rol heeft in de uitvoering van de Uitvoeringswet TOI, is de organisatie in de praktijk een cruciale schakel.

De samenwerking tussen de politie en de ATKM is gedurende de looptijd van de ATKM uitgebouwd. In de startperiode was de samenwerking grotendeels beperkt en ad hoc, recent is deze geïntensiveerd, onder meer via managementoverleg en werkgroepen.[227] Op operationeel niveau is regelmatig contact tussen de politie en de ATKM, onder andere op het

---

221 Gezien beperkte samenwerking worden partijen als de AIVD, MIVD en Autoriteit Persoonsgegevens buiten beschouwing gelaten.
222 Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM.
223 Ibid.
224 Interview met ministerie van Justitie en Veiligheid, februari 2026.
225 Interview met ministerie van Justitie en Veiligheid, februari 2026; Interviews met ATKM, februari – april 2026.
226 Interview met opsporingsdienst, april 2026.
227 Interview met opsporingsdienst, maart 2026; Interviews met ATKM, februari – mei 2026.

gebied van de deconflictie De samenwerking en 'het vinden van elkaar' gebeurt, volgens zowel de politie als de ATKM, steeds makkelijker en natuurlijker.[228]

In het voorjaar van 2026 is bovendien gestart met intensievere informatiedeling van de politie aan de ATKM. Specifiek gaat het hierbij om Artikel 8 informatie uit de Wpg (informatie uit de dagelijkse politiewerkzaamheden). Dit betreft informatie die bijvoorbeeld door politieagenten op straat wordt verwerkt en die een basis kan vormen voor een strafrechtelijk onderzoek. Deze gegevens kunnen sinds het voorjaar van 2026 onder voorwaarden met de ATKM worden gedeeld. In maart 2026 heeft de politie voor het eerst een dataset met profielen, websites en accounts met de ATKM gedeeld. De ATKM had deze informatie nog niet in beeld.[229]

Daarnaast wordt ten tijde van het schrijven van deze rapportage onderzocht in hoeverre Artikel 9 informatie (informatie die wordt verwerkt in lopende opsporingsonderzoeken), ten aanzien van bijvoorbeeld verdachten, gedeeld kan worden met de ATKM. Het beheer van deze gegevens ligt bij het OM. Indien geen sprake is van een conflict met lopende onderzoeken, dan zou deze informatie ook relevant kunnen zijn voor de ATKM om haar taak effectiever uit te kunnen voeren.[230]

Ten slotte zouden Artikel 10 gegevens (zonder concrete verdachte of strafbaar feit) mogelijk relevant zijn voor de ATKM. Deze gegevens zijn zeer privacygevoelig en het gebruik en delen ervan zijn streng gereguleerd.[231] De politie heeft de wens om Artikel 9 en 10 gegevens ook structureel te kunnen delen met de ATKM. Deze wens ligt bij het OM en het ministerie van Justitie en Veiligheid ter overweging. De frequentie waarmee deze informatie wordt gedeeld, zal uiteindelijk gebaseerd worden op de actualiteit en de hoeveelheid geïdentificeerde informatie. Een frequentie tussen eens per maand en eens per halfjaar lijkt op dit moment realistisch.[232]

Andersom is de politie ook geïnteresseerd in het nagaan welke informatie de ATKM met de politie kan en mag delen. Momenteel is de informatie die vanuit de ATKM naar de politie stroomt nog beperkt. Voorbeelden van inzichten die de politie zou kunnen verkrijgen vanuit de ATKM zijn onder andere: het gebruik van kinderpornografisch materiaal binnen de radicalisering van jongeren in het jihadistische spoor en de opkomst van nieuwe fenomenen, zoals nihilistisch extremisme.[233]

Hoewel de samenwerking tussen de ATKM en de politie naar hun zeggen over het algemeen soepel en steeds beter verloopt, vormt de beperkte toegang van de ATKM tot de Europol-systemen een structureel knelpunt. Als gevolg van deze beperking is goede samenwerking tussen de ATKM en de politie essentieel en dienen hiertoe continu afspraken te worden gemaakt (en aangescherpt).

Ten slotte is het van belang te vermelden dat de politie ook zelf kan optreden indien zij terroristische online inhoud signaleert. Zij kan in principe zelf een verwijderverzoek versturen

---

228 Interviews met opsporingsdienst, maart en april 2026.
229 Interview met opsporingsdienst, april 2026.
230 Ibid.
231 Ibid.
232 Ibid.
233 Ibid.

(dit gebeurt in de praktijk bijna niet), een opsporingsonderzoek instellen, contact opnemen met de Internet Referral Unit bij Europol en/of materiaal offline (laten) halen. Indien relevant, deelt de politie ook gesignaleerd materiaal met de ATKM.[234]

Openbaar Ministerie

Het Openbaar Ministerie is verantwoordelijk voor de strafrechtelijke handhaving en vervolging. Samenwerking met het OM is tot op heden beperkt. Het Openbaar Ministerie heeft geen directe rol in de Uitvoeringswet TOI. Het OM speelt daarentegen een indirecte rol, met name wat betreft het beheer van strafrechtelijke gegevens en de toestemming voor informatie-uitwisseling. De samenwerking tussen ATKM en OM is daarmee voornamelijk indirect en verloopt via de politie en de juridische kaders voor gegevensdeling.

Autoriteit Consument & Markt

De ACM is in Nederland aangewezen als toezichthouder op onderdelen van de DSA, waarbij zij onder meer toezicht houdt op de naleving van verplichtingen voor online platforms en digitale diensten. Binnen dit bredere stelsel vervult de ATKM een specifieke rol als bevoegde autoriteit voor de EU-verordening, terwijl de ACM een bredere toezichthoudende taak heeft ten aanzien van online platformen en hun verplichtingen.

In de praktijk is de samenwerking tussen de ATKM en de ACM op het gebied van terroristische online inhoud beperkt. Er is contact, maar er is geen sprake van structurele operationele afstemming. Aangezien de organisaties zich op verschillende aspecten van platformregulering richten en er geen geluiden zijn opgehaald over knelpunten in de samenwerking, wordt nauwere samenwerking op dit moment niet nodig geacht, aldus de ATKM.[235]

Maatschappelijk middenveld

Binnen de Uitvoeringswet TOI vervult het maatschappelijk middenveld geen formele uitvoeringsrol, maar speelt het wel een rol in de bredere uitvoering en de effectiviteit van de wetgeving. Organisaties in het maatschappelijk middenveld zoals Stichting Offlimits dragen bij aan kennis over en de signalering en duiding van online content en daarmee indirect aan de uitvoering van de TOI-taak.[236] Zo heeft Stichting Offlimits bijvoorbeeld zelf een meldpunt waar schadelijke content gemeld kan worden.[237] De organisatie meldt deze inhoud vervolgens bij HSP.[238] Wanneer seksueel kindermisbruikmateriaal of TOI niet offline wordt gehaald, zet Offlimits het materiaal door naar de ATKM voor beoordeling en, indien gerechtvaardigd, een verwijderbevel. In het kader van de Uitvoeringswet TOI is samenwerking tussen de ATKM en het maatschappelijk middenveld niet op structurele wijze ingericht, maar vindt het plaats op ad hoc-basis.

Hosting service providers

De samenwerking met HSPs vormt een kernonderdeel van de uitvoering van de Uitvoeringswet TOI. HSPs vervullen een centrale rol, omdat zij de controle hebben over de opslag en beschikbaarheid van online content. De effectiviteit van de ATKM bij het

---

234 Interview met opsporingsdienst, maart 2026.
235 Interview met ATKM, mei 2026.
236 Interview met maatschappelijk middenveld, april 2026.
237 Stichting Offlimits een *DSA trusted flagger*
238 Offlimits (g.d.), Meldpunt.

verwijderen van terroristische online-inhoud is daarmee in belangrijke mate afhankelijk van de medewerking van HSPs.

De ATKM is verantwoordelijk voor het toezien op de naleving van verplichtingen uit de EU-verordening door HSPs die in Nederland zijn gevestigd. Dit betekent dat de ATKM bevoegd is om verwijderbevelen uit te vaardigen richting deze partijen (alsook richting HSPs gevestigd in andere lidstaten en buiten Europa) en, voor de HSPs die in Nederland gevestigd zijn, toezicht te houden op het naleven van deze bevelen. Ook heeft de ATKM het blootstellingsbesluit tot haar beschikking (zie paragraaf 3.1.6). Tegelijkertijd is de relatie tussen de ATKM en HSPs niet uitsluitend handhavend van aard en stelt de ATKM zich ook op als samenwerkingspartner om samen met de HSPs na te gaan hoe terroristische online inhoud effectiever kan worden verwijderd.

De ATKM heeft een Sectorraad opgericht om structurele samenwerking met HSPs te bevorderen en de autoriteit heeft separaat contact met grotere sociale media platforms die gevestigd zijn in Nederland, zoals Discord, Reddit en Snapchat.[239] De Sectorraad heeft in 2024 met name stilgestaan bij de operationalisering door de ATKM van terroristisch online materiaal en de inwerkingtreding van de Wet bestuursrechtelijke aanpak online kinderpornografisch materiaal en de effecten hiervan voor de sector. In 2025 is de Sectorraad naast reguliere vergaderingen ook als werkgroep samengekomen om specifiek de voor- en nadelen van een DNS-blokkade[240] (onderdeel van het ATKM-instrumentarium) te bespreken.[241]

Wat betreft naleving van de Uitvoeringswet TOI geven HSPs doorgaans tijdig opvolging aan verwijderbevelen van de ATKM.[242][243] In zowel 2024 als 2025 werden alle verwijderbevelen van de ATKM opgevolgd. In 2024 werd, met uitzondering van twee verwijderbevelen naar een kleine HSP zonder vertegenwoordiging in de EU, binnen één uur gehoor gegeven aan alle bevelen. In 2025 werd in 93% van de gevallen het materiaal tijdig verwijderd of ontoegankelijk gemaakt.[244] De meeste bevelen werden verstuurd naar HSPs buiten Nederland.

De ATKM is er bovendien in geslaagd om een vertrouwens- en samenwerkingsband op te bouwen met HSPs gevestigd in Nederland; iets waar bevoegde autoriteiten in andere lidstaten meer moeite mee hebben. Zo benadrukken zowel Europol als HSPs dat de ATKM onder andere opvalt door haar proactieve samenwerking met de HSPs.[245]

Tegelijkertijd kent de samenwerking met HSPs ook uitdagingen. De ATKM is primair verantwoordelijk voor HSPs in Nederland, terwijl een groot deel van de relevante platforms internationaal opereert. Dit betekent dat de ATKM in de praktijk vaak afhankelijk is van grensoverschrijdende samenwerking en bereidheid van buitenlandse HSPs om mee te werken. Een deel van de HSPs die terroristische online inhoud hosten, bevindt zich buiten de EU. De samenwerking met HSPs die geen juridische basis in de EU hebben, verloopt

---

239 ATKM (2025), Jaarverslag 2024.
240 Een DNS-blokkade betekent dat wordt verhinderd dat een bepaalde website via de normale domeinnaam kan worden bereikt.
241 ATKM (2026), Jaarverslag 2025.
242 ATKM (2025), Jaarverslag 2024; ATKM (2026), Jaarverslag 2025.
243 Interview met HSP, april 2026; Interview met HSP, juni 2025; Interview met maatschappelijk middenveld, april 2026
244 ATKM (2025), Jaarverslag 2024; ATKM (2026), Jaarverslag 2025.
245 Interview met opsporingsdienst, maart 2026; Interview met HSP, april 2026; Interview met HSP, juni 2026.

bijzonder stroef, onder andere vanwege een gebrek aan (beschikbare) contactpersonen bij deze HSPs.[246]

Tijdens interviews geven HSPs bovendien aan dat ze het liefst eerst een verwijderverzoek zouden ontvangen, omdat dit een minder tijdgevoelige en juridisch minder complexe oplossing is die minder capaciteit vergt (zie ook paragraaf 3.2).[247] De ATKM zet op dit moment alleen in op het versturen van bindende verwijderbevelen (zie voor nadere toelichting op mogelijkheden tot uitsturen verwijderverzoeken ook paragraaf 3.2).

Daarnaast heeft de ATKM geen zicht op het materiaal dat HSPs op eigen initiatief verwijderen. HSPs geven aan gebruik te maken van verschillende AI- en menselijke contentmoderatie, die het overgrote deel van mogelijk problematisch of illegale content detecteert voordat het op de platforms wordt geplaatst.[248] Ook Europol geeft aan dat HSPs een substantieel deel van de content zelfstandig verwijderen, zelfs voordat formele verwijderbevelen worden verstuurd.[249]

HSPs maken hierover namelijk geen melding. Dit belemmert de ATKM in haar samenwerking met de HSPs, omdat onduidelijk is in hoeverre de partijen al actief en effectief modereren.[250] HSPs zijn onder zowel de TOI als de DSA verplicht om elk jaar een transparantierapport te publiceren. De TOI-transparantierapporten zijn bedoeld om inzicht te geven in het moderatiemechanisme dat HSPs zelf hebben opgezet en hoe de EU-verordening heeft bijgedragen aan het beperken van terroristisch materiaal. Hierin moet ten eerste worden aangegeven welke mechanismen de platforms beschikbaar stellen om melding te doen van terroristische en andere illegale content. Ten tweede moet hier het aantal items met terroristische inhoud worden gerapporteerd dat is verwijderd of waartoe de toegang is geblokkeerd naar aanleiding van verwijderbevelen of specifieke maatregelen.

De meeste transparantierapporten die door grote HSPs worden gepubliceerd, voldoen technisch gezien aan de minimale vereisten, maar hebben beperkte meerwaarde om nieuwe ontwikkelingen op het gebied van de verspreiding of moderatie van terroristische online inhoud te identificeren. Zo wordt bijvoorbeeld niet beschreven hoe contentmoderatie precies plaatsvindt en welke specifieke maatregelen (eventueel) zijn genomen om te voorkomen dat terroristische online inhoud wordt geplaatst.

3.4.3 Hoe functioneert de samenwerking met buitenlandse bevoegde autoriteiten onder de EU-verordening?

De samenwerking met buitenlandse bevoegde autoriteiten is primair vormgegeven binnen het kader van de EU-verordening (EU) 2021/784, die lidstaten verplicht om één of meerdere bevoegde autoriteiten aan te wijzen en samenwerking tussen deze autoriteiten te faciliteren, onder meer door het uitwisselen van verwijderbevelen en door samenwerking met Europol. De ATKM vervult in Nederland deze rol en werkt in dat kader samen met buitenlandse autoriteiten en Europol. De Europese Commissie organiseert daarnaast twee keer per jaar

---

246 Interviews met ATKM, februari – april 2026.
247 Interview met HSP, april 2026; Interview met HSP, juni 2025. Hierbij dient opgemerkt te worden dat het hierbij gaat om grotere HSPs.
248 Ibid.
249 Interview met opsporingsdienst, maart 2026.
250 Interviews met ATKM, februari – april 2026.

een workshop waarin de bevoegde autoriteiten van lidstaten samenwerken om de effectieve implementatie en uitvoering van de EU-verordening te bevorderen. Uit interviews komt naar voren dat de samenwerking tussen de ATKM en buitenlandse bevoegde autoriteiten positief verloopt. De ATKM wordt internationaal erkend als een competente en proactieve partner en is actief binnen EU-werkgroepen en samenwerkingsstructuren.[251]

In 2024 heeft de ATKM opgetreden als covoorzitter van een werkgroep van de Europese Commissie. De ATKM heeft toen het initiatief gelanceerd om samen met de andere bevoegde autoriteiten te werken aan een aangescherpte taxonomie voor terroristische online inhoud, om het identificeren en beoordelen van terroristisch materiaal binnen de EU te harmoniseren.[252] De ATKM heeft in 2025 drie thematische werkgroepsessies georganiseerd, waarin gezamenlijk voorbeelden van rechtsextremistische en jihadistische content zijn besproken en beoordeeld. Op basis hiervan wordt een richtlijn geschreven ter ondersteuning van autoriteiten bij het classificeren van terroristische online inhoud en het eenduidig beoordelen van terroristisch materiaal.[253] Daarnaast heeft de ATKM samen met de Europese Commissie een workshop georganiseerd in Rotterdam, waaraan alle bevoegde autoriteiten uit de EU-lidstaten deelnamen. Naar aanleiding van de workshop zijn er drie werkgroepen gevormd: (1) de werkgroep HSPs wettelijke vertegenwoordiging in de EU, (2) de werkgroep specifieke maatregelen en (3) de werkgroep technische maatregelen. De eerste werkgroep wordt door de ATKM geleid in samenwerking met de Zweedse Internet Referral Unit en zal in 2026 een *position paper* opstellen met een advies voor EU-lidstaten en de Europese Commissie.[254]

In de praktijk houdt de samenwerking tussen de ATKM en buitenlandse autoriteiten met name in dat onderlinge deconflictie plaatsvindt via het Europol-systeem PERCI en dat men onderling de opvolging van bevelen monitort. Ten aanzien van deconflictie op EU-niveau identificeren geïnterviewden een aantal uitdagingen. Deze hangen deels samen met de keuze om de ATKM als bestuursrechtelijke autoriteit te positioneren en niet als opsporingsdienst, waardoor zij geen directe toegang heeft tot bepaalde informatie en netwerken. In 2025 heeft de ATKM toegang gekregen tot een deel van de informatie (*databases/hashes*) van Europol op het gebied van de aanpak van terrorisme. In de EU-verordening was deze toegang voorzien, Aangezien de ATKM geen politieorganisatie is, moest dit voor de ATKM als organisatie op bestuursrechtelijke grondslag echter apart worden geregeld.[255]

Naast deconflictie op nationaal niveau dient namelijk ook op EU-niveau deconflictie plaats te vinden (zie ook paragraaf 3.4.1). Vanwege het beperkte gebruik van deze functie door opsporingsdiensten kan het voorkomen dat een autoriteit een verwijderbevel uitstuurt op materiaal dat onderdeel is van een lopend opsporingsonderzoek in een andere lidstaat.[256] Deze situatie kan óók voorkomen bij bevoegde autoriteiten die wél opsporingsbevoegdheden hebben en is dus niet uniek voor de ATKM. Opsporingsdiensten kunnen onderling echter ook informatie uitwisselen via SIENA. Hiertoe geeft de ATKM geen toegang. Het deconflicteren van materiaal op EU-niveau vormt daarom een belemmering voor de ATKM en de organisatie heeft slechts in zeer beperkte mate controle over in hoeverre deconflictie daadwerkelijk plaatsvindt.

---

251 Interview met opsporingsdienst, maart 2026.
252 ATKM (2025), Jaarverslag 2024.
253 ATKM (2026), Jaarverslag 2025.
254 Ibid.
255 Ibid.
256 Ibid.

Ten aanzien van het monitoren van de opvolging van verwijderbevelen zijn door de ATKM en andere gesprekspartners geen uitdagingen geformuleerd. Ter illustratie, als de bevoegde autoriteit van lidstaat A een verwijderbevel uitstuurt naar een HSP gevestigd in lidstaat B, dan is de bevoegde autoriteit van lidstaat B vervolgens verantwoordelijk voor het monitoren van de daadwerkelijke verwijdering van het materiaal (binnen de gestelde tijdslimieten). Het PERCI-systeem van Europol biedt bevoegde autoriteiten ondersteuning om de voortgang van grensoverschrijdende bevelen te monitoren.

3.4.4 Worden internationale verplichtingen en samenwerkingsstructuren effectief benut?

Binnen het kader van de EU-verordening maakt de ATKM gebruik van verschillende internationale structuren, waaronder het Europol-systeem PERCI ten behoeve van het opstellen en uitvaardigen van verwijderbevelen en werkgroepen van de Europese Commissie (zie hierboven). Uit interviews blijkt dat de ATKM een actieve en proactieve deelnemer is aan deze structuren en dit overleg. Dit blijkt ook uit de voortrekkersrol in de werkgroep van de Europese Commissie ten aanzien van het komen tot gemeenschappelijke standaarden (het lexicon). Gesprekspartners geven bovendien aan dat de ATKM, de enige bevoegde autoriteit zonder opsporingsbevoegdheden, zeker als ‘vol’ wordt aangezien in het Europese speelveld; te meer vanwege haar houding en specifieke expertise.[257]

De effectieve benutting van deze structuren wordt in de praktijk beperkt door de toegang die de ATKM niet heeft tot bepaalde informatie en tools (als gevolg van haar gebrek aan opsporingsbevoegdheden; zie ook hierboven). Deze beperkte toegang is met name zichtbaar in het gegeven dat de ATKM geen directe toegang heeft tot alle Europol-producten (zoals hashlijsten en ‘Check the Web’-informatie) en tot het informatie-uitwisselingssysteem SIENA. Voor toegang tot deze elementen is de ATKM afhankelijk van de Nederlandse politie (zie hierboven).

3.4.5 Welke invloed heeft het samenvoegen van de terroristische online inhoud-taak met de kinderpornografisch materiaal -taak binnen de ATKM op de uitvoering van de TOI-taak door de ATKM?

De combinatie van de terroristische online inhoud-taak en de kinderpornografisch materiaal-taak binnen één organisatie is vastgelegd in de nationale inrichting van de ATKM. In de keuze voor de ATKM als zbo is bewust gekozen voor het integreren van beide taken binnen één organisatie en zelfs binnen één cluster van primaire processen, om synergie te realiseren in kennis, capaciteit en processen.[258] De onderliggende gedachte hierbij is dat beide taken inhoudelijk verwant zijn (online contentregulering), vergelijkbare processen kennen (detectie, beoordeling, verwijdering) en kunnen profiteren van een gedeelde infrastructuur, expertise en samenwerking met de internetsector (HSPs).

De ATKM geeft zelf aan dat de keuze voor één organisatie heeft bijgedragen aan het opbouwen van specifieke expertise en een sterke positionering in het (internationale) netwerk.[259] Ook benoemt de ATKM dat de integratie van de twee taken het mogelijk maakt om expertise en werkwijzen over domeinen heen te ontwikkelen en toe te passen, bijvoorbeeld in

---

[257] Interview met opsporingsdienst, maart 2026; Interview met maatschappelijk middenveld, april 2026.
[258] Kwartiermaker ATKM (2022), Organisatie & Formatie rapport ATKM.
[259] Interview met ATKM, april 2026.

de beoordeling van online content en de omgang met HSPs. Juist omdat de ATKM beide thema's monitort, is zij in staat om dwarsverbanden en overeenkomsten te identificeren. Een voorbeeld is de link tussen kinderpornografisch materiaal en terroristische online inhoud.

Overlap kinderpornografisch materiaal en terroristische online inhoud
Terroristische online inhoud en kinderpornografisch materiaal worden steeds vaker samen gedetecteerd binnen onlinegemeenschappen die extreem gewelddadig materiaal ('*gore content*') gebruiken om kwetsbare jongeren te isoleren met vervolgens als doel *grooming* en chantage (*sextortion*). De ATKM heeft een onderzoek laten uitvoeren naar deze overlap, dat kinderpornografisch materiaal vormen van seksueel en extreem geweld doelgericht worden ingezet voor extremistische en terroristische radicalisering.[260]

Met schokkend materiaal wordt de ontvanger ongevoelig gemaakt voor extreem geweld en wordt hij/zij aangezet om kinderpornografisch materiaal of gelijkwaardig gewelddadig materiaal te verspreiden. Verschillende groeperingen binnen het 'Com'-netwerk[261] (is een nihilistisch gewelddadig extremistisch netwerk) verheerlijken terrorisme en gebruiken symbolen van extremistische en terroristische groepen in hun materiaal. Nieuwe digitale omgevingen, zoals *extended reality* (een verzamelnaam voor technologieën zoals *virtual reality* die digitale elementen met de echte wereld combineren) en de *metaverse* (een gedeelde virtuele wereld waarin mensen via *avatars* kunnen samenwerken, spelen, winkelen en sociale contacten onderhouden), worden ingezet om nieuwe vormen van emotionele manipulatie, *grooming* en radicaliseringspaden te ontwikkelen. Voor het gebruik van terroristisch materiaal om individuen aan te zetten kinderpornografisch materiaal te bekijken, te verspreiden of te maken, is in dit onderzoek geen bewijs gevonden. Wij bevelen de ATKM aan geïntegreerde monitoring en analyse in te zetten om dit fenomeen zo volledig mogelijk in kaart te brengen.

[260] Oudenhuijsen, L. & Janssen, J. (2026), De overlap tussen terroristische online inhoud en kinderpornografisch materiaal. Een (verkennende)literatuurstudie.
[261] HCSS (2026), HCSS Focus Het Com-netwerk.

3.5 Effectiviteit en impact op online veiligheid

Bevindingen in het kort

- Op outputniveau is de Uitvoeringswet TOI effectief: verwijderbevelen worden vrijwel altijd tijdig nageleefd. Tegelijkertijd wijst vergelijking met andere lidstaten, met name Duitsland, erop dat Nederland mogelijk kansen laat liggen omdat het blootstellingsbesluit niet wordt ingezet.
- Een causale koppeling met een aantoonbare vermindering van terroristische online inhoud in enge zin kan niet worden gelegd; een nulmeting ontbreekt en content herplaatst zich snel.
- Afname van terroristische online inhoud op grote platforms is hoofdzakelijk toe te schrijven aan het eigen moderatiebeleid van platforms, niet specifiek aan de Uitvoeringswet TOI.
- Een deel van de content verschuift naar besloten kanalen en fringe-platformen buiten de reikwijdte van de verordening.
- De wet heeft een reële normstellende werking: platforms zijn zich in toenemende mate bewust van hun verantwoordelijkheden.
- De meerwaarde van de wetgeving ligt mede in haar signalerende, kennisopbouwende en normstellende functie, die zich niet laat uitdrukken in aantallen verwijderingen.

3.5.1 Heeft de Uitvoeringswet TOI bijgedragen aan een aantoonbare vermindering van de beschikbaarheid van terroristische online inhoud?

De beantwoording van deze vraag vereist onderscheid tussen verschillende niveaus van effectiviteit. Enerzijds kan worden gekeken naar de output van de wet, waaronder het aantal uitgevaardigde verwijderbevelen en de mate waarin deze worden nageleefd. Anderzijds richt de evaluatievraag zich op de feitelijke beschikbaarheid van terroristische online inhoud in het digitale domein.

Hoewel de output van de wet in zekere mate meetbaar is, bijvoorbeeld in de vorm van het aantal verwijderbevelen, blijkt het aanzienlijk complexer om vast te stellen in hoeverre deze output zich vertaalt in een (substantiële) vermindering van de beschikbaarheid van terroristisch materiaal online. Om deze vraag te beantwoorden, wordt dan ook eerst ingegaan op de aantoonbare output van de wet, waarna wordt gereflecteerd op de mogelijkheden en beperkingen om uitspraken te doen over de effectiviteit in termen van de beschikbaarheid van terroristische online inhoud.

Outputniveau

Zoals eerder beschreven in paragraaf 3.1, zijn in 2024 ongeveer 330 verwijderbevelen uitgevaardigd (respectievelijk 150 en 180).[262] Vrijwel alle bevelen zijn in zowel 2024 als 2025 binnen de termijn van één uur opgevolgd. Overschrijdingen betroffen in 2024 twee gevallen en in 2025 circa dertien gevallen, waarbij het doorgaans om lichte vertragingen van enkele minuten ging.[263] Het is goed om te weten dat een verwijderbevel niet per se gelijkstaat aan het verwijderen van één afbeelding of tekst. Het kan ook zijn dat, naar aanleiding van een bevel, meerdere typen content ontoegankelijk worden gemaakt, of dat een aanbieder van een hostingdienst een heel kanaal heeft verwijderd.[264]

---

262 ATKM (2025), Jaarverslag 2024; ATKM (2026), Jaarverslag 2025.
263 Ibid.
264 Ibid.

De ATKM heeft een concreet en meetbaar aantal verwijderbevelen uitgevaardigd en HSPs volgen deze bevelen over de algehele linie op. Tegelijkertijd kan op basis hiervan niet worden vastgesteld in hoeverre dit leidt tot een aantoonbare afname van de beschikbaarheid van terroristische online inhoud. Er ontbreekt namelijk een totaalbeeld van de hoeveelheid terroristische online inhoud die circuleert, waardoor er geen nulpunt of referentiepunt is om veranderingen in de beschikbaarheid te duiden. Daarnaast kan deze verwijderde content zich snel opnieuw verspreiden, bijvoorbeeld omdat deze opnieuw (licht bewerkt) wordt geplaatst of naar andere platforms uitwijkt.[265] Dit maakt dat het effect van individuele verwijderingsinterventies vaak tijdelijk is en lastig te aggregeren tot een structureel effect. Dit hoeft volgens de geïnterviewden echter niet te betekenen dat de wet geen effect heeft (zie ook paragraaf 3.5.2).[266]

Bredere ontwikkelingen in de beschikbaarheid van terroristische online inhoud en de impact hiervan

Wanneer gekeken wordt naar bredere ontwikkelingen in de beschikbaarheid van terroristische online inhoud, schetsen de geïnterviewden een genuanceerd beeld. Enerzijds lijkt sprake te zijn van een afname van publiek zichtbare terroristische online inhoud op grote HSPs. Deze ontwikkeling wordt doorgaans toegeschreven aan een strenger moderatiebeleid van platforms in den brede en kan niet specifiek worden gekoppeld aan de werking van de Uitvoeringswet TOI.[267] Tevens signaleren geïnterviewden een verschuiving naar meer besloten kanalen. Terroristische online inhoud lijkt in toenemende mate te verplaatsen naar moeilijker toegankelijke omgevingen, waaronder besloten groepen of door gebruik te maken van verhullende taal of symboliek. In lijn hiermee geven sommige geïnterviewden aan dat de focus op openbare kanalen in toenemende mate minder effectief kan zijn, omdat een groter deel van de communicatie zich buiten het directe zicht afspeelt.[268]

Daarnaast wijzen geïnterviewden op een bredere fragmentatie van het online landschap, waarbij gebruikers en content zich over een groot aantal platforms verspreiden. Dit kan ertoe leiden dat er juist meer routes ontstaan voor de verspreiding van content, wat het zicht op en de beheersing van het fenomeen verder compliceert.[269]

Effectiviteit van de instrumentkeuze binnen de Uitvoeringswet

Wat betreft de effectiviteit van de gekozen instrumenten binnen de Uitvoeringswet TOI valt op dat in de praktijk alleen verwijderbevelen worden gebruikt. Het tweede instrument, het blootstellingbesluit, wordt vooralsnog niet ingezet. In theorie zou juist dit instrument op de middellange termijn meer structurele effecten kunnen realiseren in termen van verminderde beschikbaarheid van terroristische online inhoud.[270]

3.5.2 Is het waarschijnlijk dat de Uitvoeringswet TOI heeft bijgedragen aan de verbetering van de (online) veiligheid in het kader van nationale veiligheid en terrorismebestrijding?

De Uitvoeringswet TOI richt zich primair op het beperken van de beschikbaarheid van terroristische online inhoud en beïnvloedt daarmee met name de online informatieomgeving

---

265 Interview met academici, april 2026; Interview met academici, april 2026.

266 Ibid.

267 Interview met academici, april 2026; Interview met academici, april 2026; Interview met opsporingsdienst, maart 2026; Europese Commissie (2024), Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on adressing the dissemination of terrorist content online.

268 Ibid.

269 Ibid.

270 Interview met ministerie van Justitie en Veiligheid, februari 2026.

waarin radicalisering en propaganda plaatsvinden. Dit betekent dat de effecten van de wet niet direct zichtbaar zijn in termen van een concrete vermindering van de dreiging of het voorkomen van terroristische incidenten, maar eerder indirect. De rol van de Uitvoeringswet TOI dient daarom te worden bezien in samenhang met andere wet- en regelgeving en beleidsprogramma's binnen het bredere nationale veiligheidsstelsel.

Binnen de Nederlandse Contraterrorisme Strategie 2022-2026 (NCTS) wordt expliciet aandacht besteed aan de rol van het online domein bij terrorisme en gewelddadig extremisme, naast thema's als de alleen handelende dader en veilige re-integratie na detentie.[271] De Uitvoeringswet TOI sluit met name aan bij het onderdeel dat zich richt op het online domein door een concreet juridisch instrument te bieden om terroristische online inhoud daadwerkelijk te laten verwijderen. Daarmee vormt de wet een schakel tussen beleidsdoelen op strategisch niveau en de praktische handhaving in het online domein.

Aanvullend hierop is ook de versterkte aanpak online extremistische en terroristische content ingericht langs vier actielijnen: preventie en bewustwording, normeren en signaleren, reguleren en handhaven en kennis en onderzoek. Hieronder vallen vier inhoudelijke pijlers: dialoog met de internetsector, inzet van het wettelijk instrumentarium, de lokale aanpak en de Europese en internationale samenwerking.[272] De Uitvoeringswet TOI geeft invulling aan de actielijn 'wettelijk instrumentarium' en versterkt daarmee de andere actielijnen. Zo kan de wet de dialoog met platforms ondersteunen omdat een duidelijk normatief kader bestaat en draagt zij via samenwerking met buitenlandse autoriteiten bij aan de internationale dimensie van deze aanpak.

Een voorbeeld hiervan is dat de ATKM beoogt om, via haar interactie met de internetsector, bij te dragen aan de effectiviteit van de Uitvoeringswet TOI bij het verbeteren van de (online) veiligheid. Deze interacties kunnen bijdragen aan bewustwording bij HSPs.[273] In paragraaf 3.4.3 wordt deze rol nader beschreven.

Meerdere geïnterviewden geven dan ook aan dat de meerwaarde van de Uitvoeringswet TOI niet alleen moet worden benaderd in termen van directe veiligheidsopbrengsten, maar ook in termen van bewustwording en gedragsverandering bij platforms.[274] Zo wordt door geïnterviewden aangegeven dat ze de indruk hebben dat platforms zich in toenemende mate bewust zijn van hun verantwoordelijkheden met betrekking tot terroristische content en gemotiveerd zijn om hun platforms 'schoon' te houden.[275] Deze toegenomen alertheid kan er bovendien aan bijdragen dat potentieel schadelijke content en opkomende trends eerder worden gesignaleerd.
Tegen deze achtergrond kan de bijdrage van de Uitvoeringswet TOI aan de nationale veiligheid als volgt worden beoordeeld. De Uitvoeringswet TOI vormt slechts één van de factoren die van invloed kunnen zijn op de nationale veiligheid en dat is afhankelijk van de samenhang met andere maatregelen op EU-niveau en op nationaal niveau. Het is daarom

---

271 NCTV (2022), Nationale Contraterrorisme Strategie (NCTS) 2022-2026.

272 Ministerie van Justitie en Veiligheid (2023), Contourenbrief Versterkte Aanpak Online inzake extremistische en terroristische content; Tweede Kamer; Tweede Kamer, Beslisnota bij Kamerbrief over voortgang Versterkte Aanpak Online inzake extremistische en terroristische content, 15 mei 2026, referentie 7551976.

273 Ministerie van Justitie en Veiligheid (2023), Contourenbrief Versterkte Aanpak Online inzake extremistische en terroristische content

274 Interviews met ATKM, februari – april 2026; Interview met ministerie van Justitie en Veiligheid, februari 2026; Interview met opsporingsdienst, maart 2026.

275 Ibid; Interview HSP, april 2026.

aannemelijk dat de wet heeft bijgedragen aan bewustwording bij HSPs over hun verantwoordelijkheden en dat de aanwezigheid van de ATKM een normstellend effect kan hebben. Een directe causale koppeling met verbeterde nationale veiligheid en minder terrorisme is echter niet te maken. De ATKM is gericht op content en niet op verdachten of netwerken, waardoor haar bijdrage aan terrorismebestrijding in enge zin beperkt is. Haar meerwaarde ligt eerder in het versterken van het toezicht, kennisopbouw en normstelling rond online terroristisch materiaal.

3.5.3 Zijn aanpassingen in de wetgeving of uitvoering aan te raden om de effectiviteit van de Uitvoeringswet TOI te verbeteren. Zo ja, welke aanpassingen?

Op een aantal punten laat de Uitvoeringswet TOI effectiviteit zien. Zo worden de verwijderbevelen opgevolgd die de ATKM op grond van de wetgeving uitvaardigt en zijn er signalen dat content sneller wordt verwijderd dan voorheen. Daarmee is de wet effectief in de zin dat zij bijdraagt aan het beperken van de zichtbaarheid van terroristische online inhoud. Bovendien vervult de wet een belangrijke signaal- en normstellende functie richting platforms.

De bevindingen uit de voorgaande paragrafen wijzen erop dat de effectiviteit van de Uitvoeringswet TOI op onderdelen verder kan worden versterkt, zowel in de wetgeving als in de uitvoering. Deze mogelijke versterkingen hangen nauw samen met knelpunten die betrekking hebben op de afbakening van de wet, het beschikbare instrumentarium en de wijze waarop de uitvoering in de praktijk is ingericht.

Knelpunten en aanpassingen in de wetgeving

Uit de interviews en analyse komt naar voren dat de afbakening en toepassing van definities in de praktijk niet altijd eenduidig zijn. Zo wijzen verschillende geïnterviewden op onduidelijkheid over wanneer content onder de wet valt en wanneer andere kaders, zoals de DSA, van toepassing zijn.[276] Deze overlap maakt het voor betrokken partijen complex om te bepalen welk juridisch instrument in welke situatie moet worden ingezet.

Daarnaast wordt door sommige geïnterviewden de vraag opgeworpen in hoeverre de huidige focus op TOI nog aansluit bij bredere ontwikkelingen rondom extremistische en gewelddadige online content.[277] In dat kader wordt gewezen op een mogelijke verruiming van mandaat van de ATKM (zie ook paragraaf 3.2).[278] Een soortgelijk geluid gaat op ten aanzien van de definitie van ‘materiaal’; het valt te overwegen of moderne verschijningsvormen zoals chatbots, large *language models* of *game-mods* ook als materiaal te classificeren.[279] Ten slotte bestaat ook behoefte aan een eenduidige kader ten aanzien van materiaal dat uitgesloten is van de Uitvoeringswet TOI.[280] Er is op dit moment namelijk geen uniform kader op EU-niveau ten aanzien van de interpretatie van dit materiaal.[281]

---

276 Interview met academici, april 2026.
277 Interview met ministerie van Justitie en Veiligheid, februari 2026.
278 Ibid.
279 Schriftelijke input ATKM, april 2026.
280 Materiaal dat voor educatieve, journalistieke, artistieke of onderzoeksdoeleinden of met het oog op het voorkomen of bestrijden van terrorisme onder het publiek wordt verspreid, met inbegrip van materiaal dat een uiting vormt van polemische of controversiële standpunten in het publieke debat, wordt niet geacht terroristische inhoud te zijn (art. 1, derde lid, TOI-verordening)
281 Schriftelijke input ATKM, april 2026.

Knelpunten en aanpassingen in de uitvoering

Naast de reikwijdte van de wetgeving speelt ook de inrichting van het instrumentarium een rol. Met name het blootstellingsbesluit wordt door betrokken publieke partijen als beperkt effectief ervaren. Dit hangt samen met het feit dat dit instrument geen concrete verplichtingen aan platforms kan opleggen en slechts een inspanningsverplichting bevat, waarvan de naleving moeilijk te beoordelen is.[282] Tegelijkertijd wordt ook terughoudendheid ervaren bij het inzetten van dit instrument, mede vanwege de spanning met de gewenste samenwerking met platforms en het ontbreken van een uniforme Europese werkwijze voor de toepassing ervan.[283] Ook verschillen tussen lidstaten in de wijze waarop deze procedures zijn ingericht, dragen bij aan onzekerheid in de toepassing.[284]

Daarnaast geeft de ATKM aan dat zij ten aanzien van het opleggen van een last onder dwangsom geholpen zouden zijn met expliciete referenties in de Uitvoeringswet TOI naar de artikelen die een overtreding opleveren (in plaats van een verwijzing, zoals nu het geval is). Expliciete verwijzingen zouden de grondslag voor het opleggen van een last onder dwangsom wegens niet naleving logischer en helderder maken.[285]

In de uitvoering doen zich daarnaast knelpunten voor op het gebied van capaciteit en technische ondersteuning. Zo geeft de ATKM aan dat de beschikbare personele capaciteit en de inrichting van functies binnen haar organisatie niet altijd voldoende aansluiten bij de taken en dat de technische systemen nog in ontwikkeling zijn of beperkingen kennen. Dit heeft gevolgen voor de snelheid en efficiëntie van processen, waaronder de detectie en beoordeling van content, wat ook gevolgen heeft voor de effectiviteit van de wet.[286]

---

282 Interviews met ATKM, februari en april 2026; Validatiesessie, mei 2026.

283 Interview met ministerie van Justitie en Veiligheid, februari 2026.

284 Interview met ATKM, April 2026.

285 Specifiek is de suggestie om in de Uitvoeringswet een grondslag op te nemen voor het opleggen van een last onder dwangsom wegens de niet naleving van (o.a.) artikel 3 lid 3 van de verordening, artikel 4 lid 2, etc. (na voorbeeld van de bestuurlijke boete (zie art. 12 lid 1 Uitvoeringswet). Schriftelijke input ATKM, april 2026.

286 Interviews met ATKM, februari en april 2026; Validatiesessie, mei 2026.

4 Conclusies en aanbevelingen

Dit hoofdstuk beantwoordt de centrale onderzoeksvraag: ‘In hoeverre is de Uitvoeringswet TOI doeltreffend en hoe functioneert de wet, in het bijzonder voor wat betreft de toepassing en werking van de wet in de praktijk, de bestuurlijke constructie waarvoor is gekozen, alsook de balans tussen enerzijds de toepassing van de wet en anderzijds de rechtsstatelijke bescherming van aanbieders van hostingdiensten en internetplatformen en gebruikers van internetinhoud?’ Daarnaast worden enkele concrete aanbevelingen voor de toekomst geformuleerd.

4.1 Conclusies

Alles overziend kan worden geconcludeerd dat de Uitvoeringswet TOI in de praktijk grotendeels functioneert zoals beoogd. Verwijderbevelen worden zorgvuldig voorbereid door de ATKM, uitgevaardigd en in de regel tijdig nageleefd. Ook zijn er geen aanwijzingen dat de toepassing van de wet leidt tot onevenredige inbreuken op grondrechten of andere ongewenste neveneffecten. De ATKM heeft zich bovendien in korte tijd ontwikkeld tot een gezaghebbende uitvoeringsorganisatie en vervult internationaal een actieve rol in de verdere ontwikkeling van de uitvoering van de EU-verordening en, op Nederlands niveau, de Uitvoeringswet TOI.

Tegelijkertijd roept het onderzoek de vraag op in hoeverre het huidige instrumentarium voldoende is toegerust om de bredere uitdaging van terroristische online inhoud effectief aan te pakken. Het bereik van de wet wordt in de praktijk begrensd omdat de uitvoering sterk leunt op één instrument, het verwijderbevel, terwijl andere instrumenten die meer gericht zijn op structurele of preventieve effecten, zoals het blootstellingsbesluit, vooralsnog niet worden ingezet. Daarnaast leidt de keuze voor de ATKM als zelfstandig bestuursorgaan weliswaar tot belangrijke voordelen op het gebied van onafhankelijkheid en samenwerking met hostingdiensten, maar ook tot afhankelijkheden van andere partijen, met name de politie. Ten slotte is het aannemelijk dat de huidige, grotendeels handmatige detectiewijze ertoe leidt dat slechts een deel van de beschikbare terroristische online inhoud daadwerkelijk in beeld komt.

Deze conclusies worden verder uitgewerkt in de volgende alinea’s.

De wet functioneert, maar bereik is beperkt

De Uitvoeringswet TOI heeft in de eerste jaren na haar inwerkingtreding laten zien dat zij in beginsel effectief is als instrument om specifieke terroristische online inhoud ontoegankelijk te maken. De verwijderbevelen die de ATKM uitvaardigt, worden vrijwel zonder uitzondering tijdig nageleefd door HSPs en vrijwel alle bevelen zijn binnen de wettelijke termijn van één uur uitgevoerd. Daarmee functioneert het verwijderbevel in de praktijk zoals bedoeld. De ATKM is bovendien verantwoordelijk voor een aanzienlijk deel, ongeveer 20% van het totaal aantal verwijderbevelen verstuurd door bevoegde autoriteiten in de lidstaten in 2024 en 2025.

Tegelijkertijd is het bereik van de wet ten aanzien van de totale omvang van online terroristische inhoud beperkt. Het aantal uitgevaardigde bevelen is, afgezet tegen de schaal van het online terroristische inhoudslandschap, naar schatting klein. Van alle door de ATKM geïdentificeerde content mondt naar schatting slechts een kwart uit in een verwijderbevel. Voor het grootste deel van de overige geïdentificeerde content geldt dat het *borderline content* betreft en niet als TOI kwalificeert. Dit weerspiegelt deels een bewuste keuze van de ATKM voor zorgvuldigheid, maar ook structurele beperkingen van het instrument. Het is daarbij van belang deze cijfers met voorzichtigheid te interpreteren. Het aandeel gevallen waarin een verwijderbevel wordt opgelegd, vormt geen schatting van het aandeel terroristische online inhoud dat door de wet wordt aangepakt.

Het aandeel verwijderbevelen ten aanzien van de totale omvang van geïdentificeerde content is bovendien gebaseerd op wat de ATKM weet te identificeren. Het is aannemelijk dat een groot deel van de online terroristische inhoud door de beperkte handmatige detectiecapaciteit en de grenzen van het open internet niet in beeld komt. De wet bereikt daarmee slechts een deel van het fenomeen dat zij beoogt te bestrijden. Dit is overigens een conclusie die ook ziet op de EU-verordening en niet louter op de Nederlandse Uitvoeringswet TOI.

Borderline content blijft buiten bereik

Een aanzienlijk deel van de door de ATKM gesignaleerde online content valt buiten de reikwijdte van de Uitvoeringswet TOI. Het gaat daarbij om extremistische, radicaliserende of anderszins zorgwekkende uitingen die niet eenduidig kwalificeren als terroristische online inhoud in de zin van de EU-verordening. Voorbeelden zijn impliciete of gecodeerde boodschappen, ideologische propaganda zonder expliciete oproep tot geweld, of content die terroristische narratieven normaliseert zonder binnen de wettelijke definitie van terroristische online inhoud te vallen. De ATKM beschikt in dergelijke gevallen niet over een grondslag om handhavend op te treden.

Dit verschil tussen de bredere online problematiek en het deel waarop de Uitvoeringswet TOI daadwerkelijk van toepassing is, wordt door verschillende stakeholders als een aandachtspunt gezien. Tegelijkertijd weerspiegelt deze begrenzing een bewuste keuze van de wetgever om het optreden van de overheid te beperken tot duidelijk afgebakende vormen van terroristische online inhoud. De vraag of de ATKM ook een rol zou moeten spelen ten aanzien van dergelijke borderline content, bijvoorbeeld via niet-bindende verwijderverzoeken, blijft onderwerp van debat.

Het instrumentarium wordt onvolledig benut

De Uitvoeringswet TOI kent naast het verwijderbevel ook het blootstellingsbesluit, de last onder dwangsom, de bestuurlijke boete en de geschilbeslechtingsprocedure. In de praktijk maakt de ATKM uitsluitend gebruik van het verwijderbevel. Dit is deels een bewuste strategische keuze: de ATKM hecht aan een constructieve relatie met platforms en deels is het een gevolg van beperkte capaciteit (slechts enkele juridische experts aanwezig) en onduidelijkheden over de toepassing van een blootstellingsbesluit in de praktijk. In het bijzonder het blootstellingsbesluit is het meest structurele instrument dat de wet biedt voor langetermijneffecten, maar het is nog nooit ingezet door de ATKM. Naarmate de ATKM volwassener wordt en het aantal bevelen toeneemt, zal het onbenut laten van dit instrument een steeds groter effectiviteitslek vormen.

De rechtsstatelijke borging is vooralsnog adequaat, maar niet onafhankelijk gevalideerd

De beoordelingsprocedure van de ATKM is zo ingericht dat grondrechtelijke overwegingen, met name de vrijheid van meningsuiting, expliciet worden meegewogen in elke beslissing. Er zijn geen aanwijzingen voor structurele overblokkering of *chilling effects* die aan de Uitvoeringswet TOI toe te schrijven zijn. Tot op heden zijn geen bezwaar- of beroepsprocedures gestart, wat betekent dat de inhoudelijke beoordelingscriteria van de ATKM nog niet onafhankelijk door een rechter zijn getoetst. Dit hoeft niet te duiden op problemen, maar maakt de robuustheid van het positieve oordeel over de rechtsstatelijke borging vooralsnog beperkt.

ATKM als jonge organisatie op een keerpunt

De ATKM is een jonge organisatie die in korte tijd een aanzienlijke operationele en institutionele ontwikkeling heeft doorgemaakt. Zij heeft een werkend primair proces ingericht, samenwerkingsafspraken gesloten met ketenpartners, een internationale positie opgebouwd en expertise ontwikkeld op een complex en technisch gebied. Dat is een prestatie die niet als vanzelfsprekend mag worden beschouwd, zeker gezien de startproblemen rond ICT-systemen en de aanvankelijke onderbezetting van cruciale functies.

Tegelijkertijd is de ATKM nog niet de volwassen uitvoeringsorganisatie die de wet op termijn vereist. De detectie is volledig handmatig; geautomatiseerde detectieinstrumenten zijn niet beschikbaar. De bezetting op het primaire TOI-proces telt slechts vijf medewerkers en de huisvesting biedt onvoldoende ruimte voor de huidige organisatie. De bestedingspatronen in 2025, met overschrijdingen op externe inhuur en ICT ten opzichte van de begroting, weerspiegelen een organisatie die zich nog in een ontwikkelfase bevindt en haar processen en ramingen verder aan het verfijnen is. Kortom, terwijl de afgelopen jaren voor de ATKM in het teken stonden van het opbouwen van de organisatie, staat zij nu voor een volgende fase van doorontwikkeling waarin verdere professionalisering van de organisatie en haar processen centraal staat.

De zbo-constructie heeft meerwaarde, maar ook structurele beperkingen

De keuze om de ATKM als zelfstandig bestuursorgaan in te richten, heeft aantoonbare voordelen opgeleverd. De onafhankelijkheid van politieke aansturing borgt de zorgvuldigheid van de besluitvorming. De neutrale positie stelt de ATKM in staat een vertrouwensrelatie op te bouwen met HSPs die opsporingsdiensten doorgaans moeilijker of niet kunnen realiseren. Ook heeft de ATKM juist specialistische expertise op kunnen bouwen door zich te focussen op terroristische online inhoud. Het onderbrengen van de TOI-taak en het bestrijden van kinderpornografisch materiaal online (kinderpornografisch materiaal-taak) zorgt bovendien voor synergiën en efficiëntiewinst. De ATKM is de enige bevoegde autoriteit in de EU zonder opsporingsbevoegdheden en wordt desondanks als een volwaardige partner beschouwd in het Europese speelveld.

De prijs van die constructie is echter concreet en structureel: de ATKM is geen opsporings-instantie en heeft daarom geen directe toegang tot Europol-informatiesystemen als SIENA, geen automatische aanlevering van Europol-producten als Check the Web en hashlists en ze is afhankelijk van de politie als intermediair voor deconflictie.[287] Dit raakt zowel de

[287] Deconflictie is de controle waarbij de ATKM vooraf afstemt met politie of geïdentificeerde online content onderdeel is van een lopend onderzoek, zodat een verwijderbevel geen opsporings- of inlichtingenonderzoek verstoort.

informatiepositie als de snelheid van het primaire proces. De deconflictie op EU-niveau is bovendien niet sluitend: door beperkt gebruik van de *whitelistfunctie* in PERCI door opsporingsdiensten in andere lidstaten kan de ATKM in theorie een verwijderbevel uitsturen op materiaal dat onderdeel is van een lopend opsporingsonderzoek elders in de EU. Dit is een structureel risico dat niet uniek is voor de ATKM, maar dat bij de zbo-constructie moeilijker is te mitigeren vanwege de beperkingen die de ATKM ervaart wat betreft de communicatie met opsporingsinstanties in andere lidstaten.

Samenwerking met ketenpartners verbetert, maar heeft witte vlekken
De samenwerking tussen de ATKM en haar voornaamste ketenpartners, NCTV, nationale politie, opsporingsorganisaties in andere lidstaten en Europol, verloopt overwegend goed en is gedurende de afgelopen jaren verder uitgebouwd. Zo coördineren op zowel strategisch als operationeel niveau de ATKM en politie inmiddels met regelmaat, deelt de politie sinds het voorjaar van 2026 relevante informatie met de ATKM zoals profielen, websites en accounts en wordt onderzocht of en hoe ook andere informatie vanuit de politie met de ATKM gedeeld kan en mag worden, conform de Wet politiegegevens. Knelpunten blijven bestaan in de internationale deconflictie en in het ontbreken van structurele terugkoppeling van ATKM-trendkennis naar ketenpartners.

Een causaal verband met verminderde online veiligheidsrisico's is niet aantoonbaar
De vraag of de Uitvoeringswet TOI heeft bijgedragen aan een aantoonbare vermindering van de beschikbaarheid van terroristische online inhoud, kan op basis van dit onderzoek niet met zekerheid worden beantwoord. Er ontbreekt een nulmeting van de totale hoeveelheid TOI die online circuleert en ontoegankelijk gemaakte content kan zich (in bewerkte vorm, bijvoorbeeld door AI) snel opnieuw verspreiden op andere platforms of via besloten kanalen. Bovendien lijkt een deel van de terroristische online activiteit te zijn verschoven naar minder goed te monitoren omgevingen: besloten groepen, versleutelde communicatiekanalen en *fringe*-platformen buiten de reikwijdte van de EU-verordening. De wet vormt daarmee één instrument in een bredere aanpak en de effectiviteit ervan is mede afhankelijk van flankerend beleid, platformverantwoordelijkheden en internationale samenwerking.

De normstellende werking is reëel maar moeilijk te meten
Naast de directe effecten op het ontoegankelijk maken van content heeft de wet ook een indirecte, normstellende werking. De aanwezigheid van de ATKM als onafhankelijke autoriteit stuurt het gedrag van platforms: er zijn signalen dat HSPs zich in toenemende mate bewust zijn van hun verantwoordelijkheden en gemotiveerd zijn om hun platforms vrij te houden van terroristische inhoud. Een deel van die bewustwording is niet direct toe te schrijven aan de Uitvoeringswet TOI. Platformbeleid, DSA-verplichtingen en internationale druk spelen ook een rol. De ATKM draagt echter bij aan het bevestigen van normen en het bespreekbaar maken van verantwoordelijkheden in de sector.

4.2 Aanbevelingen

Aanbevelingen zijn onderverdeeld in aanbevelingen gericht aan het Ministerie van Justitie en Veiligheid en de regering, en aanbevelingen gericht aan de ATKM als uitvoeringsorganisatie.

Aanbevelingen aan de het Ministerie van Justitie en Veiligheid en de regering

1. Heroverweeg de geschilbeslechtingsprocedure van artikel 16 Uitvoeringswet TOI

Nederland is de enige lidstaat die een aanvullende geschilbeslechtingsprocedure heeft opgenomen in de implementatiewet. De procedure is tot op heden niet benut. Bovendien beschouwt de ATKM haar dubbele rol als complex: als autoriteit neemt zij blootstellingsbesluiten en als geschillenbeslechter bestaat de kans dat zij (de acties die voortvloeien uit) de besluiten moet toetsen. Daarnaast verwacht de ATKM dat de toepassing ervan capaciteitsintensief zal zijn. Gelet op het feit dat gebruikers via een bestuursrechteljke procedure en via de DSA al adequate rechtsbescherming genieten, verdient heroverweging, dan wel vereenvoudiging, van deze procedure aanbeveling.

2. Onderzoek de beleidsmatige haalbaarheid van een verwijderverzoek van TOI als aanvullend instrument voor de ATKM

Nederland is een van de weinige EU-lidstaten die uitsluitend het bindende verwijderbevel gebruikt. Veel lidstaten werken ook met niet-bindende verzoeken en grijpen pas naar een bevel bij niet-naleving. Een verwijderverzoek verkort de doorlooptijd, verlaagt de administratieve last en geeft de HSP meer tijd om te reageren. De juridische ruimte voor een verwijderverzoek ten aanzien van TOI-content is in de huidige wet aanwezig. De inzet van verzoeken naast bevelen kent voor- en nadelen en op basis hiervan is een zorgvuldige afweging ten aanzien van het al dan niet inzetten van verzoeken op zijn plaats.

3. Onderzoek de juridische haalbaarheid van een ruimer mandaat voor de ATKM om ook te ageren tegen borderline content

Verzoeken kunnen op dit moment door de ATKM expliciet niet op *borderline content* ingezet worden. Indien dit wenselijk wordt geacht, zouden andere routes verkend moeten worden, waaronder uitbreiding van het wettelijk kader of het aanmerken van de ATKM als *DSA trusted flagger*.

4. Investeer in de technische en personele randvoorwaarden voor de ATKM

Het huidige budget en de huidige bezetting zijn onvoldoende voor een ATKM die ook op de middellange termijn effectief kan opereren. De automatisering en financiering van geautomatiseerde detectie-instrumenten, een bezetting die continuïteitsrisico's beperkt en adequate huisvesting die rekening houdt met de bijzondere aard van het werk zijn geen luxe maar randvoorwaarden voor effectieve wetsuitvoering.

5. Faciliteer de toegang van de ATKM tot relevante Europol-informatie

De informatiepositie van de ATKM wordt begrensd door het ontbreken van directe toegang tot Europol-producten, zoals Check the Web en hashlists. In afstemming met Europol en de politie verdient het aanbeveling om afspraken te maken over de gestructureerde en tijdige aanlevering van deze informatie aan de ATKM, zonder hierbij de principiële scheiding tussen toezicht (ATKM) en opsporing (politie) uit het oog te verliezen.

Aanbevelingen aan de ATKM

6. Zet in op het operationaliseren van geautomatiseerde detectietooling als strategische prioriteit

Handmatige detectie is de voornaamste bottleneck in het primaire proces. Geautomatiseerde detectie is niet alleen een efficiëntiewinst, maar ook een voorwaarde voor schaalbaarheid (onder andere meer detectie, maar ook bijvoorbeeld detectie buiten kantooruren). De ATKM

dient het maatwerktraject voor detectiesoftware te prioriteren en waar mogelijk interimoplossingen te benutten die op korte termijn de periode tot implementatie overbruggen.

7. Ontwikkel een kader voor de inzet van het blootstellingsbesluit

Het blootstellingsbesluit is bij uitstek een instrument dat structurele gedragsverandering bij HSPs kan afdwingen. De ATKM dient, bij voorkeur in EU-verband, een werkwijze te ontwikkelen voor de toepassing ervan, inclusief criteria voor wanneer een blootstellingsbesluit proportioneel is en hoe de naleving van de inspanningsverplichting kan worden beoordeeld. De ATKM wordt aangemoedigd om op Europees niveau voor opheldering ten aanzien van de inzet van dit instrument te verzoeken.

8. Structureer de terugkoppeling van trendkennis naar ketenpartners

De ATKM bouwt waardevolle kennis op over terroristische online inhoud, narratieven en patronen. Deze kennis vloeit nog onvoldoende structureel terug naar partners als de nationale politie en de NCTV. Het inrichten van periodieke rapportages of feedbackmechanismen versterkt de positie van de ATKM in de keten en vergroot de bredere maatschappelijke waarde van haar werk.

9. Vergroot de zichtbaarheid van het meldpunt en analyseer de instroom.

Het openbare meldpunt voor derden (zoals burgers, maatschappelijke organisaties of wetenschappers) van de ATKM is in november 2025 geopend, maar hierover is tot op heden (juni 2026) nog nauwelijks gecommuniceerd. Actievere bekendmaking van het meldpunt en het opzetten van een analysekader voor de instroom, ook om te leren van meldingen die niet als TOI kwalificeren, versterkt zowel het detectievermogen als de leeropgave van de ATKM.

Bijlage I – Bibliografie

Wetgeving en wetsvoorstellen

Verordening (EU) 2021/784 van het Europees Parlement en de Raad van 29 april 2021 inzake het tegengaan van de verspreiding van terroristische online-inhoud. Europese Commissie. https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:32021R0784

Verordening (EU) 2022/2065 ban het Europees Parlement en de Raad betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening). Europese Commissie. https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022R2065

Voorstel voor een verordening van het Europees Parlement en de Raad tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen (2022/209). Europese Commissie. https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=COM%3A2022%3A209%3AFIN

Wetsvoorstel om verheerlijken van terrorisme strafbaar te stellen naar Raad van State. (2025). Rijksoverheid. https://www.rijksoverheid.nl/actueel/nieuws/2025/12/19/wetsvoorstel-om-verheerlijken-van-terrorisme-strafbaar-te-stellen-naar-raad-van-state

Uitvoeringswet verordening terroristische online-inhoud. (2021/784). *Overheid.nl.* Geraadpleegd op 8 juni 2026, van https://wetten.overheid.nl/BWBR0048064/2025-09-05.

Literatuur

Dauber, C. E., Robinson, M. D., Baslious, J. J. & Blair, A. G. (2019). Call of Duty: Jihad – How the Video Game Motif Has Migrated Downstream from Islamic State Propaganda Videos. *Perspectives on Terrorism, 13*(3). https://pt.icct.nl/article/call-duty-jihad-how-video-game-motif-has-migrated-downstream-islamic-state-propaganda

Driesse, M., Brennenraedts, R., Boiten, M. & Crielaard, J. (2023). Het belang van digitale infrastructuur voor de Nederlandse digitale knooppuntrol. *Dialogic*. https://dialogic.nl/wp-content/uploads/2024/01/Dialogic-Het-belang-van-digitale-infrastructuur-voor-de-Nederlandse-digitale-knooppuntrol.pdf

European Union Agency for Fundamental Rights. (2023). Online Content Moderation: Current Challenges in Detecting Hate Speech. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf

European Union Agency for Fundamental Rights. (2026). Regulating online terrorist content – Balancing public safety and fundamental rights. https://fra.europa.eu/en/publication/2025/regulating-online-terrorist-content

Gentile, F. & O'Keefe, I. G. (2025). Use of Coded Language by Far-Right Extremists Online: Emojis, Numbers, and Symbols Reinforce In-Group Identity. *VOX Pol.* https://voxpol.eu/coded-language-dog-whistles-tiktok-far-right/

Gherbaoui, T. & Scheinin, M. (2022). A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it. *European Journal of Human Rights, 2023*(1), 3-29. https://doi.org/10.2139/ssrn.4247120

Keats Citron, D. (2018). Extremist Speech, Compelled Conformity, and Censorship Creep. *Notre Dame Law Review, 93*(3). https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4772&context=ndlr

Macdonald, S., & Vaughan, K. (2024). Moderating borderline content while respecting fundamental values. *Policy & Internet, 16*, 347–361. https://doi.org/10.1002/poi3.376

Mehra, T. & van Ginkel, B. (2025). Boundaries to Borderline Content: Defining the scope of Implicit Extremist Content. *ICCT*. https://icct.nl/publication/boundaries-borderline-content-defining-scope-implicit-extremist-content

Oudenhuijsen, L. & Janssen, J. (2026). De overlap tussen terroristische online inhoud en kinderpornografisch materiaal: Een (verkennende)literatuurstudie. *Avans University of Applied Sciences*. https://www.researchgate.net/publication/400091861_De_overlap_tussen_terroristische_online-inhoud_en_kinderpornografisch_materiaal_Een_verkennendeliteratuurstudie

Peeters, T., van Wonderen, R., Burggraaff, D. & de Wit, N. (2022). Online extreemrechtse Radicalisering: Handvatten voor een preventieve aanpak. *Verwey Jonker*. https://www.verwey-jonker.nl/wp-content/uploads/2022/12/121650_Online-extreemrechtse-radicalisering.pdf

Sacher, A.-L., & Reinemann, C. (2025). What is Freedom of Speech? How Citizens Define and Perceive the “Bulwark of Liberty”. *The International Journal of Press/Politics*. https://journals.sagepub.com/doi/10.1177/19401612251388182

Saltman, E. & Hunt, M. (2023). Borderline Content: Understanding the Gray Zone. *Global Internet Forum to Counter Terrorism.* https://gifct.org/wp-content/uploads/2023/06/GIFCT-23WG-Borderline-1.1.pdf

The Hague Centre for Strategic Studies. (2026). HCSS Focus: Het Com-netwerk. https://hcss.nl/wp-content/uploads/2026/03/HCSS-Focus-Het-Com-Netwerk-2026.pdf

Van Ginkel, B., Mehra, T., Herbach, M. Lanchès, J. & Boerma, Y. (2025). Blurred Boundaries: Legal, Ethical and Practical limits in Detecting and Moderating Terrorist, Illegal, and Implicit Extremist Content Online While Respecting Freedom of Expression. *WODC*. https://icct.nl/publication/blurred-boundaries-legal-ethical-and-practical-limits-detecting-and-moderating

Van Noorloos, L. A. (2025). Strafbaarstelling van het verheerlijken van terrorisme en openbare steunbetuiging aan terroristische organisaties. *Tijdschrift Voor Constitutioneel Recht, 16*(4), 359-372. https://scholarlypublications.universiteitleiden.nl/handle/1887/4291796

Visser, R. (2024). Crowdfunding conspiracists: grassroots giving to January 6 participants. *ICCT*. https://icct.nl/publication/crowdfunding-conspiracists-grassroots-giving-january-6-participants

Rapporten, documenten en publicaties

Algemene Inlichtingen- en Veiligheidsdienst. (2025). Een web van haat - De online grip van extremisme en terrorisme op minderjarigen. https://www.rijksoverheid.nl/documenten/2025/04/03/een-web-van-haat-de-online-grip-van-extremisme-en-terrorisme-op-minderjarigen

Algemene Inlichtingen- en Veiligheidsdienst. (2026). AIVD Jaarverslag 2025. https://www.aivd.nl/actueel/magazines/jaarverslag/jaarverslag/2025

Anti-Defamation League. (2019). Hate on display: hate symbols database. https://www.adl.org/sites/default/files/ADL%20Hate%20on%20Display%20Printable_0.pdf

Autoriteit online Terroristisch en Kinderpornografisch Materiaal. (2025). Jaarverslag 2024. https://www.atkm.nl/documenten/2025/05/jaarverslag-atkm-2024

Autoriteit online Terroristisch en Kinderpornografisch Materiaal. (2026). Dwangsom- en boetebeleid Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM). *Staatscourant,* 21454. https://zoek.officielebekendmakingen.nl/stcrt-2026-21454.pdf

Autoriteit online Terroristische en Kinderpornografisch Materiaal. (2026). Jaarverslag 2025. https://www.atkm.nl/documenten/2026/05/20/jaarverslag-atkm-2025

Discord. (2026). EU Terrorist Content Online Regulation Transparency Report. https://cdn.discordapp.com/assets/transparency-reports/TCO-Report-2026.pdf

European Court of Human Rights. (1976, 7 december). Handyside v United Kingdom. Appl No 5493/72. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57499%22]}

Europese Commissie (2018). Commission staff working document impact assessment: Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0408

Europese Commissie. (2024). Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024DC0064

Europol. (2024). Online Jihadist Propaganda - 2023 in review. https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2023-in-review

Europol. (2025). EU Terrorism Situation and Trend Report 2025 (TE-SAT). https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2025-eu-te-sat

Facebook. (2026). European Union Terrorist Content Online Transparency Report. *Meta Platforms Ireland Limited.* [FB] EU TCO Transparency Report (27 Feb 2026)

Google. (2026). Regulation (EU) 2021/784 on addressing the dissemination of Terrorist Content Online Transparency Report. https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-26_2025-1-1_2025-12-31_en_v1.pdf

Instagram. (2026). European Union Terrorist Content Online Transparency Report. *Meta Platforms Ireland Limited*. https://transparency.meta.com/reports/regulatory-transparency-reports/

Kwartiermaker ATKM. (2022). Organisatie & Formatie rapport: Autoriteit online Terroristische en Kinderpornografisch Materiaal (ATKM).

Minister van Justitie en Veiligheid (2024). Uitvoeringsbesluitverordening terroristische online-inhoud. https://www.internetconsultatie.nl/uitvoeringsbesluittoiverordening/document/13636

Ministerie van Justitie en Veiligheid. (2025). Besluit van 30 augustus 2025, houdende regels voor de openbaar te maken gegevens in geval van openbaarmaking van boetebesluiten van de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal, wijziging van het Besluit politiegegevens met het oog op het introduceren van een grondslag voor gegevensdeling door de politie, alsmede vaststelling van het tijdstip van inwerkingtreding van de artikelen 13 en 16 van de Uitvoeringswet verordening terroristische online-inhoud. *Staatsblad van het Koninkrijk der Nederlanden, 2025*(216). https://zoek.officielebekendmakingen.nl/stb-2025-216.html

Minister van Justitie en Veiligheid, Minister van Buitenlandse Zaken, Minister van Economische Zaken en Klimaat, Minister van Sociale Zaken en Werkgelegenheid, Minister van Binnenlandse Zaken en Koninkrijksrelaties & Staatssecretaris van Koninkrijksrelaties en Digitalisering (2023). Contourenbrief Versterkte Aanpak Online extremistische en terroristische content. *Ministerie van Justitie en Veiligheid*. https://open.overheid.nl/documenten/dpc-98bd32c3b58ae623ff002c0aa085bb65dd8e0f85/pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2020). Verkenning: Een competente autoriteit voor de uitvoering van de verordening Terroristische Content Online.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2022). Nationale Contraterrorisme Strategie (NCTS) 2022-2026. https://www.nctv.nl/documenten/2022/05/20/nationale-contraterrorisme-strategie-ncts-2022-2026

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2024). Fenomeenanalyse 'Memes als online wapen'. https://www.nctv.nl/documenten/2024/05/21/fenomeenanalyse-memes-als-online-wapen

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025). Dreigingsbeeld Terrorisme Nederland 2025. https://www.nctv.nl/documenten/2025/12/09/dtn-december-2025

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2026). Dreigingsbeeld Terrorisme Nederland juni 2026. https://www.nctv.nl/documenten/2026/06/30/dreigingsbeeld-terrorisme-nederland-juni-2026

Snap Inc. (2026). 2025 Annual Report. https://investor.snap.com/financials/Annual-Report/default.aspx

Snap Inc. (2026). European Union Terrorist Content Online Transparency Report. https://values.snap.com/privacy/transparency/european-union-tco-h2-2025

Tweede Kamer. (2018). Motie van de leden Van Nispen en van Toorenburg over verzet tegen een verwijderingsbevel uit andere lidstaten. 22 112, nr. 2724. https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2018Z21597&did=2018D55474

Tweede Kamer. (2022). Amendement van het Lid Leijten: Uitvoeringswet verordening terroristische online-inhoud. 36 138, nr. 10. https://www.eerstekamer.nl/behandeling/20221221/amendement_van_het_lid_leijten_5/document3/f=/vm0ep5jbnhzv.pdf

Tweede Kamer. (2022). Memorie van toelichting: Uitvoeringswet verordening terroristische online-inhoud. 36 138, nr. 3. https://zoek.officielebekendmakingen.nl/kst-36138-3.pdf

Tweede Kamer. (2022), Nota naar aanleiding van het verslag: Uitvoeringswet verordening terroristische online-inhoud, 36 138, nr 7. https://www.eerstekamer.nl/behandeling/20221005/nota_naar_aanleiding_van_het/info

Tweede Kamer. (2022). Verslag plenair debat: Uitvoeringswet verordening terroristische online-inhoud. 36 138, nr. 6. https://www.eerstekamer.nl/behandeling/20220718/verslag/document3/f=/vlupm4hqrbrj.pdf

Twitch. (2026). EU Terrorist Content Online Regulation 2025 Transparency Report. https://safety.twitch.tv/s/article/2025-EU-Terrorist-Content-Transparency-Report?language=en_US

Van Nispen, M. & van Toorenburg, M. (2018). Motie van de leden Van Nispen en van Toorenburg over verzet tegen een verwijderingsbevel uit andere lidstaten. *Tweede Kamer*. https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2018Z21597&did=2018D55474

X. (2026). X Transparency Report for the Regulation (EU) 2021/789 on addressing the Dissemination of Terrorist Content Online January – December 2025. https://transparency.x.com/assets/country-reports/eu-tco/TERREG-Report-2025.pdf

Websites

Autoriteit Consument & Markt. (2025). Veel gebruikers onbekend met hun rechten op online platforms, ACM start voorlichtingscampagne. https://www.acm.nl/nl/publicaties/veel-gebruikers-onbekend-met-hun-rechten-op-online-platforms-acm-start-voorlichtingscampagne

Autoriteit online Terroristisch en Kinderpornografisch Materiaal. (g.d.). Meldpunt ATKM. https://www.atkm.nl/meldpunt-atkm

Europese Commissie. (2026). Counter-terrorism and radicalisation. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation_en?etransnolive=1

Europese Commissie. (2026). European Union Internet Forum. https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en

Europol. (n.d.). EU Internet Referral Unit - EU IRU. https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru

Offlimits. (g.d.). Meldpunt. https://meldpunt.offlimits.nl/

Overheid.nl. (2025). Consultatie Uitvoeringsbesluit TOI-verordening. https://www.internetconsultatie.nl/uitvoeringsbesluittoiverordening/b1

Bijlage II – Methodologie

In deze bijlage wordt de toegepaste methodologie stapsgewijs toegelicht. Er wordt ook stilgestaan bij afwegingen en beperkingen van onze methodologie. Allereerst worden de onderzoeksvragen gepresenteerd.

Onderzoeksvragen

De concrete onderzoeksvraag luidt:

'In hoeverre is de Uitvoeringswet TOI doeltreffend en hoe functioneert de wet, in het bijzonder voor wat betreft de toepassing en werking van de wet in de praktijk, de bestuurlijke constructie waarvoor is gekozen, alsook de balans tussen enerzijds de toepassing van de wet en anderzijds de rechtsstatelijke bescherming van aanbieders van hostingdiensten en internetplatformen en gebruikers van internetinhoud?'

Deze vraag valt uiteen in vijf thema's en subvragen:

1. Juiste toepassing en naleving van verwijderbevelen
   a. Op welke wijze identificeert de ATKM TOI materiaal?
   b. Hoe frequent worden verwijderbevelen uitgevaardigd? Zijn er hierbij trends te ontwaren?
   c. In welke mate geven hostingdiensten en internetplatformen daadwerkelijk en tijdig opvolging aan verwijderbevelen (inclusief de één-uursregel)?
   d. Wat zijn de ervaringen van hostingdiensten en internetplatformen met het proces rondom bevelen en rondom bezwaar- en beroepsprocedures?
   e. Wordt er in de praktijk gebruik gemaakt van bezwaar of beroep? Hoe vaak en met welk resultaat?
   f. Wordt er in de praktijk gebruik gemaakt van de mogelijkheid tot een blootstellingsbesluit en waarom wel of niet?
   g. Hoe wordt de mogelijkheid tot geschilbeslechting ervaren?

2. Juridische aspecten van verwijderbevelen
   a. In hoeverre valt de reikwijdte van verwijderbevelen binnen de kaders van de in Nederland beschermde grondrechten, met name de vrijheid van meningsuiting?
   b. Zijn er aanwijzingen van *chilling effects* of andere onbedoelde neveneffecten op toelaatbare online inhoud?
   c. Is het wenselijk dat de ATKM ook verwijderverzoeken kan uitvaardigen? Biedt het huidige wettelijke kader ruimte voor de ATKM om ook verwijderverzoeken te doen?
   d. Wordt de balans tussen effectiviteit en rechtsstatelijke bescherming in voldoende mate geborgd?

3. Capaciteit, uitvoerbaarheid en administratieve lasten
   a. Zijn de personele, juridische en technische middelen van de ATKM toereikend voor een effectieve uitvoering van haar taken en bevoegdheden?
   b. In hoeverre ervaren de ATKM of ketenpartners knelpunten in de capaciteit, uitvoerbaarheid of administratieve lasten (of anderszins) bij de Uitvoeringswet TOI?
   c. Wordt de uitvoerbaarheid van de verplichtingen als werkbaar ervaren door hostingdiensten en internetplatformen?

4. Governance en samenwerking
   a. Hoe werkt de keuze voor ATKM als zelfstandig bestuursorgaan door in een effectieve en efficiënte uitvoering van de TOI? In hoeverre zou de ATKM haar wettelijke taken en bevoegdheden (met name ten aanzien van internationale politiesamenwerking en toegang tot informatie) anders kunnen uitvoeren als ze een opsporingsinstantie zou zijn?
   d. Hoe functioneert de samenwerking tussen de ATKM en nationale actoren (zoals politie, Openbaar Ministerie, toezichthouders)?
   e. Hoe functioneert de samenwerking met de buitenlandse bevoegde autoriteiten onder de EU-verordening?
   f. Worden internationale verplichtingen en samenwerkingsstructuren effectief benut?
   g. Welke invloed heeft het samenvoegen van de TOI-taak met de kinderpornografisch materiaal-taak binnen de ATKM op de uitvoering van de TOI-taak door de ATKM?

5. Effectiviteit en impact op online veiligheid
   a. Heeft de Uitvoeringswet TOI bijgedragen aan een aantoonbare vermindering van de beschikbaarheid van terroristische online inhoud?
   b. Is het waarschijnlijk dat de Uitvoeringswet TOI heeft bijgedragen aan verbetering van de (online) veiligheid in het kader van nationale veiligheid en terrorismebestrijding?
   c. Zijn aanpassingen in de wetgeving of uitvoering aan te raden om de effectiviteit van de Uitvoeringswet TOI te verbeteren. Zo ja, welke aanpassingen?

De evaluatie is uitgevoerd in de periode van december 2025 tot en met juli 2026. De evaluatie omvat de periode vanaf de inwerkingtreding van de Uitvoeringswet TOI op 1 september 2023 tot en met juni 2026.

Methodologisch raamwerk

Om de onderzoeksvragen te beantwoorden, wordt gebruikgemaakt van een methodologisch raamwerk dat bestaat uit drie onderdelen: een interventielogica, een evaluatiematrix en een procesmatige uitwerking van de TOI cyclus.

De interventielogica (zie figuur 3) vormt het analytische vertrekpunt voor de evaluatie. In de interventielogica wordt inzichtelijk gemaakt welke problematiek de Uitvoeringswet TOI beoogt te adresseren, welke instrumenten daarvoor beschikbaar zijn, welke activiteiten en output hieruit voortvloeien en welke korte- en langetermijneffecten uiteindelijk worden nagestreefd. De interventielogica maakt daarmee inzichtelijk op welke aannames de wetgeving berust en via welke mechanismen de beoogde effecten tot stand zouden moeten komen. Dit biedt een

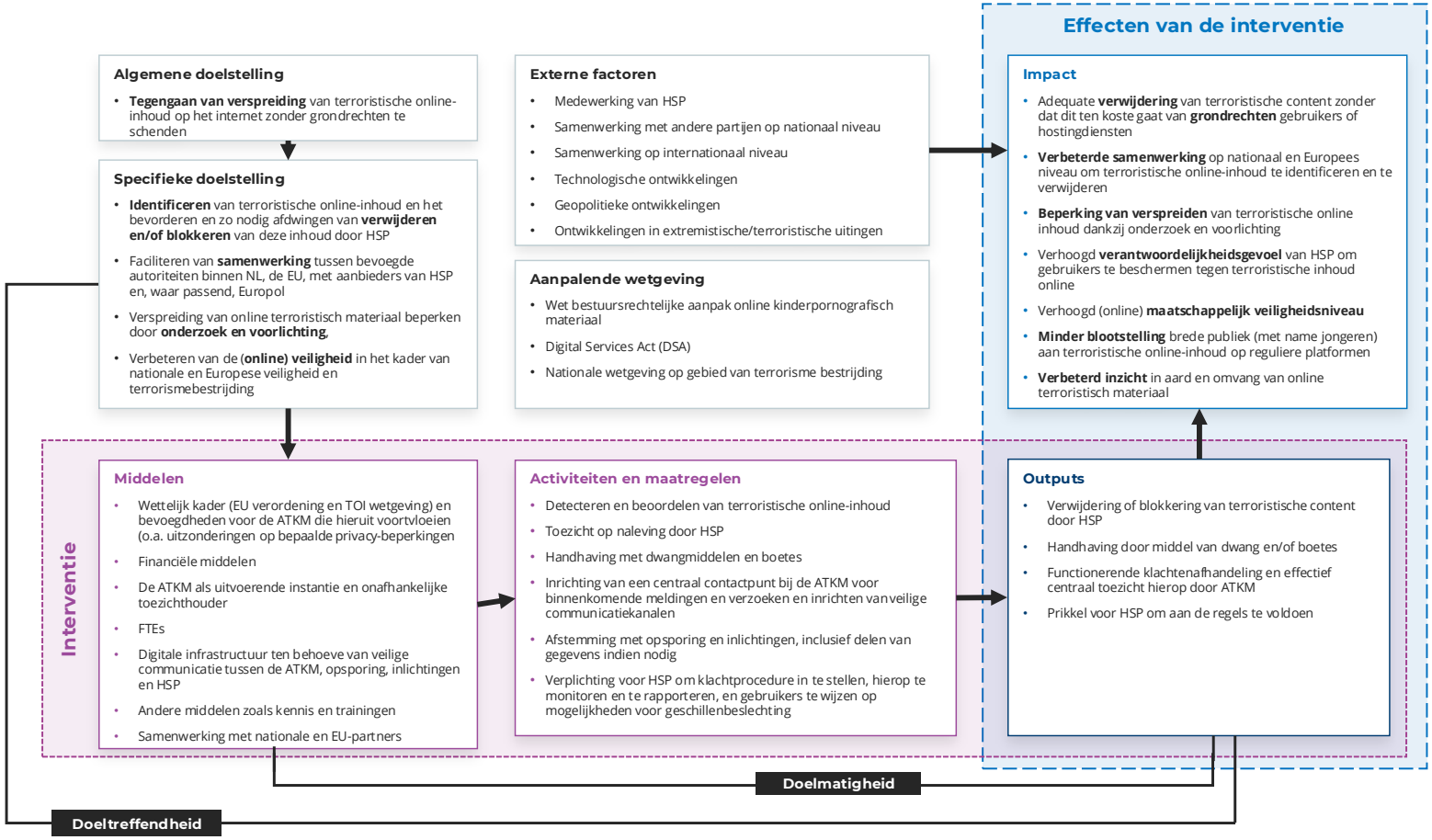
basis voor het beoordelen van zowel de doeltreffendheid van de wet als de werking ervan in de praktijk.

Op basis van deze interventielogica is vervolgens een evaluatiematrix opgesteld. In de evaluatiematrix zijn de onderzoeksvragen vertaald naar concrete beoordelingscriteria, indicatoren en informatiebronnen. De beoordelingscriteria geven weer welke aspecten centraal staan bij de beantwoording van de onderzoeksvragen. De indicatoren maken inzichtelijk welke signalen worden gebruikt om hierover uitspraken te doen, terwijl de informatiebronnen aangeven op welke empirische gegevens deze beoordeling is gebaseerd. De evaluatiematrix fungeert daarmee als verbindende schakel tussen de onderzoeksvragen, de dataverzameling en de uiteindelijke analyse.

Naast deze twee analytische instrumenten vormt de TOI-cyclus een belangrijke rode draad binnen het onderzoek. Deze beschrijft de opeenvolgende stappen die terroristische online inhoud doorloopt binnen het toepassingsbereik van de wet, vanaf het moment waarop dergelijke content wordt gesignaleerd tot en met de uitvoering van een verwijderbevel en eventuele bezwaar- en beroepsprocedures. Door de verschillende actoren, beslismomenten en processtappen systematisch in kaart te brengen, biedt de cyclus inzicht in de manier waarop de wetgeving in de praktijk functioneert. De cyclus is ontwikkeld en aangescherpt op basis van de rode draad sessie en is gedurende het onderzoek gebruikt als analytisch hulpmiddel om bevindingen te duiden, knelpunten te identificeren en mogelijke verbeterpunten in de uitvoering zichtbaar te maken.

Samen bieden de interventielogica, de evaluatiematrix en de cyclus een samenhangend analytisch kader voor het verzamelen, structureren en interpreteren van de onderzoeksbevindingen.

Figuur II.1 Interventielogica



Dataverzameling

Literatuur- en deskstudie

In de eerste fase van het onderzoek is een inventarisatie uitgevoerd om inzicht te verkrijgen in de juridische, beleidsmatige en uitvoeringscontext van de Uitvoeringswet TOI en de werking van de ATKM. De studie had ook tot doel relevante kennis over terroristische online inhoud te verzamelen ter voorbereiding op de rode draad sessie en de verdere empirische dataverzameling.

Voor de identificatie van relevante bronnen is gebruikgemaakt van een combinatie van gerichte zoekopdrachten in zoekmachines en openbare documentatiebronnen. Daarbij is gezocht op zowel Nederlandstalige als Engelstalige zoektermen, waaronder combinaties van termen als *terroristische online inhoud, terrorist content online, online extremisme, content moderatie, hosting service providers, terrorist content regulation, online platforms en online veiligheid*. Naast wetenschappelijke literatuur zijn ook beleidsdocumenten, wetsdocumentatie, jaarverslagen, transparantierapporten en andere vormen van grijze literatuur meegenomen.

De selectie van bronnen vond plaats op basis van relevantie voor de onderzoeksvragen. Daarbij is onderscheid gemaakt tussen:

- Documenten die direct betrekking hebben op de Uitvoeringswet TOI, de EU-verordening en de ATKM;
- Nationale en internationale literatuur over de verspreiding, moderatie en regulering van terroristische online inhoud;
- Literatuur over de rol van platforms, hostingdiensten en toezichthouders;
- Literatuur over fundamentele rechten en juridische vraagstukken rondom online inhoud moderatie.

Tijdens het onderzoek is de bronnenlijst iteratief verder ontwikkeld. De eerste inventarisatie vormde de basis voor de bespreking tijdens de rode draad sessie en de eerste bijeenkomst van de begeleidingscommissie. Op basis van de opbrengsten van deze bijeenkomsten is de bronnenlijst aangevuld en aangescherpt. Daarnaast zijn gedurende de looptijd van het onderzoek nieuw verschenen publicaties en beleidsdocumenten systematisch toegevoegd wanneer deze relevant waren voor de beantwoording van de onderzoeksvragen.

Voor de systematische analyse van de verzamelde documentatie is vervolgens een codeboek ontwikkeld. Dit codeboek helpt om documenten (en in een latere fase de interviewverslagen) op een transparante, consistente en reproduceerbare wijze te analyseren in Atlas.ti. De codering is gebaseerd op de onderzoeksvragen, het conceptueel kader en de thema's die voortkwamen uit de literatuur- en documentenstudie. Hierdoor konden bevindingen uit verschillende databronnen op een systematische wijze worden vergeleken en samengebracht.

De onderstaande documenten en bronnen maakten deel uit van de literatuur- en documentenstudie en zijn geanalyseerd in Atlas.ti. Een volledig overzicht van alle geraadpleegde bronnen is opgenomen in bijlage I.

- Uitvoeringswet TOI;
- EU-verordening;
- Stukken uit dossier Uitvoeringswet verordening terroristische online inhoud (36.138);
- Stukken uit de voorbereiding van de inrichting van de autoriteit bevoegd onder de Uitvoeringswet TOI;

- Stukken uit de voorbereiding van de inrichting van de EU-verordening;
- Jaarverslag(en) van de ATKM en andere stukken die de ATKM heeft gepubliceerd;
- Jaarverslagen en transparantierapporten van HSPs en bevoegde autoriteiten;
- Europose dreigingsbeelden;
- Nationale dreigingsbeelden NCTV van 2023, 2024, 2025, 2026;
- Stukken AIVD over online extremisme en radicalisering;
- Grijze literatuur zoals rapporten van EU Radicalisation Awareness Network (RAN) en EU Knowledge Hub on Prevention of Radicalisation;
- Grijze literatuur over fundamentele rechten met betrekking tot online inhoud moderatie;
- Wetenschappelijke literatuur zoals de haalbaarheidsstudie naar een duidingskader voor extremistische online inhoud van het ICCT en rechtsextremisme op sociale media van het Verwey Jonker Instituut.

Rode draad sessie

In januari 2026 is een rode draad sessie georganiseerd met verschillende betrokken partijen. Deze organisaties zijn geselecteerd omdat zij een centrale rol vervullen in de uitvoering, coördinatie en beleidsmatige inbedding van de Uitvoeringswet TOI. Een overzicht van de aanwezige partijen is te vinden in bijlage III.

Het doel van de sessie was om gezamenlijk de TOI-cyclus in kaart te brengen en daarmee inzicht te verkrijgen in de verschillende processtappen, betrokken actoren en mogelijke uitvoeringsvraagstukken. Tijdens de sessie is de uitvoering van de wetgeving stapsgewijs uitgetekend, vanaf het moment waarop terroristische content wordt geproduceerd en online wordt geplaatst tot en met eventuele bezwaar- en beroepsproces na het opleggen van een verwijderbevel of andere maatregel.

Als hulpmiddel zijn twee fictieve casussen gebruikt. De eerste casus betrof een voorbeeld van duidelijke TOI, waarbij er beperkte discussie bestond over de kwalificatie van de content. De tweede casus had betrekking op zogenoemde borderline content, waarbij juist ruimte bestond voor interpretatie en afweging ten aanzien van de toepasselijkheid van de wettelijke criteria. Door beide casussen stap voor stap langs de verschillende fasen van het proces te volgen, konden niet alleen de formele werkprocessen worden gereconstrueerd, maar ook voorlopige knelpunten, interpretatievraagstukken en verschillen in perspectief tussen betrokken partijen worden geïdentificeerd.

De opbrengsten van de rode draad sessie zijn gebruikt om de conceptuele uitwerking van de TOI-cyclus verder aan te scherpen. De uiteindelijke cyclus (zie ook paragraaf 2.2) vormde vervolgens een analytisch hulpmiddel voor de verdere dataverzameling, de ontwikkeling van interviewleidraden en de beantwoording van de evaluatievragen gedurende het onderzoek.

Semigestructureerde interviews

De semigestructureerde interviews vormden een belangrijke bron voor het beantwoorden van de onderzoeksvragen. De interviews hadden drie doelen. Ten eerste werden zij ingezet om bevindingen uit de literatuur- en documentenstudie te valideren en aan te vullen. Ten tweede boden zij inzicht in de wijze waarop de Uitvoeringswet TOI in de praktijk wordt toegepast door verschillende betrokken partijen. Ten derde maakten de interviews het mogelijk om ervaringen, knelpunten en verbetermogelijkheden met betrekking tot de uitvoering en

effectiviteit van de wet in kaart te brengen. De interviews waren opgebouwd rond de hoofdthema's uit het onderzoek.

Voor de uitvoering van het onderzoek zijn in totaal 28 interviews gehouden met een brede groep partijen die vanuit verschillende perspectieven betrokken zijn bij de uitvoering, toepassing of context van de Uitvoeringswet TOI. Bijlage III geeft een overzicht van de respondenten.

Eerst was voorzien om drie expertmeetings te organiseren, waarin verschillende externe deskundigen gezamenlijk zouden reflecteren op voorlopige bevindingen uit het onderzoek. Vanwege agenda-technische beperkingen bleek het niet mogelijk om voldoende experts op hetzelfde moment bijeen te brengen. Daarom is ervoor gekozen om afzonderlijke interviews te houden met relevante experts. Deze aanpak bood bovendien de mogelijkheid om dieper in te gaan op specifieke expertisegebieden en om gevoelige of specialistische onderwerpen uitgebreider te bespreken dan in een groepssetting mogelijk zou zijn geweest. De respondenten die geïnterviewd zijn, staan ook in bijlage III.

De gesprekken zijn gehouden aan de hand van interviewleidraden. Deze zijn toegespitst op de belangrijkste respondentgroepen: de ATKM, overheidsorganisaties, aanbieders van hostingdiensten en academici. De leidraden zijn gebaseerd op de onderzoeksvragen, de resultaten van de literatuur- en documentenstudie en de inzichten die voortkwamen uit de rode draad sessie. Hoewel voor iedere respondentgroep een vaste thematische structuur werd gehanteerd, bood de semigestructureerde opzet ruimte om door te vragen naar onderwerpen die specifiek relevant waren voor de kennis, ervaring of rol van de betreffende respondent.

De interviews zijn vervolgens uitgewerkt en, samen met de bevindingen uit de literatuur- en documentenstudie, gecodeerd en geanalyseerd in Atlas.ti. Door deze systematische analysemethode konden bevindingen uit verschillende bronnen worden vergeleken en, waar mogelijk, triangulatie plaatsvinden tussen documenten, interviews en overige onderzoeksonderdelen.

Case studies

Als aanvulling op de Nederlandse analyse zijn drie internationale case studies uitgevoerd. Het doel van deze case studies was om de Nederlandse uitvoeringspraktijk in internationaal perspectief te plaatsen en inzicht te verkrijgen in de wijze waarop andere lidstaten invulling geven aan de EU-verordening inzake terroristische online inhoud. De case studies dienden in het bijzonder om inzicht te verschaffen in verschillen in institutionele inrichting, gebruik van het instrumentarium en ervaringen met de uitvoering van de EU-verordening.

De selectie van de lidstaten vond plaats op basis van hun relevantie voor de onderzoeksvragen en de beschikbaarheid van gegevens en gesprekspartners. Gedurende het onderzoek is de oorspronkelijke selectie aangepast. In eerste instantie werd gekozen voor Duitsland, Spanje en Frankrijk. Omdat het niet lukte om respons te krijgen van de laatste twee lidstaten, is besloten om twee andere lidstaten te selecteren. Uiteindelijk zijn de case studies uitgevoerd voor Duitsland, Ierland en Zweden. De geselecteerde lidstaten vertegenwoordigen verschillende uitvoeringsmodellen en bieden daarmee inzicht in variaties in toezicht, handhaving en samenwerking met online platforms:

- In Duitsland zijn zowel de Bundeskriminalamt en de Bundesnetzagentur aangewezen als bevoegde autoriteit. De Bundeskriminalamt heeft opsporingsbevoegdheden en vormt daarmee de evenknie van de bestuurlijke ‘agentur’. Daarnaast is Duitsland actief betrokken in de uitvoering van de EU-verordening op nationaal niveau.
- Ierland is gekozen vanwege de centrale rol van de Coimisiún na Meán als bevoegde autoriteit en de aanwezigheid van verschillende grote online platforms binnen de Ierse jurisdictie.
- Zweden is geselecteerd vanwege de actieve betrokkenheid van de Zweedse autoriteiten bij de Europese uitvoering van de verordening en de samenwerking met andere lidstaten op dit gebied.

De case studies zijn uitgevoerd op basis van een combinatie van documentanalyse en vier interviews met vertegenwoordigers van bevoegde autoriteiten en andere relevante stakeholders in de betreffende lidstaten. De bevindingen uit de case studies zijn gebruikt ter contextualisering van de Nederlandse situatie en zijn verwerkt in de relevante hoofdstukken van het rapport.

Validatiesessie

Na afronding van de analysefase zijn de voorlopige bevindingen besproken tijdens een validatiesessie met vertegenwoordigers van organisaties die betrokken zijn bij de uitvoering van de Uitvoeringswet TOI. Het doel van deze sessie was om de feitelijke juistheid van de bevindingen te toetsen, eventuele omissies te identificeren en te verifiëren of de onderzoeksresultaten herkenbaar waren voor de betrokken partijen.

Aan de validatiesessie namen dezelfde betrokken partijen deel. Tijdens de bijeenkomst zijn de voorlopige bevindingen per onderzoeksvraag gepresenteerd en besproken. De deelnemers kregen gelegenheid om feitelijke onjuistheden te corrigeren, aanvullende context te bieden en te reflecteren op de interpretatie van de resultaten.

De validatiesessie had nadrukkelijk geen besluitvormend karakter en diende niet om conclusies aan te passen op basis van voorkeuren of belangen van betrokken partijen. De sessie werd ingezet als instrument voor kwaliteitsborging en voor het toetsen van de herkenbaarheid en plausibiliteit van de bevindingen. Waar relevant zijn opmerkingen uit de validatiesessie verwerkt in de definitieve analyse en rapportage.

Bijlage III – Respondentenoverzicht

Figuur 4.1 Overzicht van de respondenten

Organisatie	Positie	Rode draad sessie	Interview	Validatieworkshop
ATKM	Bestuur	✓	✓	✓
	Operationele werknemers		✓	
	Juridische werknemers		✓	
Ministerie van Justitie en Veiligheid	Beleidsadviseur		✓	
	Taakveldcoördinator	✓	✓	✓
	Eigenaarsadviseur	✓	✓	✓
	Nationaal coördinator		✓	
Ministerie van Economische Zaken en Klimaat	Beleidsadviseur		✓	
Opsporingsdienst	Politie – eenheid landelijke opsporing en interventies strategisch		✓	✓
	Politie – eenheid landelijke opsporing en interventies operationeel		✓	✓
	PERCI platform manager		✓	✓
Bevoegde autoriteiten andere lidstaten	Teamleiders bevoegde autoriteiten Duitsland		✓	✓
	Directeuren bevoegde autoriteit Ierland		✓	✓
	Teamleider bevoegde autoriteit Zweden		✓	✓
Hosting Service Providers	Beleid & compliance team Discord		✓	✓
	Publiek beleidsadviseur Snapchat		✓	
Academici	Expert schadelijke content online		✓	
	Expert terroristische propaganda online		✓	
	Expert dreigingen in de democratie in het online domein		✓	
	Expert online terrorisme en extremisme		✓	
	Expert terrorisme		✓	
Maatschappelijk middenveld	Beleidsadviseur College van de Rechten van de Mens		✓	
	Adviseur brancheverenigingen		✓	
	Teamleider Stichting Offlimits		✓	

Postbus 4175
3006 AD Rotterdam
Nederland

Watermanweg 44
3067 GG Rotterdam
Nederland

T 010 453 88 00
E netherlands@ecorys.com

K.v.K. nr. 24316726

W www.ecorys.nl