Over de grens

Lessen uit buitenlandse aanpakken van online aangejaagde ordeverstoringen

EINDRAPPORT

WODC
Hans Moors, Marnix Eysink Smeets en Lidwien van de Wijngaert

8 juli 2026

E:M+MA.

Inhoudsopgave

Samenvatting

Over de grens. Lessen uit buitenlandse aanpakken van online aangejaagde ordeverstoringen

Openbare ordeverstoringen spelen zich af in een omgeving waarin sociale media een belangrijke rol spelen. Via sociale media kunnen (des)informatie, geruchten en oproepen zich snel verspreiden. Voor overheden roept dit de vraag op hoe zij met (dreigende) verstoringen van de openbare orde moeten omgaan, zonder fundamentele rechten zoals de vrijheid van meningsuiting en het demonstratierecht uit het oog te verliezen. Dit onderzoek verkent hoe een selectie van Europese landen omgaat met verstoringen van de openbare orde waarin sociale media een rol spelen en welke lessen daaruit voor Nederland kunnen worden afgeleid.

Om dit te kunnen doen, is het nodig eerst stil te staan bij de relatie tussen online dynamiek en openbare-ordeverstoringen. Online aangejaagde openbare ordeverstoringen (OAOV) staan de laatste jaren in de belangstelling van politie, bestuur en politiek. Deze verstoringen van de openbare orde doen zich in uiteenlopende vormen voor en incidenten verschillen in aanleiding, dynamiek, organisatiegraad en verloop. Het kan bijvoorbeeld gaan om demonstraties die via sociale media worden georganiseerd en uitlopen op rellen, spontane samenkomsten die online snel grote groepen mensen trekken, of situaties waarin geruchten en online onrust bijdragen aan paniek, spanningen of escalatie in de publieke ruimte.

Ook de rol van online communicatie varieert per situatie. Sociale media en andere online platforms worden gebruikt om mensen te mobiliseren, (des)informatie te verspreiden, gebeurtenissen te duiden en spanningen te versterken. De aard en betekenis van die online communicatie verschilt sterk per situatie. Online communicatie kan bijdragen aan vreedzame bijeenkomsten en vormen van maatschappelijke participatie, maar ook aan het ontstaan, de versnelling of de escalatie van ordeverstoringen.

Deze variatie maakt het in de praktijk niet eenvoudig om vast te stellen wanneer online signalen wijzen op een reëel risico op openbare-ordeverstoring en wanneer optreden noodzakelijk of proportioneel is. Demonstraties, maatschappelijke onrust en scherpe (online) uitingen vallen immers binnen de grenzen van vrijheid van meningsuiting. Tegelijkertijd kunnen situaties ontstaan waarin spanningen escaleren, de openbare orde daadwerkelijk wordt verstoord of strafbare feiten dreigen of plaatsvinden. Juist in dat spanningsveld moeten bestuur, politie en andere betrokken partijen afwegen welke vormen van optreden passend zijn en hoe grondrechten daarbij kunnen worden gewaarborgd.

Doel van het onderzoek

Overheden in binnen- en buitenland zoeken naar manieren om openbare-ordeverstoringen waarin online communicatie een rol speelt bijtijds te signaleren, te voorkomen, of te beheersen. Daarbij

worden in verschillende landen uiteenlopende keuzes gemaakt in bevoegdheden, samenwerking, toezicht en handhaving. Dit onderzoek verkent hoe andere landen omgaan met openbare-ordeverstoringen waarin online communicatie een rol speelt en welke lessen daaruit kunnen worden geleerd voor de Nederlandse context.

Hiervoor zijn de volgende deelvragen geformuleerd:

1. Hoe manifesteren online aangejaagde openbare-ordeverstoringen zich in de praktijk?
2. Welke (typen) aanpakken hanteren verschillende Europese landen om OAOV te signaleren, te voorkomen en te beheersen, en hoe functioneren deze in de praktijk?
3. Welke elementen uit de onderzochte buitenlandse aanpakken zijn relevant voor de Nederlandse context?

Om antwoord te geven op deze vragen is eerst een verkenning uitgevoerd van incidenten in verschillende Europese landen. Vervolgens is op basis van documentanalyse geïnventariseerd welke bestuurlijke, juridische en operationele aanpakken daarbij werden toegepast. Deze inventarisatie vormde de basis voor de selectie van een aantal landen en aanpakken die vervolgens verdiepend zijn onderzocht aan de hand van aanvullende documentanalyse, casuïstiek en (online) interviews met experts en beleidsmakers. De bevindingen uit de verschillende landen zijn vervolgens vergelijkend geanalyseerd en samengebracht in een aantal lessen voor de Nederlandse context. Deze lessen zijn besproken en getoetst in een reflectiesessie met Nederlandse experts.

Typen incidenten

Het onderzoek laat zien dat online aangejaagde openbare ordeverstoringen een veelzijdig fenomeen vormen. De onderzochte incidenten verschillen langs drie samenhangende dimensies:

- Ten eerste verschillen zij in hun aanleiding: het kan gaan om ideologisch gedreven protesten, door desinformatie of geruchten aangejaagde mobilisaties, influencer- of hypegedreven samenkomsten, groeps- en aan rivaliteit gerelateerde incidenten of situaties waarin online communicatie paniek of massaal gedrag versterkt.
- Ten tweede verschilt de rol van online communicatie. Online communicatie kan dienen voor het organiseren en mobiliseren van deelnemers, voor informatievoorziening en beeldvorming, voor coördinatie tijdens een incident of voor het versterken van emoties, spanningen en escalatie.
- Ten derde verschillen incidenten in hun dynamiek: zij variëren in organisatiegraad, snelheid van mobilisatie, de wisselwerking tussen online en offline ontwikkelingen en de mate waarin gebeurtenissen zich ontwikkelen tot een openbare-ordeverstoring.

Deze dimensies staan niet los van elkaar, maar komen in de praktijk in uiteenlopende combinaties voor. Daardoor bestaat er geen eenduidig type OAOV. De aard van het incident, de rol van online communicatie en het verloop van de dynamiek bepalen gezamenlijk welke risico's ontstaan en welke vormen van duiding en optreden passend zijn.

Typen aanpakken van OAOV

De variatie in openbare-ordeverstoringen en in de rol van sociale media daarin werkt door in de manier waarop overheden, politie, toezichthouders en maatschappelijke partijen met dergelijke situaties omgaan. In de praktijk zetten landen uiteenlopende vormen van handhaving, monitoring, samenwerking, regulering en preventie in.

Hoewel de aangetroffen aanpakken sterk verschillen, zijn er ook overeenkomsten zichtbaar. Op basis van een analyse van een groot aantal aanpakken in verschillende landen onderscheiden we vier clusters die helpen om de verschillende aanpakken te beschrijven.

Cluster 1. Preventieve en maatschappelijke aanpakken
Deze aanpakken richten zich op het voorkomen van escalatie door versterking van weerbaarheid en focus op maatschappelijke dynamiek. Ze grijpen vroeg in en werken via netwerken van publieke en maatschappelijke actoren. Deze aanpakken zijn afhankelijk zijn van samenwerking, vertrouwen en institutionele inbedding. Het effect is indirect en moeilijk meetbaar.

Cluster 2. Regulerende en toezichthoudende aanpakken
Deze aanpakken richten zich op het stellen en handhaven van regels voor de online omgeving, met name voor platforms. Ze werken vooral randvoorwaardelijk door de online context te beïnvloeden waarin mobilisatie kan plaatsvinden. In verschillende landen spelen toezichthouders een steeds grotere rol bij het reguleren van online content, de providers en de platforms. Deze aanpakken worden ook steeds meer gekaderd in Europese wetgeving.

Cluster 3. Informatie- en intelligencegerichte aanpakken
Deze aanpakken richten zich op het verkrijgen en duiden van informatie over online dynamiek, vaak vlak vóór of tijdens escalatie. Ze vormen in de praktijk een cruciale schakel: ze maken het mogelijk om patronen te herkennen, dreigingen te duiden en gericht te handelen.

Cluster 4. Handhavings- en repressieve aanpakken
Deze aanpakken richten zich op het direct ingrijpen en sanctioneren van strafbaar gedrag. Ze zijn het meest zichtbaar en concreet, maar ook sterk afhankelijk van timing, bewijspositie en maatschappelijke acceptatie. In de landenstudies blijkt dat zij noodzakelijk zijn voor normhandhaving, maar op zichzelf onvoldoende om onderliggende dynamiek te beïnvloeden.

Buitenlandse aanpakken

Op basis van de inventarisatie van aanpakken is een selectie gemaakt van landen en aanpakken die relevant kunnen zijn voor de Nederlandse context. De geselecteerde landen en aanpakken verschillen onder meer in de rol van de overheid, de inzet van toezicht en handhaving en de manier waarop veiligheid en grondrechten tegen elkaar worden afgewogen.

Zweden: Psychological Defence Agency

De Zweedse aanpak die we hebben onderzocht is een preventieve aanpak waarin maatschappelijke weerbaarheid centraal staat. Binnen een breed stelsel voor crisisbeheersing en veiligheid speelt de *Swedish Psychological Defence Agency* (MPF) een belangrijke rol. Deze organisatie monitort en analyseert desinformatie en buitenlandse beïnvloeding, ontwikkelt kennis, ondersteunt publiekscommunicatie en werkt samen met maatschappelijke partners. De nadruk ligt niet op individuele online uitingen, maar op het versterken van de weerbaarheid van de samenleving en het begrijpen van de bredere informatieomgeving. Daarmee laat Zweden zien hoe preventie, kennisontwikkeling en samenwerking kunnen bijdragen aan het voorkomen van online aangejaagde openbare-ordeverstoringen. De effectiviteit van de MPF voor het daadwerkelijk voorkomen van OAOV is niet vastgesteld, maar de aanpak biedt wel een interessant voorbeeld van hoe weerbaarheid tegen desinformatie institutioneel kan worden vormgegeven.

Verenigd Koninkrijk: NSOIT en Prevent Duty Guidance

Voor het Verenigd Koninkrijk hebben we twee aanpakken onderzocht die vroegsignalering centraal stellen. Het *National Security Online Information Team* (NSOIT) monitort online informatie om snel zicht te krijgen op narratieven, desinformatie en andere online ontwikkelingen die kunnen bijdragen aan maatschappelijke onrust of veiligheidsrisico's. De *Prevent Duty Guidance* verplicht publieke organisaties, zoals scholen, universiteiten en zorginstellingen, om signalen van radicalisering vroegtijdig te herkennen en waar nodig door te geleiden. Beide aanpakken laten zien hoe vroegsignalering kan bijdragen aan het voorkomen van escalatie, zowel via de online informatieomgeving als via maatschappelijke organisaties. Tegelijkertijd wordt duidelijk dat dergelijke preventieve instrumenten alleen houdbaar zijn wanneer zij beschikken over een helder mandaat, transparantie, toezicht en voldoende rechtsstatelijke waarborgen. De effectiviteit van beide aanpakken is bovendien lastig vast te stellen en onderwerp van maatschappelijk en wetenschappelijk debat.

Ierland: Coimisiún na Meán

In Ierland richt de *Coimisiún na Meán* zich op toezicht op online platforms en digitale diensten. De toezichthouder combineert mediatoezicht met online-platformregulering en werkt via de Online Safety Code, DSA-toezicht en de Terrorist Content Online Regulation. De nadruk ligt op platformprocessen, moderatiesystemen, meldmechanismen en ontwerpmaatregelen. Deze aanpak verlegt de aandacht van incidentgerichte handhaving naar structurele verantwoordelijkheden van platforms voor het beperken van online risico's. Coimisiún na Meán is daarbij toezichthouder en normsteller, geen opsporingsinstantie. De relevantie voor voor Nederland is dat platformtoezicht een aanvulling kan vormen op klassieke openbare-ordehandhaving en strafrecht. De aanpak is nog in opbouw en duidelijke evaluaties ontbreken vooralsnog.

Frankrijk: VIGINUM en Pharos

Frankrijk verbindt de aanpak van OAOV met nationale veiligheid, desinformatie en buitenlandse beïnvloeding. Binnen deze bredere benadering illustreren de twee onderzochte aanpakken hoe wordt ingezet op zowel strategische informatievergaring als operationele opvolging. *VIGINUM* analyseert buitenlandse beïnvloedingscampagnes en bredere informatiepatronen die maatschappelijke onrust of mobilisatie kunnen versterken, terwijl *Pharos* meldingen van onder meer online haat, opruiing en andere strafbare content verzamelt, beoordeelt en doorgeleidt naar politie en justitie. Samen laten deze aanpakken zien hoe een sterke informatiepositie kan worden opgebouwd door strategische analyse te verbinden met opsporing en vervolging. Tegelijkertijd roepen beide voorzieningen vragen op over transparantie, capaciteit en publieke verantwoording. Ook voor deze aanpakken ontbreken publiek beschikbare evaluaties, waardoor onduidelijk blijft in

hoeverre deze aanpakken daadwerkelijk bijdragen aan het voorkomen of beperken van openbare-ordeverstoringen.

Duitsland: KI4Demokratie en Landelijke actiedagen tegen strafbare haat-posts
Duitsland beschikt over een breed palet aan maatregelen waarin strafrechtelijke handhaving, toezicht en monitoring van online extremisme samenkomen binnen een sterk rechtsstatelijk en federaal georganiseerd stelsel. De twee onderzochte aanpakken illustreren deze benadering. *KI4Demokratie* laat zien hoe AI kan worden ingezet om online narratieven en netwerken vroegtijdig te analyseren en te duiden, terwijl de *Landelijke actiedagen tegen strafbare haatposts* laten zien hoe dergelijke signalen kunnen worden verbonden aan zichtbaar strafrechtelijk optreden. Samen illustreren deze aanpakken het belang van een sterke informatiepositie in combinatie met normstellende handhaving. Tegelijkertijd laten zij zien dat zowel de analyse van grote hoeveelheden online data als de stap naar proportioneel optreden complex blijft. Ook voor deze aanpakken ontbreken publieke evaluaties van de structurele effecten.

Overkoepelende bevindingen

OAOV wordt in geen van de onderzochte landen gezien als een puur digitaal probleem. Online dynamiek staat altijd in wisselwerking gebeurtenissen in de fysieke wereld. Bovendien laten de onderzochte incidenten zien dat OAOV vele verschijningsvormen kent. Ze verschillen in aanleiding, mobilisatie, verloop en impact. Juist deze diversiteit maakt dat landen niet kiezen voor één dominante interventie, maar voor combinaties van verschillende aanpakken. De onderzochte aanpakken richten zich op verschillende onderdelen van het vraagstuk, variërend van preventie en weerbaarheid tot monitoring, analyse en handhaving. De landenvoorbeelden illustreren verschillende onderdelen van zo'n gelaagde aanpak.

Bij de analyse van de onderzochte aanpakken viel op dat de kennis over de effectiviteit van aanpakken beperkt is. Dat is deels inherent aan het feit dat het bij preventieve en systeemgerichte interventies vaak moeilijk is vast te stellen in hoeverre uitblijvende ordeverstoringen daadwerkelijk aan een specifieke maatregel kunnen worden toegeschreven. Daarnaast echter ontbreken voor veel aanpakken publiek beschikbare evaluaties. Daardoor blijft onduidelijk in welke mate de aanpakken bijdragen aan het voorkomen of beperken van ordeverstoringen.

Verder bieden de resultaten van het onderzoek weinig aanleiding om te veronderstellen dat verdergaande repressieve bevoegdheden of intensievere monitoring op zichzelf een oplossing vormen voor OAOV. Repressieve maatregelen die ingrijpen in grondrechten roepen vragen op over legitimiteit en kunnen onder omstandigheden bijdragen aan escalaties. Voor monitoring geldt dat zonder een helder mandaat, adequate waarborgen, transparantie en democratische controle zorgen ontstaan over proportionaliteit, *mission creep* en de bescherming van fundamentele rechten.

We concluderen dat geen enkele afzonderlijke aanpak een *silver bullet* is. De meest kansrijke koers is een zorgvuldig uitgebalanceerde combinatie van weerbaarheid, regulering, samenwerking, intelligence en begrensde repressie.

Lessen

Op basis van de bevindingen uit de landenstudies zijn acht lessen voor Nederland geformuleerd. Deze lessen zijn besproken en aangescherpt in een expertsessie met deskundigen uit wetenschap, beleid en praktijk op het terrein van openbare orde en veiligheid, digitalisering, online gedrag, platformregulering, grondrechten, strafrecht en lokaal bestuur. Gezamenlijk wijzen deze lessen op het belang van een gelaagde aanpak. De uitdaging is niet het ontwikkelen van nieuwe

bevoegdheden, maar het versterken van het vermogen om bestaande instrumenten in samenhang, proportioneel en lerend in te zetten.

Les 1. Online is onderdeel van openbare orde

Online communicatie speelt een rol bij openbare-ordeverstoringen, niet als afzonderlijk domein maar als onderdeel van de dynamiek tussen on- en offline. De relevante vraag is daarom niet óf online communicatie een rol speelt, maar hoe die rol eruitziet en welke gevolgen dat heeft voor het verloop van een incident.

Les 2. Stem de aanpak af op het type incident

Openbare-ordeverstoringen verschillen sterk in aanleiding, mobilisatie, snelheid van escalatie en betrokken netwerken. Effectief optreden vraagt daarom om een goede afstemming tussen het type incident en de gekozen combinatie van interventies, zowel voorafgaand aan als na afloop van een incident.

Les 3. Zorg voor een breed repertoire aan aanpakken

Het onderzoek laat zien dat geen enkele aanpak op zichzelf voldoende is. Effectief beleid op het gebied van OAOV vraagt om een samenhangend repertoire van preventie, regulering, informatievergaring, samenwerking en handhaving, waarbij per situatie de juiste combinatie wordt gekozen.

Les 4. Grondrechten zijn het uitgangspunt

De bescherming van fundamentele rechten, zoals vrijheid van meningsuiting en demonstratievrijheid, vormt het vertrekpunt van overheidsoptreden. De landenstudies laten zien dat zowel monitoring als repressie zorgvuldig moeten worden afgewogen vanwege hun mogelijke effecten op vertrouwen, legitimiteit en gedrag.

Les 5. Ontwikkel en evalueer preventieve aanpakken

Veel landen investeren in weerbaarheid, mediageletterdheid, lokale netwerken en andere vormen van preventie. Tegelijkertijd is nog weinig bekend over de effectiviteit van dergelijke interventies, waardoor systematische monitoring en evaluatie noodzakelijk zijn.

Les 6. Werk structureel samen

Omdat online aangejaagde openbare-ordeverstoringen verschillende domeinen raken, beschikken afzonderlijke organisaties nooit over het volledige beeld. Structurele samenwerking tussen overheid, politie, justitie, maatschappelijke organisaties, platforms en andere partijen is daarom essentieel voor signalering, duiding en optreden.

Les 7. Reguleer platforms en spreek hen aan op hun verantwoordelijkheid

Platforms beïnvloeden actief hoe informatie zich verspreidt en hoe mobilisatie plaatsvindt. De onderzochte landen laten zien dat toezicht, regelgeving en samenwerking met platforms een steeds belangrijkere aanvulling vormen op traditionele instrumenten van openbare orde en veiligheid.

Les 8. Creëer een lerende praktijk

Over de werking en effectiviteit van veel aanpakken is nog relatief weinig bekend. Een duurzame aanpak vraagt daarom om continue kennisontwikkeling, evaluatie en bijstelling van beleid, zodat ervaringen uit incidenten systematisch kunnen worden benut. Nederland kan hierin een voortrekkersrol vervullen.

1 Inleiding

Nieuw is het niet: de online aangejaagde openbare ordeverstoring (OAOV). In 1997 sprak de harde kern van Ajax en Feijenoord via sms af om te gaan vechten. De 'Slag bij Beverwijk' had één dode tot gevolg. De 'vechtafspraken' bleken een blijvertje (Wolsink & Ferwerda, 2022), tegenwoordig niet alleen in bos of weiland, maar ook in uitgaansgebieden, zoals op de Scheveningse boulevard rond het Kurhaus op 1 mei 2025. Honderden jongeren komen af op een oproep via sociale media, gaan met elkaar op de vuist en keren zich daarna tegen de politie. In Zandvoort gebeurt in het Pinksterweekend van 2026 iets soortgelijks op kleinere schaal. Jongeren worden via sociale media opgeroepen om snel te verzamelen op verschillende plekken, aan de boulevard of op het strand, waar gewelddadige opstootjes ontstaan.

Een ander fenomeen is het online delen van oproepen tot deelname aan illegale feesten. Project X Haren (2012) is het bekendste voorbeeld (Commissie Project X Haren, 2013). Dat er korte tijd later vergelijkbare facebook-oproepen verschijnen om te komen feesten in Enschede, Arnhem en Katwijk is in de vergetelheid geraakt. Illegale raves, zoals in maart 2026 in Willemstad, vallen vaak ook in deze categorie. Een grote hoeveelheid feestgangers komt in heel korte tijd opdagen waarna de politie op last van de burgemeester het feest beëindigt.

Tijdens de COVID-pandemie was er sprake van online aangejaagde ordeverstoringen rond demonstraties en protesten tegen de maatregelen die de overheid neemt om de pandemie te bestrijden. Ook de vreedzame en ontregelende blokkades en bezettingen door Extinction Rebellion sinds 2022 zijn tegen overheidsbeleid gericht, online gemobiliseerd en voorzien van een uitgekiende media- en woordvoeringsstrategie. Beide typen protest brengen burgemeesters in een lastig parket, omdat die de demonstraties moesten laten doorgaan, maar tegelijkertijd de verstoring van de openbare orde moesten zien te voorkomen of beperken. Eerder al was dit dilemma scherp zichtbaar geworden tijdens de talrijke acties tegen Kick out Zwarte Piet (KOZP). Met als dieptepunten de gebeurtenissen rond de Sinterklaasintochten in Dokkum (18 november 2017) en Staphorst (19 november 2022).

Soms is de aanleiding niet zo prominent. De hete zomer en de kick om handhaving en politie te tarten (tegen de achtergrond van de beperkingen die de pandemie met zich meebracht) veroorzaken groots straatrumoer tijdens de 'Zomerrellen' in Den Haag en Utrecht (augustus 2020). Van nog groter kaliber zijn de plots opvlammende gewelddadige ongeregeldheden in Rotterdam – de burgemeester noemde het een 'orgie van geweld' – na een kleine demonstratie op 17 november 2021 tegen het 2G-beleid van de regering (Moors et al., 2020; Moors, 2023). Het afkondigen van een iconische maatregel als de avondklok (om de verspreiding van de pandemie te beperken) vormt de aanleiding voor onverwacht grimmig verzet. Tijdens de Avondklokrellen van januari 2021 komt het in de binnensteden van Eindhoven, 's-Hertogenbosch, Utrecht en wat later ook op de Rotterdamse Coolsingel tot grootschalige ongeregeldheden, geweldpleging en vernielingen. Sociale media en online platforms, zoals Facebook, Instagram en Telegram, hebben vooraf en tijdens een enorme impact op het bijeenbrengen en informeren van grote, diverse en diffuse groepen mensen (Moors et al., 2022; Moors, 2023).

In dezelfde lijn liggen de protesten tegen het asiel- en migratiebeleid, gelardeerd met anti-overheidsframes en radicaal-rechts gedachtegoed. Tijdens de vluchtelingencrisis van 2015 en 2016 liepen protesten in onder meer Geldermalsen, Heesch en Enschede uit op ernstige ordeverstoringen. Destijds stonden vooral lokale besluitvorming over nieuwe opvanglocaties en bewonersprotesten centraal. In 2025 en 2026 hebben protesten rondom asiel en migratie, die tot ordeverstoringen leiden, een ander karakter gekregen. Landelijke en lokale protesten tegen de opvang van asielzoekers worden steeds vaker onderdeel van brede online netwerken waarin activisten (met uiteenlopende overtuigingen en motieven), hooligangroepen, Defend-formaties en politieke actoren elkaar vinden. Terwijl dit onderzoek werd uitgevoerd[1], waren zulke protesten aan de orde van de dag. In Berlicum en Uden, bijvoorbeeld, of in Didam, Houten en Amersfoort (in 2025), later ook in IJsselstein, Den Bosch, Apeldoorn, Uithoorn en Wijk bij Duurstede (in 2026). Online en in de media zijn deze protesten zeer zichtbaar.

Veel aandacht krijgt bijvoorbeeld de oproep via instagramgroepen, hooligancollectieven en rechtse onlinekanalen om op 20 september 2025 naar het Malieveld in Den Haag te komen. Deze demonstratie ('Elsfest-demo') loopt gruwelijk uit de hand. De snelweg wordt geblokkeerd, er wordt geweld gepleegd tegen politie en journalisten, brandgesticht, met veel vernielingen en schade als gevolg. Bij het partijkantoor van D66 worden ruiten ingegooid. Een ander voorbeeld is het anti-AZC protest in Loosdrecht (gemeente Wijdemeren). Sinds half april 2026 zijn inwoners in verzet tegen een tijdelijke opvanglocatie. Defend-groepen en diffuse gelegenheidsformaties doen mee, net als op het Malieveld en bij vrijwel alle grootschalige demonstraties tegen de vestiging van opvanglocaties sinds september 2025. Leden van de Tweede Kamer geven *acte de présence* op locatie. Er zijn vlaggenparades, rechtszaken, rellen, vernielingen, vuurwerk en brandjes. Demonstranten zingen kwetsende, AI-gegenereerde liederen over handhavers en gezagsdragers. Professionals worden bedreigd. Er komt een zelfbenoemde burgerwacht, die in het dorp mensen van kleur staande houdt en ondervraagt. Alle activiteiten worden online gecoördineerd, versterkt, van complottheorieën voorzien, beschreven, in beeld gebracht en internationaal verspreid.

Hoewel deze situaties sterk van elkaar verschillen, laten zij ook overeenkomsten zien. Waar de aanleiding voor ordeverstoringen varieert (van voetbalgeweld en illegale feesten tot demonstraties, maatschappelijke spanningen en protesten tegen overheidsbeleid), worden sociale media en online platforms toegepast om mensen te informeren, te mobiliseren en met elkaar te verbinden. Geruchten, desinformatie en emotioneel geladen boodschappen verspreiden zich snel, waardoor gebeurtenissen kunnen escaleren en een eigen online dynamiek ontwikkelen die ook na afloop van een incident blijft doorwerken.

De rol van sociale media verandert ook de bestuurlijke opgave. Openbare ordeverstoringen beginnen niet pas wanneer mensen zich op straat verzamelen, maar ontwikkelen zich tevoren al online. Burgemeesters, politie en andere betrokken organisaties moeten daardoor eerder, onder grotere onzekerheid en met beperkte informatie afwegingen maken over monitoring, communicatie en eventueel ingrijpen. Daarbij moeten zij voortdurend een evenwicht vinden tussen het beschermen van de openbare orde en het respecteren van fundamentele rechten, zoals de

[1] De dataverzameling voor dit onderzoek heeft plaatsgevonden tussen 1 juli 2025 en 1 juni 2026.

uitingsvrijheid en het demonstratierecht. De voorbeelden laten zien dat de gevolgen van zulke afwegingen groot kunnen zijn: voor bewoners, bestuurders, politie en hulpverleners.

Nederland is niet het enige land dat zoekt naar manieren om hiermee om te gaan. Veel landen experimenteren met aanpakken op het gebied van bijvoorbeeld monitoring, samenwerking, preventie en handhaving. Dit onderzoek verkent hoe andere Europese landen omgaan met openbare-ordeverstoringen waarin online communicatie een rol speelt en welke lessen daaruit kunnen worden afgeleid voor Nederland. Om dit te kunnen doen is het nodig eerst stil te staan bij de relatie tussen online dynamiek en openbare-ordeverstoringen.

1.1 Online dynamiek en offline verstoringen

In het maatschappelijk debat wordt vaak onderscheid gemaakt tussen online en offline, alsof het om twee afzonderlijke werelden gaat. Dat onderscheid is in de praktijk steeds minder houdbaar. Online en offline zijn sterk met elkaar verweven. Mensen verkeren in wat wel wordt getypeerd als *The Onlife*: het resultaat van het doordringen van informatie- en communicatietechnologie in alle facetten van het samenleven (Floridi, 2015). Gebeurtenissen moeten daarom worden begrepen als het resultaat van interacties tussen en wederzijdse beïnvloeding door online en offline processen. Die wisselwerking kan beide kanten op gaan. Niet alleen kunnen online processen bijdragen aan verstoringen van de openbare orde, ook kunnen gebeurtenissen in de fysieke wereld aanleiding geven tot grootschalige online onrust.

Op sociale media en online platforms krijgt deze verwevenheid concreet vorm. Deze platforms bieden gebruikers mogelijkheden (*affordances*; Boyd, 2010) die het ontstaan en verloop van interacties tussen online en offline beïnvloeden. Zo maken zij snelle en grootschalige verspreiding van informatie mogelijk, vaak zonder voorafgaande toetsing, en bieden zij ruimte voor anonimiteit en directe communicatie met grote groepen. Hierdoor kunnen informatie, beelden, geruchten en desinformatie zich snel verspreiden binnen netwerken van gelijkgestemden. Dit beïnvloedt hoe situaties zich ontwikkelen en hoe mensen zich organiseren.

Deze kenmerken van online platforms maken het bovendien mogelijk om mensen op grote schaal te mobiliseren. Oproepen kunnen gericht zijn op uiteenlopende activiteiten, zoals demonstraties, bijeenkomsten, evenementen of andere vormen van collectief handelen. In sommige gevallen kunnen dergelijke mobilisatieprocessen bijdragen aan spanningen, confrontaties of verstoringen van de openbare orde. Wanneer online uitingen expliciet oproepen tot geweld in de publieke ruimte, kan worden gesproken van online aangejaagd geweld (Greijdanus et al., 2023).

De verwevenheid van online communicatie en openbare orde roept de vraag op hoe situaties waarin online mobilisatie een rol speelt bij ordeverstoringen moeten worden begrepen en afgebakend. Om dit fenomeen nader te duiden, is het nodig te verhelderen wat onder online aangejaagde openbare-ordeverstoringen wordt verstaan.

Online aangejaagde (openbare) ordeverstoringen (OAOV)

De formulering 'online aangejaagd' verwijst naar een verband tussen het gebruik van online platforms en het ontstaan of versterken van verstoringen van de openbare orde. Het gaat daarbij om intentioneel handelen: het bewust inzetten van online platforms om mensen te informeren, desinformeren, mobiliseren of aan te zetten tot gedrag dat kan bijdragen aan een verstoring van de openbare orde. De Veen et al. (2024) definiëren een online aangejaagde openbare-ordeverstoring daarom als:

Een situatie waarin de openbare orde wordt verstoord, omdat personen, al dan niet in groeps- of organisatieverband, bewust online platforms gebruiken om mensen te (des)informeren en op te roepen om op een specifiek moment op een bepaalde fysieke plek (offline) te zijn en te dreigen (al dan niet strafbare) handelingen te verrichten, die tot openbare ordeverstoring leiden.

Deze werkdefinitie helpt om het fenomeen af te bakenen, maar lost niet alle vragen op. Omdat (online aangejaagde) ordeverstoringen niet centraal worden geregistreerd, is weinig bekend over zowel de omvang van het fenomeen als over de samenhang tussen online activiteiten en feitelijke openbare-ordeverstoringen. Daardoor is in de praktijk lastig vast te stellen hoe sterk het verband is tussen online gedrag en een (dreigende) verstoring van de openbare orde. Oproepen die op zichzelf legitiem zijn, kunnen uitmonden in situaties waarin de openbare orde onder druk komt te staan. Omgekeerd leiden niet alle problematische of gewelddadige online uitingen daadwerkelijk tot openbare-ordeverstoringen. Ook vallen geweld en openbare-ordeverstoringen niet volledig samen: sommige ordeverstoringen verlopen zonder geweld, terwijl niet elk geweldsincident een verstoring van de openbare orde vormt.

Het handelingsvraagstuk voor bestuur en handhaving ligt daarom niet zozeer in de beschrijving van het fenomeen, maar in de beoordeling van concrete situaties. Wanneer is er sprake van online aanjaging die ingrijpen rechtvaardigt, en wanneer niet? Juist omdat online mobilisatie op zichzelf vaak een legitieme vorm van communicatie is, ontstaat de vraag wanneer online gedrag overgaat van wettig handelen naar een aanleiding voor overheidsoptreden.

Het normatieve kader: vrijheid en openbare orde

Dit roept de vraag op wat in dit verband onder een 'verstoring van de openbare orde' moet worden verstaan. Een verstoring van de openbare orde kan in algemene zin worden opgevat als een inbreuk op de normale gang van zaken in de publieke ruimte, die voor een bredere groep mensen merkbaar is en die als ontwrichtend wordt ervaren[2]. Wat als een ordeverstoring geldt, is echter afhankelijk van het perspectief van waaruit deze wordt benaderd.

Wel ordeverstoring, maar als demonstratie niet strafbaar

De oproepen van Extinction Rebellion om de A12 en de A10 te bezetten of luchthavens te betreden, hebben de intentie om de openbare orde te verstoren, met als doel meer aandacht voor klimaat en biodiversiteit. De verstoring van de snelweg of het (al dan niet met vernieling) binnendringen van een luchthaven brengt gevaarzetting die als strafbaar kan worden gezien met zich mee. Tegelijkertijd is de demonstratie als zodanig echter niet strafbaar, want niet opruiend en beschermd door het demonstratierecht en de grondwettelijke uitingsvrijheid.

Aan de ene kant gaat het om fundamentele vrijheden, zoals de vrijheid van meningsuiting en het recht om te demonstreren. Deze rechten zijn verankerd in de Grondwet, en maken het mogelijk om standpunten te uiten, anderen te mobiliseren en zichtbaar deel te nemen aan het publieke debat. Uitgangspunt daarbij is dat voorafgaand geen toestemming nodig is en dat beperkingen slechts onder voorwaarden en op basis van een wettelijke grondslag zijn toegestaan. Bovendien heeft de overheid niet alleen de taak deze rechten te respecteren, maar ook om demonstraties zoveel mogelijk te faciliteren en te

[2] https://www.burgemeesters.nl/themas/openbare-orde-en-veiligheid/begripsbepaling/

beschermen, ook wanneer deze hinder, overlast of maatschappelijke spanning veroorzaken (Swart et al., 2025, Nationale ombudsman, 2018; 2026). Aan de andere kant heeft de overheid de taak om de openbare orde en veiligheid te waarborgen. Dat betekent dat zij verantwoordelijk is voor het voorkomen en beëindigen van situaties waarin de normale gang van zaken in de publieke ruimte wordt verstoord. Het uitoefenen van grondrechten kan overigens gepaard gaan met verstoring van de openbare orde, terwijl het handhaven van de openbare orde beperkingen kan meebrengen voor de uitoefening van diezelfde rechten. De verhouding tussen vrijheid en openbare orde is daarmee per definitie een kwestie van afweging.

Deze verschillende perspectieven maken duidelijk dat het begrip OAOV niet eenduidig is: wat vanuit het ene perspectief aanleiding kan zijn om in te grijpen, kan vanuit een ander perspectief juist als toegestaan of zelfs beschermd worden beschouwd. Deze afweging krijgt concreet vorm binnen verschillende juridische kaders, die elk hun eigen invalshoek en mogelijkheden bieden om met ordeverstoringen om te gaan (zie ook Swart et al., 2025; Roorda et al., 2025).

Bestuurlijk perspectief
Vanuit bestuurlijk perspectief ligt de nadruk op het kunnen optreden tegen (dreigende) verstoringen van de openbare orde. De burgemeester is op grond van de Gemeentewet belast met de handhaving daarvan. Hij of zij beschikt over verschillende bevoegdheden, zoals het geven van bevelen en het treffen van maatregelen als een gebiedsverbod, een meldingsplicht, het aanwijzen van een veiligheidsrisicogebied en het inzetten van noodbevelen en noodverordeningen (Greijdanus et al., 2020; 2023). Vanuit de APV kunnen aanvullende maatregelen worden opgelegd, zoals een samenscholingsverbod of verblijfsontzegging. Voor de uitvoering van deze bevoegdheden kan de burgemeester gebruikmaken van de politie, die daarbij onder het gezag van de burgemeester opereert.

Deze bestuursrechtelijke bevoegdheden zijn echter primair ontwikkeld voor het adresseren van verstoringen in de fysieke ruimte. In situaties van OAOV, waarin online en offline dynamiek nauw met elkaar zijn verweven, sluiten deze instrumenten niet altijd goed aan. Met name de online component is binnen bestaande juridische kaders moeilijk te adresseren, terwijl juist daar signalen ontstaan en dynamieken zich ontwikkelen. Dat geldt voor Nederland, maar ook voor andere Europese landen (Winter et al., 2025).

Zoals de landsadvocaat laat zien, bieden de bestaande bevoegdheden weinig houvast om in te grijpen in de fase waarin online aanjaging zich ontwikkelt, terwijl juist daar de behoefte aan optreden ligt (Bierens et al., 2023). Dit betekent dat het lokale bestuur wel verantwoordelijk is voor het voorkomen van ordeverstoringen, maar in de praktijk slechts beperkt kan ingrijpen op de processen die daaraan voorafgaan.

Strafrechtelijk perspectief
Vanuit strafrechtelijk perspectief staat de vraag centraal of er sprake is van een strafbaar feit en, zo ja, welk delict er aan de orde is. Dit perspectief biedt duidelijke aanknopingspunten als grenzen van het strafrecht worden overschreden, maar sluit minder goed aan bij situaties waarin gedrag wel bijdraagt aan ordeverstoring maar er niet direct sprake is van strafbaarheid. Bovendien is het niet altijd duidelijk of en in welke mate bepaald gedrag – online of offline – daadwerkelijk bijdraagt aan een verstoring van de openbare orde (De Jong et al., 2016).

Civielrechtelijk perspectief
Het civiele recht biedt in sommige gevallen aanvullende mogelijkheden, zoals bijvoorbeeld het aanspreken van partijen op onrechtmatige daad of procedures die zijn gericht op het verwijderen

van online content. Daarbij spelen met name private partijen, zoals platforms, een belangrijke rol. Deze routes zijn in de regel echter reactief van aard en afhankelijk van concrete gevallen, en bieden daarmee geen structureel antwoord op de bestuurlijke behoefte om bij dreigende ordeverstoringen vroegtijdig in te grijpen. Zie bijvoorbeeld het onderzoek van Eysink Smeets et al. (2025) naar de aanpak van de complottheorie rond de begraafplaats in Bodegraven. In deze casus werden strafrechtelijke, civielrechtelijke en bestuursrechtelijke instrumenten in samenhang ingezet om de ontstane online en offline problematiek aan te pakken.

1.2 Doel- en vraagstelling

Online aangejaagde openbare-ordeverstoringen zijn geen exclusief Nederlands fenomeen. Ook in andere landen worden overheden geconfronteerd met de vraag hoe om te gaan met de rol van online dynamiek bij ordeverstoringen en hoe daarop tijdig en rechtmatig te kunnen ingrijpen.

De vraag hoe om te gaan met online aangejaagde openbare-ordeverstoringen kent geen eenduidig antwoord. Landen maken hierin verschillende keuzes, die samenhangen met verschillen in juridische kaders, bestuurlijke organisatie en maatschappelijke context. Juist deze variatie biedt de mogelijkheid om inzicht te krijgen in verschillende manieren waarop overheden proberen grip te krijgen op OAOV, welke afwegingen daarbij worden gemaakt en welke voor- en nadelen aan verschillende benaderingen zijn verbonden. Daarmee maakt een internationale vergelijking het mogelijk om oplossingsrichtingen te identificeren en te bezien welke elementen daarvan voor de Nederlandse context relevant kunnen zijn.

Dit onderzoek richt zich daarom op het in kaart brengen van aanpakken die in andere landen worden ontwikkeld en toegepast om online aangejaagde openbare-ordeverstoringen te signaleren, te voorkomen en te beheersen, met als doel te bezien welke elementen daarvan relevant en bruikbaar kunnen zijn voor de Nederlandse praktijk. De hoofdvraag luidt:

Wat kan worden geleerd van de aanpakken die andere landen hebben ontwikkeld om online aangejaagde ordeverstoringen te adresseren?

Om deze vraag te beantwoorden, wordt eerst verkend hoe dergelijke ordeverstoringen zich in de praktijk manifesteren. Daarbij gaat het om de wijze van mobilisatie, de gebruikte online kanalen en de interactie tussen online dynamiek en fysieke ordeverstoringen, evenals om de reacties van betrokken autoriteiten. Vervolgens wordt in een selectie van landen onderzocht welke aanpakken zijn ontwikkeld om OAOV te voorkomen, erop te reageren en de gevolgen ervan te beperken. Hiervoor formuleren we de volgende deelvragen:

1. Hoe manifesteren online aangejaagde openbare-ordeverstoringen zich in de praktijk?
2. Welke (typen) aanpakken hanteren verschillende Europese landen om OAOV te signaleren, te voorkomen en te beheersen, en hoe functioneren deze in de praktijk?
3. Welke elementen uit de onderzochte buitenlandse aanpakken zijn relevant voor de Nederlandse context?

1.3 Opzet van het onderzoek

Om de onderzoeksvragen te beantwoorden, is het onderzoek opgebouwd uit drie samenhangende stappen: (1) een verkenning van het fenomeen online aangejaagde ordeverstoringen, (2) een inventarisatie van buitenlandse aanpakken en (3) een verdieping in een selectie van landen en aanpakken.

Stap 1: Verkenning van het fenomeen

De eerste stap betreft een verkenning van hoe online aangejaagde openbare-ordeverstoringen zich in verschillende landen in de praktijk manifesteren. Deze verkenning is uitgevoerd aan de hand van wetenschappelijke literatuur en een inventarisatie van incidenten in Nederland en het buitenland. Voor die inventarisatie is gebruikgemaakt van nieuwsberichten, rapporten en openbare bronnen. Het doel was niet het verkrijgen van een uitputtend overzicht, maar om zicht te krijgen op de verschillende verschijningsvormen van online aangejaagde openbare-ordeverstoringen en de rol van online dynamieken daarin. Daarbij is gekeken naar de wijze waarop mobilisatie tot stand komt, welke online kanalen en dynamieken daarbij een rol spelen, hoe online en offline processen op elkaar ingrijpen en welke reacties van overheden en andere actoren zichtbaar zijn. Deze stap dient om zicht te krijgen op relevante verschijningsvormen en variatie daarin. Dat is nodig om te kunnen bepalen welke typen situaties en interventies in de internationale vergelijking van belang zijn.

In hoofdstuk 2 wordt het fenomeen online aangejaagde openbare-ordeverstoringen verkend aan de hand van literatuur en empirische voorbeelden. Daarbij ligt de nadruk op de wijze waarop dergelijke ordeverstoringen zich manifesteren, en welke online en offline dynamieken daarbij een rol spelen.

Stap 2: Inventarisatie van buitenlandse aanpakken

De tweede stap bestaat uit een inventarisatie van buitenlandse aanpakken. Deze inventarisatie is uitgevoerd aan de hand van een brede verkenning van openbare bronnen, waaronder beleidsdocumenten, wet- en regelgeving, rapporten van overheden en toezichthouders, nieuwsbronnen en wetenschappelijke literatuur. De geïdentificeerde aanpakken zijn beschreven aan de hand van verschillende kenmerken, waaronder hun doelstelling, juridische grondslag, betrokken actoren en het type interventie. Omdat de gevonden aanpakken sterk uiteenliepen, is niet gekozen voor een systematische vergelijking op één uniforme set criteria. In plaats daarvan is de inventarisatie gebruikt om patronen te identificeren en een selectie van relevante landen en aanpakken samen te stellen voor nadere verdieping.

In hoofdstuk 3 gaan we nader in op welke typen interventies we konden onderscheiden. Deze inventarisatie vormde de basis voor de selectie van vijf landen en aanpakken voor nadere bestudering. Bij die selectie is gelet op relevantie voor de Nederlandse context, variatie in institutionele en juridische inrichting, concrete ervaring met het fenomeen en de aanwezigheid van herkenbare of juist afwijkende benaderingen.

Stap 3: Verdieping van de landen

In de derde stap worden de geselecteerde aanpakken onderzocht. Voor de geselecteerde landen is aanvullend documentonderzoek uitgevoerd naar wet- en regelgeving, beleidsdocumenten, parlementaire stukken, rapporten van toezichthouders en wetenschappelijke publicaties. Daarnaast zijn semigestructureerde interviews gehouden met deskundigen uit de wetenschap en de beleids- en uitvoeringspraktijk uit de verschillende landen. De interviews vonden telefonisch plaats en waren gericht op het duiden van de institutionele context, de werking van de geselecteerde aanpakken en de betekenis daarvan in de praktijk.

De hoofdstukken 4 tot en met 8 bevatten de resultaten voor de geselecteerde landen: Zweden, Ierland, het Verenigd Koninkrijk, Frankrijk en Duitsland. In elk hoofdstuk wordt de relevante institutionele context geschetst, worden voorbeelden van ordeverstoringen besproken, en worden de belangrijkste juridische en beleidsmatige kaders en geselecteerde aanpakken geanalyseerd. Deze verdieping is uitgevoerd aan de hand van documentanalyse van wet- en regelgeving, beleidsdocumenten, parlementaire stukken en rapporten van toezichthouders, aangevuld met wetenschappelijke en journalistieke bronnen en interviews. Waar mogelijk is gebruikgemaakt van

oorspronkelijke (nationale) bronnen. In elk landenhoofdstuk wordt eerst de bestuurlijke en juridische context van openbare orde en veiligheid geschetst. Vervolgens wordt aan de hand van incidenten en casuïstiek geïllustreerd in welke situaties online aanjaging een rol speelt. Daarna worden de relevante juridische en beleidsmatige kaders beschreven, gevolgd door een analyse van één of meerdere concrete aanpakken, inclusief de betrokken actoren, hun bevoegdheden en de wijze waarop deze aanpakken in de praktijk functioneren (zie ook: Winter et al., 2025).

Stap 4: Synthese en lessen

In hoofdstuk 9 en 10 sluiten we het onderzoek af met een synthese van de bevindingen uit de landenstudies. We analyseren de overeenkomsten en verschillen tussen de onderzochte aanpakken en reflecteren op de betekenis daarvan voor de Nederlandse context. Doel is om inzicht te krijgen in de werkzame elementen, de randvoorwaarden en de mogelijke spanningen die relevant zijn voor de verdere ontwikkeling van beleid en instrumentarium in Nederland.

Op basis van een vergelijkende analyse van de landenstudies zijn lessen geformuleerd. Deze lessen zijn vervolgens besproken tijdens een online expertsessie met Nederlandse deskundigen op het gebied van openbare orde, veiligheid, bestuur, recht en handhaving. De sessie diende om de bevindingen en conclusies te toetsen en te verdiepen, en zo de lessen aan te scherpen.

2 Verschijningsvormen OAOV

In dit hoofdstuk werken we uit in welke verschijningsvormen OAOV zich in de praktijk voordoen. Hoewel in het maatschappelijk en bestuurlijk debat vaak over *online* aangejaagde opbenbare-ordeverstoringen wordt gesproken alsof het om één duidelijk afgebakend fenomeen gaat, laat de praktijk een gevarieerd beeld zien. Bovendien hebben vrijwel alle hedendaagse openbare-ordeverstoringen een online component, maar verschillen de aard, intensiteit en betekenis daarvan sterk van geval tot geval. Soms speelt online communicatie vooral een organiserende rol, soms versterkt zij bestaande spanningen, en soms fungeert zij vooral als versneller van een dynamiek die al in gang was gezet.

Tabel 1: Enkele voorbeelden van OAOV in Europa in de afgelopen jaren.

Voorbeeld	Jaar	Toelichting	Toelichting
Paasrellen (Zweden)	2022	Rellen naar aanleiding van aangekondigde koranverbrandingen door Rasmus Paludan. In meerdere steden vonden confrontaties met de politie plaats.	§ 4.2 p. 30
Oxford Street-rellen (VK)	2023	Grote groepen jongeren verzamelden zich in het centrum van Londen na oproepen waarin werd gesuggereerd dat winkels zouden worden geplunderd en gratis goederen konden worden verkregen.	§ 5.2 p. 36
Southport-rellen (VK)	2024	Rellen na de verspreiding van onjuiste informatie over een verdachte van een steekincident.	§ 5.4 p. 40
Dublin-rellen (Ierland)	2023	Rellen na een steekincident waarbij online geruchten over de afkomst van de verdachte snel werden verspreid.	§ 6.2 p. 45
Bloquons Tout! (Frankrijk)	2024	Een online georganiseerde Franse protestbeweging die opriep tot boycots, blokkades en een algemene staking uit protest tegen bezuinigingen en sociale afbraak.	§ 7.2 p. 50
Nahel Merzouk-rellen (Frankrijk)	2023	Landelijke rellen na het doodschieten van de 17-jarige Nahel Merzouk door de politie.	§ 7.2 p. 54
Boeren-protesten (Duitsland)	2024	Grootschalige protesten tegen landbouw-, milieu- en economisch beleid.	§ 8.2 p. 67

Om die variatie systematisch te begrijpen, onderscheiden we in dit hoofdstuk drie vragen. Waarom mobiliseren mensen zich? Via welke online netwerken, platforms en communicatievormen komt die mobilisatie tot stand? Hoe vertaalt die mobilisatie zich in gedrag in de publieke ruimte, en hoe verloopt zo'n incident vervolgens? Daarbij gaat het niet uitsluitend om demonstraties die uit de hand lopen, maar bijvoorbeeld ook om onrust rondom politieke besluiten, overlast door groepen en individuen en illegale evenementen.

We werken deze drie vragen uit aan de hand van wetenschappelijke literatuur over online mobilisatie, collectieve actie en openbare orde, aangevuld met voorbeelden uit verschillende landen. Het doel van dit hoofdstuk is om zicht te krijgen op de verschillende manieren waarop online en offline dynamiek met elkaar verweven zijn. Die variatie vormt vervolgens de opmaat naar het volgende hoofdstuk, waarin verschillende typen aanpakken worden onderscheiden. Ter illustratie toont Tabel 1 een aantal voorbeelden van OAOV die zich in de afgelopen jaren in verschillende Europese landen hebben voorgedaan.

2.1 Motivatie en thematiek

Een eerste manier om variatie in OAOV te begrijpen, is door te kijken naar de motieven en thema's die aan mobilisatie ten grondslag liggen. Onderzoek naar protestmobilisatie laat zien dat deelnemers zich om uiteenlopende redenen organiseren (Hutter & Borbáth, 2019), variërend van sociaaleconomische belangen en identiteitsvraagstukken tot migratie, discriminatie, religieuze spanningen en maatschappelijke onvrede. In de literatuur over ordeverstoringen wordt vaak onderscheid gemaakt tussen meer ideologisch gedreven en niet-ideologisch gedreven incidenten. Walgrave et al. (2013) laten bijvoorbeeld zien dat motivaties van demonstranten kunnen worden begrepen langs dimensies als instrumenteel versus expressief en individueel versus collectief. Die indeling maakt duidelijk dat sommige vormen van mobilisatie primair zijn gericht op het uitdrukken van overtuigingen, waarden of identiteiten, terwijl andere vormen meer draaien om concrete eisen, directe belangen of groepsdynamiek.

Bovendien geldt dat niet elke verstoring van de normale gang van zaken direct een onaanvaardbare aantasting van de openbare orde vormt. Demonstraties en andere collectieve acties kunnen gepaard gaan met hinder, overlast of tijdelijke ontregeling van de publieke ruimte, terwijl zij tegelijkertijd bescherming genieten onder het recht op vrijheid van vergadering en vereniging (artikel 11 EVRM[3]).

Tabel 2 toont enkele voorbeelden van motieven en thema's die ten grondslag kunnen liggen aan online aangejaagde openbare-ordeverstoringen. Sommige incidenten draaien om religieuze en culturele spanningen, zoals de Zweedse Paasrellen en de protesten rond koranverbrandingen. Andere hangen samen met migratie en nationale identiteit, zoals de rellen in Southport. Daarnaast kunnen sociaaleconomische grieven een belangrijke rol spelen, zoals bij Bloquons Tout! in Frankrijk en de Duitse boerenprotesten. Ook incidenten rond politiegeweld, discriminatie en sociale uitsluiting kunnen leiden tot grootschalige mobilisatie, zoals bij de rellen na de dood van Nahel Merzouk in Frankrijk.

[3] Raad van Europa. (1950). Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

Deze voorbeelden laten zien dat online aangejaagde openbare-ordeverstoringen niet aan één specifiek thema zijn verbonden. De onderliggende motieven verschillen sterk, maar kunnen in alle gevallen via online communicatie worden versterkt en verspreid met mogelijke polarisatie tot gevolg. Naast ideologisch gedreven incidenten zijn er ook ordeverstoringen waarbij politieke overtuigingen geen of slechts een beperkte rol spelen. Jusko en Weihe (2024) beschrijven bijvoorbeeld hoe hooliganisme vaak eerder voortkomt uit rivaliteit, status, groepsdynamiek en situationele escalatie dan uit een inhoudelijk politiek motief. De massale vechtpartij tussen Napoli- en Roma-supporters op de snelweg A1 in Italië laat zien hoe ook zonder ideologische inzet ernstige ordeverstoringen kunnen ontstaan. Iets vergelijkbaars geldt voor incidenten die samenhangen met de influencer-cultuur of online hypes. Abidin (2021) laat zien hoe influencers via platforms als TikTok grote groepen kunnen mobiliseren rond consumptie, aandacht of beloftes van gratis goederen, zonder dat daar een politiek programma achter zit. De Oxford Street-rellen in Londen (in 2023) zijn daarvan een illustratief voorbeeld.

Tabel 2: Enkele voorbeelden van motieven en thema's die ten grondslag kunnen liggen aan protesten die zijn uitgelopen op openbare-ordeverstoringen.

Voorbeeld	Motieven en thema's
Paasrellen (Zweden)	Religieuze en culturele spanningen; vrijheid van meningsuiting; identiteit
Oxford Street-rellen (VK)	Influencercultuur, online hype, aandachtseconomie en groepsdynamiek; geen duidelijk politiek of ideologisch motief
Southport-rellen (VK)	Migratie; desinformatie; maatschappelijke spanningen
Dublin-rellen (Ierland)	Migratie; maatschappelijke onvrede; desinformatie
Bloquons Tout! (Frankrijk)	Sociaaleconomische grieven; sociale rechtvaardigheid; wantrouwen jegens overheid en instituties.
Nahel Merzouk-rellen (Frankrijk)	Politiegeweld; discriminatie; sociale uitsluiting
Boerenprotesten (Duitsland)	Beroeps- en sectorbelangen; sociaaleconomische zorgen

Deze indeling is analytisch behulpzaam, maar de praktijk is zelden zuiver. Ideologisch gemotiveerde incidenten kunnen opportunistische of speelse elementen bevatten, terwijl niet-ideologische incidenten achteraf alsnog ideologisch worden geframed. Ook kunnen motieven tijdens een incident verschuiven: wat begint als protest, hype of herdenking, kan door escalatie, politieoptreden of online verspreiding een andere betekenis krijgen (Donson et al., 2004). Dat maakt het van belang om motivatie en thematiek niet als vaste categorieën te behandelen, maar als een eerste dimensie van variatie.

2.2 Mobilisatie en netwerken

Een tweede dimensie betreft de manier waarop mobilisatie tot stand komt. Tabel 3 toont voor de eerdergenoemde voorbeelden manieren waarop deelnemers aan openbare-ordeverstoringen online worden gemobiliseerd.

Waar protest en collectieve actie traditioneel vaak werden verbonden aan organisaties, leiders en formele structuren, benadrukt recente literatuur dat mobilisatie steeds vaker verloopt via digitale, gepersonaliseerde en deels diffuse netwerken. Bennett en Segerberg (2012) beschrijven dit als *connective action*: collectieve actie die minder afhankelijk is van centrale organisatie en sterker draait om losse verbindingen tussen individuen, gedeelde verontwaardiging en snelle online verspreiding.

Tabel 3: Enkele voorbeelden van manieren waarop deelnemers aan openbare-ordeverstoringen online worden gemobiliseerd.

Voorbeeld	Vormen van online mobilisatie
Paasrellen (Zweden)	Sociale media, online discussieplatforms en berichtenapps verspreidden oproepen en reacties
Oxford Street-rellen (VK)	TikTok, influencers, virale video's en algoritmische verspreiding van content
Southport-rellen (VK)	TikTok, X, Telegram en influencers speelden een belangrijke rol bij verspreiding en mobilisatie
Dublin-rellen (Ierland)	Sociale media, online geruchten en informele netwerken
Bloquons Tout! (Frankrijk)	Via sociale media georganiseerd in een burgercollectief dat los stond van politieke partijen en vakbonden
Nahel Merzouk-rellen (Frankrijk)	Virale verspreiding van videobeelden via Snapchat, TikTok en andere sociale media
Boerenprotesten (Duitsland)	Telegram, Facebook, X en bestaande boerennetwerken

Dat betekent niet dat klassieke organisaties zijn verdwenen. Vakbonden, actiegroepen, bewegingen en maatschappelijke organisaties kunnen nog altijd een belangrijke rol spelen in het bijeenbrengen van mensen. Maar daarnaast zien we steeds vaker mobilisatie via overlappende online netwerken waarin geen duidelijke hiërarchie of centrale regie zichtbaar is. Denk bijvoorbeeld aan de protesten van Bloquons Tout! in Frankrijk. Juist in zulke netwerken kunnen oproepen, beelden, slogans en frames zich snel verspreiden onder mensen met uiteenlopende achtergronden, die elkaar online tegenkomen, elkaars verontwaardiging herkennen en elkaars taal en gedragingen overnemen. Mobilisatie verloopt in zulke gevallen dus niet primair via één zender of organisatie, maar via een veelheid aan gebruikers, accounts en kanalen die elkaar versterken.

De online structuren waarlangs dat gebeurt verschillen per incident. Soms verloopt mobilisatie via open en zichtbare platforms. De protesten van de Franse Bloquons Tout! werden bijvoorbeeld grotendeels georganiseerd via netwerken als X, TikTok en Facebook. Maar ook hebben gesloten of semi-gesloten kanalen, zoals Telegram hier een belangrijke rol gespeeld. Zulke kanalen worden relatief vaak genoemd in verband met radicale, extremistische of gewelddadige mobilisaties, mede omdat zij ruimte bieden voor snellere onderlinge afstemming, minder publieke zichtbaarheid en een sterkere groepsdynamiek. De Zweedse Paasrellen of de Southportrellen in het Verenigd Koninkrijk zijn hier voorbeelden van.

Daarnaast spelen influencers, rappers of andere figuren met een grote online zichtbaarheid een specifieke rol. Zij fungeren niet noodzakelijk als leiders in klassieke zin, maar kunnen wel dienen als trigger of katalysator. Door hun bereik en zichtbaarheid kunnen zij een bestaande sfeer van verontwaardiging of opwinding plotseling omzetten in concrete actie. Dat zagen we bijvoorbeeld bij de Oxford Street-rellen, maar ook bij Franse straatprotesten rond politiegeweld, waar oproepen en beelden via influencers verdere verspreiding kregen.

Een belangrijk punt is dat online mobilisatie niet alleen bestaat uit het doorgeven van praktische informatie, zoals tijd en plaats. Zij draait ook om affect, herkenning en legitimatie. Emotioneel geladen beelden, geruchten, desinformatie en moraliserende frames kunnen bijdragen aan het gevoel dat deelname aan een actie, protest of bijeenkomst noodzakelijk of gerechtvaardigd is. Tijdens de rellen in Southport (VK) werden geruchten over asielzoekers via sociale media versterkt, waardoor verontwaardiging, dreiging en mobilisatie elkaar konden versterken. Postma et al. (2025) beschrijven een Nederlandse casus waarin online geruchten en desinformatie rondom vermeende zedendelicten uitmondden in fysieke onrust en geweld. De online dimensie is daarmee niet slechts een communicatiemiddel, maar een onderdeel van de dynamiek zelf. In sommige gevallen worden dergelijke processen overigens bewust versterkt door gecoördineerde beïnvloedingsactiviteiten. In Europees beleid wordt hiervoor de term *Foreign Information Manipulation and Interference* (FIMI) gebruikt.

De wijze van mobilisatie zegt daarmee veel over het karakter van een incident. Sommige ordeverstoringen worden zichtbaar georganiseerd, andere ontstaan uit diffuse, decentrale en elkaar snel overlappende online netwerken. Juist die variatie helpt verklaren waarom vergelijkbare offline gebeurtenissen toch heel verschillend kunnen verlopen.

2.3 Actievormen en verloop

Een derde dimensie is de manier waarop mobilisatie zich vertaalt naar gedrag in de publieke ruimte. De literatuur over protest en ordeverstoringen laat zien dat sociale bewegingen en groepen beschikken over een brede set van tactieken en gedragsvormen waaruit ze kunnen kiezen om hun onvrede of boodschap te uiten. Berglund (2023) beschrijft bijvoorbeeld hoe bewegingen als Extinction Rebellion en de Spaanse anti-huisuitzettingsbeweging (PAH) gebruikmaken van protesten, variërend van vreedzame demonstraties tot blokkades van infrastructuur en vormen van burgerlijke ongehoorzaamheid. Daarmee sluit Berglund aan bij het klassieke overzicht van 198 methoden van *non-violent action* van Sharp (1973/2010), waarin ook symbolische protesten, herdenkingen en creatieve theatrale acties worden onderscheiden.

Voor het begrijpen van OAOV is vooral van belang dat deze actievormen niet vastliggen. Enkele voorbeelden van actievormen en ontwikkelpaden van online aangejaagde openbare-ordeverstoringen zijn in Tabel 4 samengevat. Incidenten kunnen vreedzaam beginnen en later escaleren, of juist beginnen als diffuse onrust en pas later een meer herkenbare protestvorm

aannemen. De herdenking van Ibrahima Barrie in Brussel (2021) begon bijvoorbeeld als een stille wake, maar mondde uit in confrontaties en massale arrestaties. Ook onderzoek naar de protesten in Hongkong laat zien dat mobilisatie in de loop van de tijd kan verschuiven van vreedzame manifestatie naar meer disruptieve of gewelddadige tactieken, mede afhankelijk van interacties tussen deelnemers, omstanders en autoriteiten.

Tabel 4: Enkele voorbeelden van actievormen en ontwikkelpaden van online aangejaagde openbare-ordeverstoringen.

Voorbeeld	Actievormen en ontwikkelpaden
Paasrellen (Zweden)	Demonstraties rond een controversiële gebeurtenis die op meerdere locaties uitmonden in grootschalige rellen
Oxford Street-rellen (VK)	Online hype leidt binnen korte tijd tot massale fysieke samenkomst; verstoring ontstaat vooral door massaliteit, groepsdynamiek en verwachtingen rond deelname
Southport-rellen (VK)	Online geruchten leiden tot snelle mobilisatie en verspreiding van rellen naar meerdere steden
Dublin-rellen (Ierland)	Geweld en wanorde vormen vanaf het begin onderdeel van de mobilisatie
Bloquons Tout! (Frankrijk)	Decentrale protestbeweging die zich ontwikkelt van demonstraties naar blokkades en periodieke escalaties
Nahel Merzouk-rellen (Frankrijk)	Politieoptreden en virale beelden fungeren als katalysator voor grootschalige nationale mobilisatie en rellen
Boeren-protesten (Duitsland)	Gecoördineerde protestcampagne met blokkades, demonstraties en langdurige actiedruk

Het is daarom nuttig om niet alleen naar de vorm van een gebeurtenis of samenkomst te kijken, maar ook naar het verloop ervan. Online oproepen kunnen immers leiden tot zeer verschillende uitkomsten: een geordende demonstratie, een blokkade, een ongeregelde samenkomst, een confrontatie met tegenbetogers of politie, of opportunistische plundering. De manier waarop een incident zich ontwikkelt, hangt samen met de combinatie van motieven, mobilisatiekanalen, groepssamenstelling, ruimtelijke context en de respons van autoriteiten.

Ook politieoptreden en bestuurlijke interventies beïnvloeden het verloop. Onderzoeken van Den Heyer (2019) en Moors et al. (2020; 2022) laten zien dat de eerste uren van een incident vaak bepalend zijn. Wanneer de politie laat of met beperkte capaciteit optreedt, kan dit bijdragen aan snelle escalatie. Andersom kan ook grootschalig en repressief optreden de spanning vergroten, zeker wanneer dit door betrokkenen of omstanders als disproportioneel wordt ervaren. Tijdens de Oxford Street-incidenten leidde de snelle online mobilisatie tot een situatie waarin jongeren zich al

verzamelden voordat de politie zichtbaar aanwezig was. In andere gevallen leidde juist de directe en grootschalige inzet van ordediensten tot nadrukkelijke confrontaties in de publieke ruimte.

Daarmee is het verloop van een incident geen neutraal eindpunt van voorafgaande mobilisatie, maar onderdeel van een voortdurende interactie tussen deelnemers, online dynamiek, publieke ruimte en autoriteiten. Voor OAOV is juist die wisselwerking van belang; niet alleen hoe mensen online worden gemobiliseerd, maar ook hoe die mobilisatie onderweg van vorm verandert.

2.4 Conclusie

De analyse in dit hoofdstuk bevestigt dat OAOV geen eenduidig fenomeen vormen. Wat de onderzochte voorbeelden gemeen hebben, is niet een specifieke aanleiding, actievorm of groep betrokkenen, maar de aanwezigheid van een betekenisvolle wisselwerking tussen online en offline processen. De rol die online communicatie daarin vervult, verschilt echter sterk. Zij kan bijdragen aan mobilisatie, coördinatie, escalatie, informatieverspreiding of groepsvorming en vervult vaak meerdere functies tegelijk.

Deze bevinding laat zien dat OAOV niet kunnen worden teruggebracht tot één type incident of één onderliggend mechanisme. De betekenis van online communicatie hangt steeds samen met de bredere maatschappelijke en situationele context waarin een incident ontstaat en zich ontwikkelt. Voor de analyse van buitenlandse aanpakken betekent dit dat niet alleen moet worden gekeken naar het type incident, maar ook naar de specifieke rol die online communicatie daarin speelt.

3 Aanpakken van OAOV

Om zicht te krijgen op de manieren waarop verschillende landen omgaan met online aangejaagde openbare-ordeverstoringen, is een inventarisatie van buitenlandse aanpakken uitgevoerd. Het doel daarvan was niet om een uitputtend overzicht van alle bestaande maatregelen te geven, maar om inzicht te krijgen in de verscheidenheid aan benaderingen die in verschillende landen worden toegepast.

De inventarisatie is uitgevoerd aan de hand van een brede verkenning van openbare bronnen, waaronder wet- en regelgeving, beleidsdocumenten, rapporten van overheden en toezichthouders, nieuwsbronnen en wetenschappelijke literatuur. De inventarisatie laat zien dat de aangetroffen aanpakken sterk verschillen in doelstelling, juridische inbedding, betrokken actoren en wijze van uitvoering. Tegelijkertijd zijn er ook overeenkomsten zichtbaar. Op basis van deze overeenkomsten onderscheiden we in dit hoofdstuk vier clusters van aanpakken met vergelijkbare kenmerken. Deze clusters moeten niet worden opgevat als strikt afgebakende categorieën. Zij dienen vooral als hulpmiddel om de grote verscheidenheid aan aangetroffen aanpakken overzichtelijk te beschrijven. In de praktijk bevatten veel aanpakken kenmerken van meerdere clusters, en worden verschillende benaderingen ook vaak gecombineerd.

Cluster 1. Preventieve en maatschappelijke aanpakken
Deze aanpakken richten zich op het voorkomen van escalatie door het versterken van weerbaarheid, het bevorderen van bewustwording en het vroegtijdig signaleren van risico's. Ze grijpen in een vroeg stadium in, nog voordat zich concrete ordeverstoringen voordoen, en doen dat vooral via sociale, communicatieve en netwerkgerichte interventies. Het gaat om het beïnvloeden van gedrag en percepties, en om het mobiliseren van maatschappelijke actoren als onderwijsinstellingen, lokale overheden en maatschappelijke organisaties.

- Prevent Duty Guidance (VK)
  Wettelijke verplichting voor onderwijs, zorg en lokale overheden om signalen van extreem gedachtegoed en handelen vroegtijdig te herkennen en te delen met politiediensten, ter voorkoming van escalatie en ordeverstoring; werkt via professionele netwerken en meldstructuren en grijpt in vóórdat mobilisatie escaleert.
- Psychological Defence Agency – MPF (Zweden)
  Nationale aanpak gericht op het versterken van maatschappelijke weerbaarheid tegen desinformatie en buitenlandse beïnvloeding via monitoring, publiekscommunicatie en samenwerking met media en overheidsorganisaties.
- Malaga Preventieprogramma (Spanje)
  Gemeentelijk programma dat inzet op sociale cohesie, onderwijs en vroegsignalering van extreem gedachtegoed dat zou kunnen leiden tot ordeverstoring en radicalisering; werkt via lokale netwerken en richt zich op het verminderen van voedingsbodems voor mobilisatie via onder meer online platforms.
- Safer Internet Centre (Denemarken)
  Educatie- en ondersteuningsprogramma voor jongeren en ouders rond online risico's en schadelijke content; versterkt digitale weerbaarheid en vermindert vatbaarheid voor online aanjaging.

- Community Resilience Initiatives (Frankrijk)
  Lokale programma's gericht op burgerparticipatie, dialoog en mediavaardigheden om maatschappelijke spanningen en online aangewakkerde onrust te verminderen.

Cluster 2. Regulerende en toezichthoudende aanpakken
Deze aanpakken zijn eveneens vooral voorafgaand aan escalatie gepositioneerd, maar grijpen minder aan op individueel gedrag en meer op de structuur van de online omgeving. Ze richten zich op het vastleggen en handhaven van regels voor platforms en andere actoren, met als doel risico's systemisch te beperken. Door verplichtingen, toezicht en sanctiemogelijkheden wordt geprobeerd de voorwaarden te creëren waaronder schadelijke dynamiek minder snel kan ontstaan of escaleren.

- Coimisiún na Meán – Online Safety Code / Digital Services Act (Ierland)
  Onafhankelijke toezichthouder die toezicht houdt op online platforms en kan optreden wanneer zij hun wettelijke verplichtingen onder de Online Safety Code of Digital Services Act niet naleven.
- NetzDG-handhaving (Duitsland)
  Verplicht platforms om strafbare content snel te verwijderen en transparant te rapporteren; handhaving via boetes dwingt naleving en beperkt verspreiding van haat en opruiing.
- ARCOM (Frankrijk)
  Toezichthouder die platforms controleert op naleving van wettelijke verplichtingen en handhavend kan optreden bij overtredingen.
- Ofcom – Online Safety (VK)
  Britse toezichthouder die toezicht houdt op de naleving van de Online Safety Act door online platforms.
- Terrorist Content Online Regulation (EU)
  Europees kader dat snelle verwijdering van terroristische content verplicht stelt; harmoniseert regels en versterkt grensoverschrijdende handhaving richting platforms.

Cluster 3. Informatie- en intelligencegerichte aanpakken
Deze aanpakken bevinden zich dichter bij het moment waarop dynamiek zich ontwikkelt of al zichtbaar wordt. Zij zijn gericht op het verkrijgen, analyseren en duiden van informatie over online processen die kunnen leiden tot ordeverstoringen. Door monitoring en analyse wordt geprobeerd inzicht te krijgen in dreigingen, mobilisatiepatronen en desinformatie, zodat tijdig en gericht kan worden gehandeld. Deze aanpakken vormen vaak de schakel tussen preventie en interventie.

- Psychological Defence Agency – MPF (Zweden)
  Nationale aanpak gericht op het versterken van maatschappelijke weerbaarheid tegen desinformatie en buitenlandse beïnvloeding via monitoring, publiekscommunicatie en samenwerking met media en overheidsorganisaties.
- VIGINUM (Frankrijk)
  Gespecialiseerde eenheid die buitenlandse desinformatiecampagnes detecteert en analyseert; levert strategisch inzicht in online beïnvloeding en mobilisatie.
- NSOIT (VK)
  Overheidsunit die online desinformatie en andere risico's voor de openbare veiligheid monitort.
- KI4Demokratie (Duitsland)
  AI-gedreven analysetool die extremistische en antidemocratische boodschappen op sociale media identificeert en analyseert.
- NPoCC Internet Intelligence Team (VK)
  Politie-eenheid die sociale media monitort op signalen van openbare-orderisico's en deze informatie deelt met operationele eenheden voor vroegtijdig handelen.

- PET dreigingsanalyses (Denemarken)
  Nationale veiligheidsdienst die digitale ecosystemen en extremisme monitort en analyseert; ondersteunt vroegsignalering en beleidsbeslissingen.

Cluster 4. Handhavings- en repressieve aanpakken
Tot slot zijn er aanpakken die zich richten op het direct ingrijpen wanneer normen worden overtreden of wanneer ordeverstoringen zich voordoen. Deze interventies vinden plaats tijdens of na escalatie en zijn gericht op het stoppen, begrenzen of sanctioneren van gedrag. Ze maken gebruik van strafrechtelijke of bestuurlijke bevoegdheden, en zijn vaak zichtbaar en incidentgericht van aard.

- Landelijke actiedagen tegen haatpostings (Duitsland)
  Gecoördineerde opsporingsacties met doorzoekingen, verhoren en vervolging van verdachten van strafbare online uitingen; zichtbaar en direct ingrijpen.
- PHAROS / PNLH (Frankrijk)
  Meldplatform en gespecialiseerde vervolgingseenheid voor online haat en opruiing; verzamelt signalen en zet deze om in strafrechtelijke onderzoeken en vervolging.
- Zentrale Meldestelle für strafbare Inhalte – ZMI (Duitsland)
  Centrale meld- en triagefunctie die strafbare online content beoordeelt en doorgeleidt naar opsporing; versterkt de handhavingsketen.
- CITCO/Perci-aanpak (Spanje)
  Gericht op opsporen en verwijderen van terroristische online content in samenwerking met Europol; combineert detectie met directe interventie.
- Guardia Civil – aanpak Tsunami Democràtic (Spanje)
  Integrale interventie tegen Catalaanse onafhankelijkheidsbeweging, inclusief sluiten van platforms, digitale opsporing en vervolging; gericht op het ontmantelen van online gecoördineerde mobilisatie.

De inventarisatie laat een breed scala aan aanpakken zien. Sommige leggen de nadruk op preventie, monitoring en weerbaarheid, terwijl andere vooral zijn gericht op handhaving, vervolging en het beperken van schade tijdens of na incidenten. Daarnaast verschillen aanpakken in de mate waarin zij steunen op formele bevoegdheden, regelgeving en toezicht, dan wel op samenwerking, informatie-uitwisseling en operationele coördinatie. Deze twee dimensies bieden een bruikbaar perspectief om de verscheidenheid aan aangetroffen aanpakken te ordenen, zonder dat aanpakken zich altijd eenduidig in één categorie laten plaatsen.

Tegelijkertijd laat de inventarisatie zien dat landen in de praktijk vrijwel altijd verschillende benaderingen combineren. De onderscheiden clusters moeten daarom niet worden opgevat als afzonderlijke strategieën, maar als analytische accenten binnen een breder handelingsrepertoire. Juist deze diversiteit laat zien dat online aangejaagde openbare-ordeverstoringen vanuit verschillende invalshoeken kunnen worden benaderd, en dat landen daarin uiteenlopende keuzes maken.

3.1 Selectie van landen en aanpakken

De selectie van landen en aanpakken is gebaseerd op verschillende overwegingen. In de eerste plaats is ervoor gekozen voorbeelden op te nemen uit alle onderscheiden clusters van aanpakken. Daarmee wordt geborgd dat de verdere analyse niet beperkt blijft tot één type interventie, maar recht doet aan de breedte van het handelingsrepertoire dat uit de inventarisatie naar voren komt. De geselecteerde aanpakken vertegenwoordigen verschillende manieren waarop overheden en

andere actoren omgaan met online aangejaagde openbare-ordeverstoringen, variërend van maatschappelijke preventie en regulering van online omgevingen tot informatiegestuurde interventies en strafrechtelijke handhaving.

In de tweede plaats is gelet op de relevantie voor de Nederlandse context in termen van de institutionele en juridische inrichting. Daarom is gekozen voor landen die zijn gebonden aan het Europees Verdrag voor de Rechten van de Mens (EVRM), en die opereren binnen een democratische rechtsstaat waarin vergelijkbare eisen aan de bescherming van grondrechten en de legitimiteit van overheidsoptreden worden gesteld.

In de derde plaats is bewust gekozen voor een beperkt aantal landen. De aanpakken die in dit onderzoek centraal staan, zijn sterk verweven met hun institutionele, juridische en bestuurlijke context. Om deze aanpakken goed te kunnen begrijpen, is het noodzakelijk om niet alleen de interventie zelf te beschrijven, maar ook de context waarin deze functioneert. Een brede, maar oppervlakkige vergelijking van veel landen zou dit inzicht onvoldoende bieden. Daarom is gekozen voor een selectie waarin per land één of enkele aanpakken verdiepend worden uitgewerkt.

De uiteindelijke selectie bestaat uit een combinatie van landen en aanpakken die zowel inhoudelijk als institutioneel variatie bieden. Zweden en het Verenigd Koninkrijk illustreren verschillende vormen van preventieve en maatschappelijke aanpakken, waarbij de nadruk respectievelijk ligt op nationale coördinatie van weerbaarheid (MPF) en op vroegsignalering via publieke instellingen (Prevent). Het Verenigd Koninkrijk is daarnaast opgenomen vanwege de sterke ontwikkeling van informatiegestuurde aanpakken (NSOIT), waarin monitoring en duiding van online dynamieken centraal staan.

Ierland is geselecteerd vanwege de prominente rol die het land speelt in de Europese regulering van online platforms, met Coimisiún na Meán als belangrijke toezichthouder binnen het kader van de Digital Services Act. Frankrijk combineert verschillende typen aanpakken met zowel een informatiegerichte benadering (VIGINUM) als een duidelijke inbedding van handhaving via PHAROS en het PNLH. Duitsland is opgenomen vanwege de combinatie van technologische en juridische benaderingen, met enerzijds KI4Demokratie als voorbeeld van geavanceerde analyse van het online discours, en anderzijds de landelijke actiedagen tegen strafbare haatposts als schakel in de strafrechtelijke handhavingsketen.

3.2 Opzet van de landenhoofdstukken

De verdere verkenning van de geselecteerde aanpakken is in de eerste plaats uitgevoerd door middel van een uitgebreide documentanalyse. Voor alle aanpakken is gebruikgemaakt van publiek beschikbare bronnen, waaronder wet- en regelgeving, beleidsdocumenten, rapporten van toezichthouders, parlementaire stukken en relevante wetenschappelijke en journalistieke publicaties. Deze bronnen zijn systematisch geanalyseerd met het oog op de institutionele inrichting, de juridische kaders en de praktische werking van de beschreven aanpakken.

Voor het merendeel van de landen konden de oorspronkelijke documenten worden geraadpleegd in het Engels, Duits of Frans. Voor Zweden waren veel relevante stukken eveneens in het Engels beschikbaar, maar een deel van de literatuur – voornamelijk de grijze – was er uitsluitend in het Zweeds. Deze bronnen zijn gebruikt ter ondersteuning van de contextbeschrijving, maar bevindingen eruit zijn alleen opgenomen wanneer zij konden worden bevestigd in Engelstalige of anderszins toegankelijke bronnen.

De landenhoofdstukken zijn opgebouwd volgens een vaste structuur. Elk hoofdstuk begint met een beschrijving van de institutionele inrichting van de openbare orde en veiligheid in het betreffende land. Daarbij wordt ingegaan op de verdeling van verantwoordelijkheden tussen bestuur, politie en eventuele toezichthouders, evenals op de formele gezagsverhoudingen. Vervolgens wordt een beknopte schets gegeven van relevante incidenten en recente casuïstiek. Deze beschrijving dient niet als uitputtend overzicht, maar als illustratie van de wijze waarop online aanjaging van ordeverstoringen zich in het betreffende land manifesteert en van de context waarbinnen de geselecteerde aanpakken functioneren. Daarna worden de belangrijkste juridische en beleidsmatige kaders besproken die richtinggevend zijn voor het optreden bij (online aangejaagde) ordeverstoringen. Hierbij wordt aandacht besteed aan zowel bevoegdheden als aan de grenzen die daaruit voortvloeien, bijvoorbeeld op het terrein van grondrechten, privacy en bevoegdheidsafbakening (zie ook: Winter et al., 2025).

Tot slot beschrijft elk hoofdstuk één of meer geselecteerde aanpakken. Daarbij wordt ingegaan op de inhoud van de aanpak, de betrokken actoren en hun verantwoordelijkheden en bevoegdheden, evenals op beschikbare praktijkervaringen. De nadruk ligt op het feitelijke functioneren van de aanpakken in de praktijk. Omdat een deel van de aanpakken relatief recent is en nog beperkt is geëvalueerd, zijn aanvullende interviews uitgevoerd om dit beeld waar mogelijk te verdiepen.

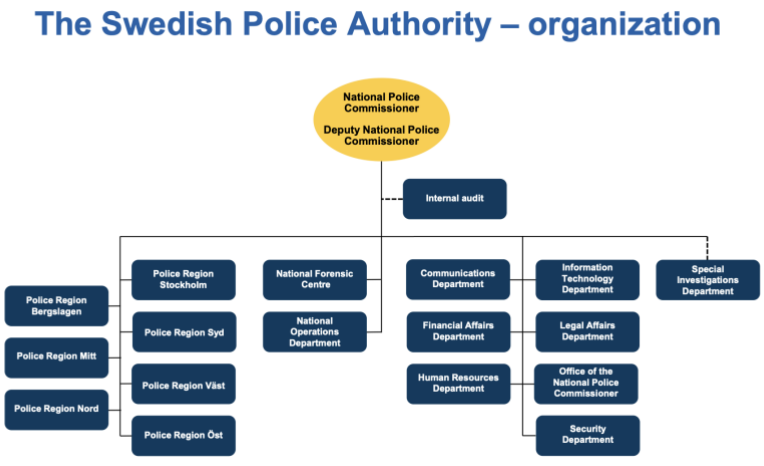
4 Zweden

De verantwoordelijkheid voor het tegengaan van OAOV ligt in Zweden primair bij de politie. De organisatie van de politie - inclusief die van de inlichtingenfunctie - kent grote overeenkomsten met die in Nederland. De Zweedse politie is echter autonoom in de manier waarop haar functie uitoefent: er is geen sprake van 'ondergeschiktheid aan het bevoegd gezag' zoals in Nederland. In 2022 leerde de Zweedse politie bij de zogenaamde Paasrellen (zie Tabel 1) een pijnlijke les waar het gaat om het voorzien en beheersen van OAOV. Naar aanleiding daarvan wordt gewerkt aan verbetering op meerdere fronten. De revitalisering van het concept van *total defence,* met daarin een belangrijke rol voor het zogenaamde *Psychological Defence Agency* lijkt voor de Nederlandse situatie echter wellicht het meest tot de verbeelding te spreken.

4.1 Algemeen kader handhaving Openbare Orde en veiligheid

De verantwoordelijkheid voor de handhaving van de openbare orde in Zweden ligt primair bij de nationale politie, de *Polismyndigheten,* door die organisatie zelf in het Engels aangeduid als de *Swedish Police Authority* (Polisen n.d.). De Zweedse politie oefent haar taal en functie uit binnen de kaders van de Zweedse politiewet 1984 (Riksdag 2025), maar zeker ook binnen de kaders van een aantal specifieke wetten waarin waarborgen voor burgerlijke vrijheden zijn vastgelegd, zoals de vrijheid van expressie, de persvrijheid, of het recht op demonstratie (Ministry of Justice 2023).

In 2015, op vrijwel hetzelfde moment als dat in Nederland gebeurde, werd de Zweedse politie gevormd door een samenvoeging van de tot dan toe bestaande lokale of regionale politiekorpsen tot één nationale politie (Uhnoo and Hansen Löfstrand 2018). Door de oogharen bezien heeft de ook de structuur van de daarbij gevormde nationale organisatie sindsdien veel weg van die van de Nederlandse politie, met (7) regionale eenheden, onderverdeeld in (25) districten en (95) lokale eenheden, ondersteund door (7) landelijke diensten voor uiteenlopende vormen van ondersteuning en specialistische diensten (Police n.d.).



Figuur :1 Organisatiestructuur Zweedse politie, zoals weergegeven op haar website Polisen.se.

De Zweedse politie oefent haar taak en functie op het gebied van de ordehandhaving autonoom uit, bewust op afstand gezet van bestuur en politiek. Zweden kent drie bestuurslagen: het landelijke niveau, het regionale (met 21 'counties' of *län*) en het lokale (met 290 gemeenten of *kommuner*) (Government Offices of Sweden 2025). Op lokaal niveau kiest de gemeenteraad steeds voor één jaar een lid dat als voorzitter van de gemeente fungeert (Cachet et al. 2002; Government Offices of Sweden n.d.). Deze voorzitter heeft niet het gezag over de politie zoals dit in Nederland bij de burgemeester is belegd, noch andere met de Nederlandse burgemeester vergelijkbare bevoegdheden ter beheersing van de openbare orde. Dat betekent bijvoorbeeld ook dat het de politie zelf is die vergunning ('permit') voor demonstraties verleent, getoetst aan criteria voor een ordelijk of beheersbaar verloop[4].

Voor de handhaving van de openbare orde bij grootschalige evenementen of ongeregeldheden beschikken de Zweedse politie-eenheden onder meer over mobiele interventieteams. Die kunnen worden ingezet bij grootschalige evenementen, demonstraties of ordeverstoringen. Net als bij de Nederlandse Mobiele Eenheid zijn dit geen fulltime 'rellen-eenheden', maar worden deze teams op het moment dat ze nodig zijn samengesteld uit reguliere politiemensen die aanvullend getraind en uitgerust zijn. Ook wordt gebruik gemaakt van *dialogue policing*, een werkwijze die sterk overeenkomt met de werkwijze van de Nederlandse Netwerkeenheid (eerder Vredeseenheid) en mogelijk zelfs daarvan is overgenomen. Wederom net als in Nederland is de inlichtingenfunctie met name belegd op districts- en eenheidsniveau. Waar nodig worden de eenheden – ook waar het gaat om inlichtingen – ondersteund door een landelijke eenheid, (met name) de landelijke *Nationell Operativa Avdelingen* (NOA) (Police n.d.; Homrighausen, 2024).

4.2 OAOV: recente casuïstiek in Zweden

Uit zowel de gesprekken als de literatuur komt naar voren dat Zweden deze eeuw ruwweg eenmaal per decennium grootschalige ongeregeldheden kende die de samenleving schokten en de politie deden nadenken over de manier waarop ze adequater het hoofd konden worden geboden.

In 2001 haalde Zweden het wereldnieuws met grootschalige en gewelddadige rellen rond de EU-top in Gotenburg. Bijna zeventig mensen raakten daarbij gewond, onder wie tien politiemensen. Drie betogers werden door politiekogels getroffen. Naar aanleiding van de rellen herzag de Zweedse politie haar strategieën in de omgang met grootschalige protesten. Dat leidde in 2002 onder meer tot de introductie van hiervoor al genoemde 'dialoogagenten', een werkwijze die opvallend veel lijkt op de werkwijze die de Amsterdamse politie bij de Eurotop van 1997 introduceerde, en die bekend zou worden als de Vredeseenheid (nu: Netwerkeenheid) (Amnesty International 2013; Vugts 2025). In de scan van de literatuur die we voor dit onderzoek verzorgden, komen we niet of nauwelijks verwijzingen tegen naar een *online dimensie* van deze ongeregeldheden[5]. Dat veranderde in later jaren echter.

[4] https://polisen.se/en/the-swedish-police/demonstrations---questions-and-answers

[5] De protesten in Gotenburg brachten demonstranten of activisten bijeen uit diverse Europese landen; het laat zich vermoeden zij tevoren (ook) met elkaar contact hadden via de online communicatievormen die destijds al bestonden, zoals email, instant messaging of internetforums. Wij hebben hier in het kader van deze inventarisatie niet verder naar gezocht.

De eerste (grootschalige) ongeregeldheden in Zweden waarin wél gesproken wordt van een dergelijke dimensie zijn de ongeregeldheden in Stockholm van 2013 (Jarynowski en Rostami, 2013). Die deden zich voor in Husby, een buitenwijk van Stockholm met een relatief hoog aantal immigranten. De ongeregeldheden braken uit nadat een politieke actiegroep uit deze wijk in een blogpost opriep tot protest tegen politiegeweld, naar aanleiding van het neerschieten van een oudere man met een mes. De (heftige en grootschalige) ongeregeldheden duurden meerdere dagen (Evans, 2013; Van Rijsingen en Bomers, 2013; Schierup et al., 2014; Sveriges Radio, 2014).

Weer zo'n tien jaar later (in de periode 2020-2023) deden zich bij herhaling grootschalige ongeregeldheden voor, die direct of indirect werden getriggerd door Koran-verbrandingen door een (Deense) extreemrechtse politicus (BBC, 2020; Toft, 2024). De zogenaamde Paasrellen (*Påskuppploppen*) van april 2022, met ongeregeldheden gedurende meerdere dagen en in meerdere Zweede steden, waren hiervan het heftigste voorbeeld. Bij deze ongeregeldheden raakte een groot aantal politiemensen gewond. In meerdere gevallen zagen politiemensen zich genoodzaakt het vuurwapen te gebruiken, ook om ter zelfverdediging gericht te schieten (Al Jazeera, 2022; Naber, 2022).

Deze rellen hadden in meerdere opzichten een online dimensie. De Zweedse politie vermoedde bijvoorbeeld dat bij de ongeregeldheden criminele bendes betrokken waren, die jongeren via Telegram ronselden voor deelname en er vooral op uit zouden zijn geweest de politie te treffen (Associated Press, 2022; Naber, 2022). Ook waren er nadrukkelijk signalen dat statelijke actoren bij het stimuleren van onrust in de betrokken doelgroepen betrokken waren (Al Jazeera 2022; APNews, 2023; Swedish Ministry of Defence, 2023).

4.3 Kaders voor aanpak van OAOV

Uit de geraadpleegde bronnen blijkt dat de hiervoor beschreven OAOV in Zweden grotendeels zijn aangepakt binnen bestaande structuren voor openbare orde en veiligheid. Voor de online dimensie werden lokale en regionale politie-eenheden ondersteund door de landelijke operationele eenheid *Nationella Operativa Avdelningen* (NOA), die beschikt over aanvullende monitoring- en inlichtingencapaciteit. Tegen deze achtergrond vallen enkele aspecten van de Zweedse aanpak in het bijzonder op.

Evaluatie Påskuppploppen (Paasrellen)

Meteen na de Påskuppploppen drong een Zweedse politievakbond aan op een onafhankelijke evaluatie van het politieoptreden tijdens deze rellen (SverigesRadio, 2022). Nog datzelfde jaar vond inderdaad zo'n evaluatie plaats (Hagström, 2022), maar die lijkt niet geheel boven twijfel verheven. Knutsson en Holgersson (2023) bijvoorbeeld merken op dat de evaluatie onvoldoende onafhankelijk was, en dat vraagtekens kunnen worden geplaatst bij de gebruikte methoden. Ook verschenen andere studies over de manier waarop de betreffende rellen het hoofd was geboden, inclusief de inlichtingenfunctie van de politie rond deze rellen en de verbeteringen die hierop mogelijk zijn. Homrighausen (2024)[6] constateert op basis van een synthese van eerdere onderzoeken van de Paasrellen dat vrijwel elke fase van de inlichtingencyclus rond deze rellen tekortkomingen kende. In

[6] Let op: dit betreft een studie in de Zweedse taal, die wij daarom eerst met behulp van AI hebben samengevat. We hebben de zo verworven inzichten vervolgens gecheckt in een interview met de auteur, en ze bezien op hun implicaties voor de Zweedse politie in de toekomst.

het denken op strategisch niveau kwam het risico op zodanig grote ongeregeldheden eenvoudigweg niet voor. Signalen die er in de aanloop naar de Paasrellen op wezen werden onvoldoende in de analyses meegenomen, mede doordat zij ook te weinig in de (sociale) context van dat moment werden gezien. Nationale en regionale inlichtingen sloten niet adequaat op elkaar aan. Tot slot bereikte inlichtingen de besluitvormers soms pas nadat operationele beslissingen al genomen waren.

Verbeteringen

Sinds de Paasrellen werkt de Zweedse politie aan verbeteringen om de op uiteenlopende vlakken geleerde lessen in praktijk te brengen. Ook op het gebied van intelligence, zo stelt Homrighausen,[7] die daaraan toevoegt dat zoiets in zo'n grote organisatie relatief langzaam gaat. Een andere respondent voegt daaraan toe dat de Zweedse politie, mede door politieke druk, al langere tijd bezig is met een omvangrijke uitbreidingsoperatie. Daardoor moet de personele capaciteit met zo'n 50% groeien.

De Zweedse politie wilde ons geen informatie verstrekken over de wijze waarop zij haar inlichtingenfunctie vervult waar het gaat om online informatie en communicatie. Wel liet de communicatieafdeling weten dat de politie in Zweden geen bijzondere bevoegdheden kent waar het gaat om het verwijderen van als schadelijk beschouwde content op digitale platforms.

"The police only send requests to remove contents that are considered illegal. We send so-called referrals to the platforms. This means that we send content that we consider to be in violation of Swedish law to the platform and ask them to review the content against their terms of use. The decision lies with the platforms whether they intend to remove the post or not. In 2/3 of the cases the platform takes action to remove the content. This process is based on cooperation and there is therefore nothing we can do if the platform does not want to take action. Examples of contents that can be considered to be in violation of Swedish law: fraudulent websites or posts, drug sales, illegal posts or accounts on social media, terror related material on websites or social platforms." (uit: mailwisseling met Swedish Police Authority, maart 2026)

Wel wijst de website van het Zweedse ministerie van Justitie op een wetsvoorstel dat stapsgewijs in werking zou moeten treden, en dat de Zweedse politie niet alleen de bevoegdheid zou geven digitale platforms te bevelen terroristische content onmiddellijk te verwijderen, maar ook de bevoegdheid om aanbieders boetes op te leggen wanneer zij daar niet aan voldoen. Daarnaast zou de wet de informatie-uitwisseling tussen politie en andere autoriteiten, waaronder de Zweedse veiligheidsdienst, moeten vergemakkelijken (Ministry of Justice, 2023).

Naast deze juridische ontwikkelingen heeft Zweden in 2022 het *Psychological Defence Agency* opgericht. Deze organisatie speelt een belangrijke rol bij het signaleren en tegengaan van buitenlandse informatiebeïnvloeding en desinformatiecampagnes van statelijke actoren. Dergelijke campagnes hebben de afgelopen jaren ook invloed gehad op OAOV in Zweden. In de volgende paragraaf gaan we nader in op de taken en werkwijze van het Psychological Defence Agency.

[7] Die na zijn studie ook korte tijd als *OSINT-operator* bij de politie werkzaam was

4.4 Aanpak: Psychological Defence Agency

In de eerste fase van dit onderzoek werden twee Zweedse 'aanpakken' aangewezen als mogelijk inspirerend voor de Nederlandse aanpak van OAOV: de *Nationell Operativa Avdelingen* (NOA) en de *Myndigheten för psykologiskt försvar,* in het Engels *Psychological Defence Agency* (PDA) geheten[8]. Wij zullen die laatste aanduiding volgen.

Nu we in deze tweede fase meer verdiepend naar de Zweedse werkwijze en daarbij betrokken organisaties hebben gekeken, lijkt de NOA vooralsnog[9] minder inspiratie te bieden dan gedacht. De activiteiten van deze landelijke politie-eenheid (en ook haar plaats in de politieorganisatie) vertonen grote overeenkomsten met die van de Landelijke Eenheid (inmiddels Eenheden) van de Nederlandse politie. Wij besteden daarom aan deze eenheid verder geen aandacht.

Dat geldt echter zeker niet voor de tweede aanpak: het Psychological Defence Agency. Bij het voorkomen en beheersen van OAOV is het tegengaan van desinformatie – zoals ook uit de hiervoor beschreven casussen blijkt – een belangrijk element. En juist daarop is het *Psychological Defence Agency* gericht. De organisatie kent een doordachte, brede benadering, en richt zich niet alleen op het tegengaan van desinformatie zelf, maar juist ook op de impact en doorwerking van die desinformatie. Niet voor niets werd het PDA door sprekers op *Disinfo 2025*[10] – samen met het Franse Viginum – betiteld als *best of class* in Europa (eigen aantekeningen auteur).

Missie en taak van het PDA

Het is de taak van het PDA om de psychologische weerbaarheid van de Zweedse samenleving tegen buitenlandse beïnvloeding te versterken. Het PDA is daarmee vooral gericht op *Foreign Information Manipulation and Interference (*FIMI), en helpt overheid, bedrijfsleven, maatschappelijke organisaties en de bevolking zich daartegen weerbaar te zijn (Government Offices of Sweden, n.d.). Het PDA doet dit door middel van kennisontwikkeling, kennisbevordering en het verzorgen van training en oefeningen. Een tweede component van zijn taak is echter ook het voorkomen, signaleren, analyseren en zo nodig *counteren* van opzettelijk desinformatie van buitenlandse actoren (Kozlowski en Tofvesson, 2024). Het PDA heeft ook als taak de Zweedse samenleving voor te bereiden op daadwerkelijke oorlog en de psychologische oorlogvoering die daarmee gepaard kan gaan. Het tegengaan van (desinformatie van) binnenlandse actoren behoort nadrukkelijk *niet* tot het mandaat van het PDA (Suliman, 2022).

Aanleiding van de oprichting

Van Vark (2025) beschrijft de instelling van het PDA binnen de revitalisering van de Zweedse strategie van *total defence.* Deze verdedigingsstrategie ontstond in de Tweede Wereldoorlog, toen Zweden tot de conclusie kwam dat het land voor haar verdediging niet langer kon vertrouwen op louter *militaire* defensie, maar dat defensie als het ware moet worden 'ingebakken' in de samenleving als geheel. Zo ontstond een concept van *total defence,* met vier kernelementen*: military defence, economic defence, psychological defence* en *civil defence.* Het concept bleef lang

[8] https://mpf.se/psychological-defence-agency

[9] Wanneer uit de verdiepende interviews blijkt dat de aanpak van de NOA toch substantieel afwijkt van wat wij in Nederland gewend zijn, zullen wij dit in de definitieve versie van dit rapport natuurlijk melden.

[10] Het Europese congres over (het tegengaan van) desinformatie van september 2025 in Ljubljana.

leidend in het Zweedse verdedigingsdenken, tot aan het begin van deze eeuw de verdediging tegen externe dreigingen als minder urgent werd gezien.

De geopolitieke veranderingen van de afgelopen jaren en – met name – de ervaren toenemende dreiging van Rusland brachten het belang van een afdoende defensie tegen uiteenlopende – ook hybride – dreigingen weer terug op de agenda. Dat leidde tot een revitalisering van het *total defence* concept. Vanaf 2015 werd Zweden ook geconfronteerd met een sterke toename van desinformatie vanuit – op dat moment – vooral Rusland, gericht op het zaaien van onrust. Daarbij werden narratieven gebruikt die onder de Zweedse bevolking onrust moesten veroorzaken over immigratie, waarbij een sterk verband werd gesuggereerd met criminaliteit, terrorisme en publiek ongenoegen. Ook waren de narratieven gericht op het ondergraven van het publieke vertrouwen in de overheid. Het vermoeden ontstond daarbij dat door binnenlandse conflicten aan te jagen en het vertrouwen binnen de samenleving te laten afnemen (Kozlowski and Tofvesson, 2024) ook een voedingsbodem werd geschapen voor een aanval op Zweden. Deze ontwikkelingen bij elkaar leidde in 2022 tot de oprichting van het PDA.

Werkwijze

Het PDA werkt op basis van theoretische grondslagen, die zijn vertaald in vier praktische kernpunten: weerbaarheid, dreigingsdetectie, afschrikking en strategische communicatie (Pamment en Isaksson, 2024). In de werkzaamheden van het PDA zijn al deze punten terug te zien: van het versterken van weerbaarheid door kennisdisseminatie (via bijvoorbeeld handboeken en training), via dreigingsdetectie en afschrikking door realtime analyse en intelligence, tot nationale en internationale samenwerking met uiteenlopende partners (Karlsson et al., 2026; Oksanen, 2023; Pamment en Tsurtsuma, 2025; Psychological Defence Agency, 2023; Ranstorp en Ahlerup, 2024).

Veel aandacht wordt besteed aan verdere kennisontwikkeling en het op basis daarvan ontwikkelen en aanscherpen van effectieve werkwijzen. Daarvoor volgt het PDA zelf de internationale state-of-the-art waar het gaat om (het tegengaan van) FIMI, maar financiert het PDA ook het – eveneens in 2022 opgerichte – multidisciplinaire *Psychological Defence Research Institute* aan de Universiteit van Lund (Kozlowski en Tofvesson, 2024; Lund University n.d.). Het werk van dit instituut resulteert niet alleen in wetenschappelijke publicaties, maar ook in toepassingsgerichte publicaties voor beleid en bestuur, waarvan een aanmerkelijk deel ook in het Engels beschikbaar is (Pamment et al., 2019, 2024; Pamment et al., 2023; Pamment en Isaksson, 2024)

Organisatie

Het PDA ressorteert onder het Zweedse ministerie van Defensie, dat ook een aparte minister voor civiele defensie kent, in lijn met het hierboven beschreven concept van total defence (Kozlowski en Tofvesson, 2024). De organisatie kent een relatief beperkte omvang van (anno 2024) zo'n 60 medewerkers, bestaande uit juristen, onderzoekers, analisten en communicatiemedewerkers, verdeeld over drie afdelingen: een operationele afdeling, een afdeling voor *capacity building* en een beheers- en bestuursafdeling (Government Offices of Sweden, n.d.; Kozlowski en Tofvesson, 2024).

Bevindingen ten aanzien van het PDA

Wij hebben binnen het bestek van deze inventarisatie nog niet kunnen beoordelen in hoeverre de activiteiten van het PDA al aantoonbare effecten hebben op het daadwerkelijk voorkomen en tegengaan van (de impact van) desinformatie, en daarmee mogelijk ook van OAOV. Van Vark (2025) beschrijft het in een korte telefonische toelichting op haar studie als 'een inspirerend voorbeeld' van hoe psychologische defensie kan worden vormgegeven, maar benadrukt daarbij dat het veldwerk voor haar studie plaatsvond in 2021-2022, toen de organisatie net werd opgericht. Er van uitgaande dat desinformatie met regelmaat een factor is in het ontstaan van OAOV, lijkt het in

elk geval conceptueel een interessant initiatief in – wat je zou kunnen noemen - de tweede lijns-verdediging tegen OAOV. Het sluit ook naadloos aan op de manier waarop wij volgens Van der Linden (2023) onze samenleving weerbaar kunnen maken tegen mis- en desinformatie. Sowieso lijkt Zweden een aansprekend voorbeeld waar het gaat om het vormgeven van de weerbaarheid die ook in Nederland nu zo hoog op de agenda is gekomen. Dus óók – maar niet alleen – waar het gaat om het tegengaan van desinformatie en OAOV.

5 Verenigd Koninkrijk

5.1 Algemeen kader handhaving Openbare Orde en veiligheid

De politie in Engeland & Wales bestaat uit 43 lokaal georganiseerde korpsen, aangevuld met enkele specialistische diensten zoals de *British Transport Police* en de *Civil Nuclear Constabulary*[11]. Deze 43 korpsen zijn geografisch afgebakende autonome organisaties, met ieder een eigen *chief constable* (operationele leiding) en democratisch toezicht via gekozen *Police and Crime Commissioners* (PCC's)[12]. Anders dan in Nederland is er dus geen nationaal politiekorps dat regionale eenheden hiërarchisch aanstuurt.

Veel lokale politiekorpsen beschikken over eigen public-order-units en onderhouden contacten met lokale autoriteiten en *Community Safety Partnerships* (CSP's). CSP's brengen politie, gemeenten, brandweer, gezondheidsdiensten, reclassering en (soms) maatschappelijke organisaties samen om criminaliteit, overlast, antisociaal gedrag en wanorde integraal aan te pakken[13]. Zij vormen daarmee de basis voor een community-georiënteerde veiligheidsbenadering, en spelen een rol bij preventie, vroegsignalering en interventie, inclusief situaties waarin (online) spanningen of oproepen tot geweld een risico vormen (Clark, 2023).

Sinds 2015 fungeert de *National Police Chiefs' Council* (NPCC) als het nationale coördinatieplatform voor de *chief constables*[14]. De NPCC heeft geen hiërarchische aansturingsbevoegdheid over de 43 korpsen (zoals de Nationale Politie in Nederland), maar faciliteert strategische en operationele afstemming en organiseert samenwerking rond nationale dreigingen, terrorisme, georganiseerde criminaliteit en grootschalige (online aangejaagde) ordeverstoringen. Wanneer meerdere korpsen gezamenlijk moeten optreden, zoals bij massaprotesten of landelijke incidenten, coördineert de NPCC de onderlinge bijstand[15].

De verantwoordelijkheid voor het operationele optreden bij openbare-ordeproblemen ligt in Engeland en Wales dus bij de chief constable van het betrokken politiekorps. Democratisch toezicht op de politie wordt uitgeoefend door de gekozen Police and Crime Commissioners, die strategische prioriteiten vaststellen maar geen operationele leidinggeven. Anders dan in Nederland bestaat er geen bestuurslaag die vergelijkbaar is met de veiligheidsregio: coördinatie bij grootschalige

[11] https://www.college.police.uk/app/public-order-public-safety/legal-framework-and-legislation

[12] https://www.gov.uk/police-and-crime-commissioners

[13] https://www.gov.uk/government/publications/community-safety-partnerships/community-safety-partnerships

[14] Hoewel chief constables, net als Nederlandse eenheidschefs, verantwoordelijk zijn voor een geografisch afgebakend gebied, verschillen hun institutionele posities wezenlijk. Chief constables staan aan het hoofd van juridisch en organisatorisch zelfstandige politiekorpsen en beschikken over volledige operationele autonomie. Nederlandse eenheidschefs daarentegen geven leiding aan regionale onderdelen binnen één nationale politieorganisatie, en zijn hiërarchisch ondergeschikt aan de landelijke korpschef. https://www.legislation.gov.uk/ukpga/2011/13/contents

[15] https://www.npcc.police.uk/About-Us/about-us/

incidenten verloopt primair via samenwerking tussen politiekorpsen en nationale afstemming via de NPCC.

5.2 OAOV: recente casuïstiek in het VK

Het Verenigd Koninkrijk heeft geregeld te maken met verstoringen van de openbare orde, variërend van grootschalige protesten tot spontane samenkomsten die in korte tijd uit de hand kunnen lopen. Om inzicht te krijgen in hoe online dynamiek kan bijdragen aan verstoringen van de openbare orde, bespreken we hieronder enkele recente incidenten uit het Verenigd Koninkrijk. Deze casussen zijn niet geselecteerd om een compleet of chronologisch overzicht te bieden, maar dienen als illustraties van verschillende manieren waarop online mobilisatie en informatieverspreiding een rol kunnen spelen bij ordeverstoringen. In sommige gevallen gaat het om online oproepen die leiden tot fysieke samenkomsten, in andere om situaties waarin online geruchten of desinformatie bijdragen aan spanningen die zich vervolgens offline manifesteren. De voorbeelden zijn gekozen op basis van zichtbaarheid in publieke berichtgeving en beleidsreacties, en dienen primair om te laten zien hoe de interactie tussen online en offline dynamieken in de praktijk kan verlopen. Hoewel de aanleiding, vorm en betrokken groepen per incident verschillen, tekenen zich verschillende rode lijnen af.

Ten eerste laat de analyse incidenten zien die door geruchten en desinformatie zijn aangejaagd. Deze mobilisaties vormen zich vaak rond thema's die gerelateerd zijn aan identiteit, waarbij asiel en migratie vaak als trigger fungeren. Bij incidenten als in Southport[16], Knowsley[17] en Erskine[18] bijvoorbeeld werd morele verontwaardiging online gevoed door geruchten, misleidende video's en complotnarratieven waarin overheden bijvoorbeeld werden verdacht van het achterhouden van informatie. Een dergelijke online dynamiek kan leiden tot mobilisatie waarbij sociale spanningen hoog oplopen, doordat bepaalde groepen als probleem of bedreiging worden geframed (Verma et al., 2025).

Daarnaast zien we een tweede, relatief nieuw patroon bij opportunistische of door influencers aangejaagde massabijeenkomsten, zoals de TikTok-rellen op Oxford Street[19] en Carnaby Street[20]. Hier is geen sprake van een politiek motief, maar van laagdrempelige online prikkels die door algoritmische versterking grote aantallen jongeren op korte termijn mobiliseren. De offline verstoring ontstaat vooral door massaliteit, FOMO-effecten en een menging van relationele en instrumentele deelnemers. Dit type ordeverstoring illustreert dat online dynamiek zonder ideologische inhoud toch substantiële impact op de openbare orde kan hebben.

[16] https://www.emma.nl/artikelen/southport-revisited-wat-nederland-kan-leren-van-een-onrustige-engelse-zomer

[17] https://www.theguardian.com/uk-news/2023/feb/10/far-right-demonstrators-clash-with-police-at-liverpool-hotel-housing-asylum-seekers

[18] https://www.bbc.com/news/articles/czxyj5w5jn0o

[19] https://www.theguardian.com/uk-news/2023/aug/09/oxford-street-shoppers-locked-in-stores-amid-social-media-robbery-campaign

[20] https://www.lbc.co.uk/article/soho-riot-pop-up-streetware-poser-london-gen-z-5Hjczk6_2/

Een derde rode lijn betreft ideologisch gemotiveerde mobilisaties, zowel progressief (Black Lives Matter[21], Kill the Bill[22], Gaza-protesten[23]) als reactionair (anti-lockdown[24], anti-migratie[25]). Deze acties worden doorgaans georganiseerd via informatieve en identiteitsversterkende online netwerken. Escalatie treedt vooral op bij massaliteit, tegenprotesten of confrontaties met de politie. Ondanks hun inhoudelijke verschillen delen deze bewegingen een vergelijkbare digitale logica: online organisatie en emotionele mobilisatie vergroten het bereik, terwijl offline interacties bepalen of ordeverstoringen ontstaan.

Daarnaast vormen sport- en feestgerelateerde incidenten een eigen rode lijn. In deze gevallen spelen ideologische frames of geruchten een rol maar gaat het om bestaande groepsnormen, rivaliteit en uitgaanscultuur. Dat zien we bijvoorbeeld bij de Wembley EURO 2020-finale[26] en de terugkerende confrontaties tussen Millwall en West Ham[27].

Tot slot zien we een categorie van situatie gedreven of door paniek gevoede escalaties, zoals de *crowd risks* rondom de begrafenis van koningin Elizabeth[28] of de golf aan bommeldingen bij scholen[29]. Deze incidenten worden niet gedragen door duidelijk afgebakende groepen of motieven, maar door de snelle verspreiding van angst, waarschuwingen of ambigue informatie. In deze categorie is online communicatie geen middel tot protest, maar een trigger die de dynamiek van grote menigten direct beïnvloedt.

5.3 Kaders voor aanpak van OAOV

Het wettelijke kader voor de handhaving van de openbare orde in Engeland en Wales wordt in belangrijke mate gevormd door de *Public Order Act 1986*. Deze wet bevat bepalingen over demonstraties en openbare bijeenkomsten, en definieert onder meer de strafbare feiten *riot* (rellen), *violent disorder* (gewelddadige wanordelijkheden) en *public nuisance* (openbare overlast)[30]. Daarnaast vormen de *Police and Criminal Evidence Act 1984* (PACE) en de *Criminal Justice and Public*

[21] https://www.bbc.com/news/uk-england-53120735

[22] https://www.bigissue.com/news/activism/what-are-the-kill-the-bill-protests-police-crime-sentencing-courts-bill/

[23] https://www.theguardian.com/world/2025/oct/11/thousands-gather-london-march-lasting-peace-gaza

[24] https://www.bbc.com/news/uk-56469687

[25] https://www.theguardian.com/uk-news/2025/sep/20/anti-immigration-protesters-and-counter-protesters-clash-in-glasgow

[26] https://www.theguardian.com/football/2021/dec/03/england-fan-disorder-at-euro-2020-final-almost-led-to-deaths-review-finds

[27] https://www.theguardian.com/football/2009/aug/26/west-ham-millwall-report

[28] https://www.theguardian.com/uk-news/2022/sep/16/met-to-deploy-10000-officers-for-queens-funeral-in-biggest-ever-operation

[29] https://www.theguardian.com/education/2018/mar/19/more-than-400-schools-in-england-receive-hoax-bomb-threats

[30] https://www.legislation.gov.uk/ukpga/1986/64/contents

Order Act 1994 belangrijke grondslagen voor de bevoegdheden van politie en justitie op het terrein van opsporing, arrestatie, bewijsvergaring en de aanpak van verstoringen van de openbare orde[31].

Met de invoering van de *Police, Crime, Sentencing and Courts Act 2022* (PCSC)[32] werd het begrip *serious disruption* verruimd tot aanzienlijke verstoring van dagelijkse activiteiten, zoals belemmering van werk en dienstverlening, verstoring van transport of logistiek en – onder omstandigheden – hinderlijke geluidsoverlast. Hierdoor veranderde de juridische afbakening van situaties waarin tegen protesten kan worden opgetreden en werd het toepassingsbereik van de openbare-ordebevoegdheden verbreed[33].

Aanpakken voor OAOV

De uiteenlopende incidenten in het VK laten zien dat online aangejaagde ordeverstoring geen uniform fenomeen is, maar ontstaat uit verschillende sociale, digitale en situationele dynamieken. Tegelijkertijd hebben zij als gemeenschappelijk element dat in vrijwel alle gevallen digitale communicatie een centrale rol speelt in het ontstaan, de versnelling of de schaal van de verstoring. De casuïstiek onderstreept dat effectieve openbare-ordeaanpak in het VK niet alleen offline gericht is, maar in toenemende mate afhankelijk is van vroegtijdige signalering, analyse en beïnvloeding van online dynamiek.

Juist in deze gecombineerde online–offline context positioneren zich de twee landelijke aanpakken die in dit onderzoek centraal staan: het *National Special Operations and Intelligence Team* (NSOIT) en de *Prevent Duty Guidance*. Het NSOIT richt zich primair op de operationele kant van openbare orde en veiligheid, met een nadruk op inlichtingen, monitoring en een gecoördineerde respons op verstoringen. De Prevent Duty Guidance betreft een wettelijk verankerde aanpak binnen het Britse terrorismebeleid, die publieke en private organisaties verplicht om signalen van radicalisering vroegtijdig te herkennen en daarop te handelen. Daarmee sluit deze aanpak vooral aan bij incidenten waarin ideologische, identitaire of door desinformatie gedreven narratieven een organiserende rol spelen. In de volgende paragrafen worden deze twee aanpakken nader uiteengezet, met aandacht voor hun doelstellingen, werkwijze en relevantie voor de hierboven beschreven vormen van ordeverstoring.

5.4 Aanpak: National Special Operations and Intelligence Team (NSOIT)

Volgens de verplichte *privacy notice*[34] geeft het NSOIT leiding aan de Britse aanpak van online informatiedreigingen. Omdat mis- en desinformatie kunnen bijdragen aan verstoringen van de nationale of de openbare veiligheid, zorgt het team ervoor dat de overheid tijdig stappen kan zetten om zulke informatie aan te pakken.

[31] https://www.college.police.uk/app/public-order-public-safety/legal-framework-and-legislation

[32] https://www.legislation.gov.uk/ukpga/2022/32/contents

[33] https://netpol.org/pcsc-act-2022

[34] https://www.gov.uk/government/publications/national-security-online-information-team-privacy-notice

Volgens Birchall en Knight (2025) kent het NSOIT geen afzonderlijke wettelijke verankering of een openbaar mandaatdocument. In plaats daarvan opereert het NSOIT binnen een aantal bredere wettelijke en beleidsmatige kaders:

- De Online Safety Act (2023)[35]: deze wet verplicht sociale-mediaplatforms om risico's te beperken, waaronder risico's verbonden aan schadelijke of misleidende online informatie.
- Ofcom houdt als regulator onder de Online Safety Act wel toezicht op de naleving van wettelijke verplichtingen door platforms[36].
- De National Security Act (2023)[37]: bevat onder meer een nieuwe strafbaarstelling voor buitenlandse inmenging, waaronder door staten gesteunde desinformatie, en vormt een deel van het bredere nationale veiligheidskader.
- DSIT Media Literacy Strategy[38]: ondersteunt beleidsmaatregelen om burgers beter te beschermen tegen online informatiebedreigingen.

Praktisch is het NSOIT is ondergebracht bij het *Department for Science, Innovation and Technology* (DSIT). Het team ontstond in 2019 uit de voormalige *Counter-Disinformation Unit* (CDU), die destijds viel onder het *Department for Digital, Culture, Media and Sport* (DCMS). De transitie naar NSOIT vond plaats in een periode waarin de CDU aanzienlijke kritiek kreeg op zijn rol tijdens de COVID-19-pandemie, onder meer over de monitoring van binnenlandse kritiek. De herpositionering binnen het DSIT bracht het NSOIT dichter bij digitale beleidsontwikkeling en verder af van het mediabeleid bij DCMS[39]. Inmiddels pleiten Seger et al. (2025) ervoor om het NSOIT steviger te verankeren binnen het overheidsstelsel dat de kwaliteit, betrouwbaarheid en weerbaarheid van de publieke informatievoorziening moet beschermen. Zij vinden de huidige inrichting te weinig transparant en te versnipperd.

Het team wordt operationeel geactiveerd als op basis van een ministeriële beoordeling wordt vastgesteld dat sprake is van een *high-risk information threat*[40]. In publieke documenten wordt niet gespecificeerd welke ministers bij deze beoordeling betrokken zijn. Gezien de positionering van het NSOIT binnen het *Cabinet Office* ligt betrokkenheid van de ministers die verantwoordelijk zijn voor nationale veiligheid en binnenlandse zaken voor de hand.

[35] https://www.legislation.gov.uk/ukpga/2023/50/contents

[36] https://www.gov.uk/government/collections/online-safety-act

[37] https://www.legislation.gov.uk/ukpga/2023/32/contents/2025-07-01

[38] https://www.gov.uk/government/publications/online-media-literacy-strategy

[39] https://bigbrotherwatch.org.uk/wp-content/uploads/2024/11/BigBrotherWatch-Briefing-on-the-National-Security-Online-Information-Team.pdf

[40] https://questions-statements.parliament.uk/written-questions/detail/2025-03-03/35204

Afgezien van een zeer korte omschrijving van het NSOIT en enkele zeer algemene antwoorden op parlementaire vragen[41, 42, 43] bevatten officiële Britse overheidspagina's echter geen nadere informatie over het mandaat, de organisatie, taken of verantwoording van het team. Ook na nadere raadpleging van publieke en parlementaire bronnen blijkt deze informatie niet beschikbaar. Zo wordt ook niet duidelijk welke instantie verantwoordelijk is voor de operationele opvolging van signalen of voor eventuele contacten met online platforms. Het ontbreken van verdere informatie wordt door de Britse regering gerechtvaardigd met een beroep op *national security*, waaronder dergelijke operationele details niet openbaar worden gemaakt[41].

Southport en het NSOIT

De onrusten die zich in de zomer van 2024 in Southport voordeden, gelden inmiddels als een illustratief voorbeeld van een door sociale media aangewakkerde ordeverstoring. Binnen enkele uren na een steekincident ontstond via TikTok, X en Telegram een golf van virale desinformatie, waarbij vooral de – onjuiste – claim dat de dader een asielzoeker was grote verspreiding kreeg. Vergani et al. (2026) constateren dat vooral online berichten waarin expliciet werd opgeroepen tot mobilisatie samenhingen met de locaties waar later rellen plaatsvonden. Gebieden waar uitsluitend sprake was van algemene anti-immigratiesentimenten vertoonden deze samenhang veel minder. Na de verspreiding van onjuiste berichten over de identiteit van de dader vonden in de daaropvolgende dagen in verschillende Britse steden anti-immigratiedemonstraties en rellen plaats, waarbij onder meer moskeeën en locaties voor asielopvang werden aangevallen [44].

Deze casus is relevant omdat de Southport-rellen het type incident vertegenwoordigen dat binnen het mandaat van het NSOIT valt: een bedreiging van de publieke veiligheid die voortvloeit uit de snelle verspreiding van online mis- en disinformatie[45]. Volgens de *privacy notice*[34] en parlementaire antwoorden omvat dit mandaat het monitoren van openbaar beschikbare online informatie, het identificeren van narratieven die een risico vormen voor de publieke veiligheid en – indien nodig – het melden van schadelijke content aan sociale-mediaplatforms via hun *trusted flagger*-functie.

Hoewel er geen publieke informatie beschikbaar is waaruit blijkt of en hoe het NSOIT in de Southport-casus daadwerkelijk heeft gehandeld, kan op basis van dit mandaat worden geanalyseerd welke rol het team in een dergelijke situatie zou kunnen hebben. In een casus als Southport zou het NSOIT in elk geval verantwoordelijk zijn voor het volgen van zich snel verspreidende narratieven, het duiden van hun potentiële veiligheidsimpact en het – waar passend – onder de aandacht brengen van problematische content bij platforms, zoals ook wordt beschreven in parlementaire verwijzingen naar zogenoemde *high-risk public safety situations*.

Kumar (2025) beschrijft hoe misinformatie rondom Southport door algoritmische versterking snel een groot bereik realiseerde: volgens Kumar bereikte het dominante – onjuiste – narratief in de

[41] Https://questions-statements.parliament.uk/written-questions/detail/2024-02-19/HL2530

[42] https://questions-statements.parliament.uk/written-questions/detail/2024-02-19/HL2529

[43] https://questions-statements.parliament.uk/written-questions/detail/2025-08-29/70395

[44] https://commonslibrary.parliament.uk/policing-response-to-the-2024-summer-riots/

[45] https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru

eerste dagen na het incident circa 15,7 miljoen gebruikers op TikTok en X. Ook speelden extreemrechtse Telegramkanalen, influencers en internationaal verbonden digitale gemeenschappen een aanjagende rol. Verma et al. (2025) reconstrueerden (achteraf) een uitgebreid *web-of-influence* van extreemrechtse, xenofobe en anti-migratiekanalen dat al vóór de rellen actief was. Zij laten zien dat dit netwerk transnationaal (grensoverschrijdend) was en meerdere onderwerpen (immigratie, publieke orde, lokale misdaad) verbond, waardoor het incident in Southport een bestaand ecosysteem activeerde in plaats van een nieuw systeem te creëren.

Bevindingen ten aanzien van het NSOIT

Het NSOIT is gepositioneerd als een instrument om acute online informatiedreigingen voor de nationale en openbare veiligheid te adresseren. De beperkte transparantie over taken, werkwijze en afbakening van het team brengt risico's voor vrijheid van meningsuiting met zich mee.

Big Brother Watch (2024)[46] wijst in dat kader op twee samenhangende kritiekpunten. Ten eerste wordt gesteld dat de activiteiten van het NSOIT niet altijd strikt beperkt zijn gebleven tot het monitoren van desinformatie, maar zich mede hebben uitgestrekt tot legale politieke uitingen en vormen van *dissent*. In door Big Brother Watch geanalyseerde rapportages werden bijvoorbeeld tweets en online uitingen van politici, journalisten en activisten opgenomen, ook wanneer deze feitelijk juist en juridisch toegestaan waren. Volgens Big Brother Watch wijst dit op het risico van *mission creep*, waarbij een instrument dat formeel is gericht op het bestrijden van desinformatie in de praktijk ook (binnenlandse) meningsvorming en politiek debat kan omvatten.

Een tweede kritiekpunt betreft de mogelijke indirecte beperkingen van de vrijheid van meningsuiting die samenhangen met de *trusted flagger*-status van het NSOIT. Via deze status kan het team online content melden bij sociale-mediaplatforms, die dergelijke signalen met prioriteit behandelen. Hoewel het NSOIT zelf geen bevoegdheid heeft om content te verwijderen, kan deze werkwijze ertoe leiden dat legale uitingen sneller worden beperkt of verwijderd door platforms, zonder transparantie over de herkomst van het signaal en zonder voorafgaande rechterlijke toetsing.

Ook in de academische literatuur wordt gewezen op deze spanningen. Birchall en Knight (2025) en Seger et al. (2025) signaleren dat de institutionele inbedding van het NSOIT onvoldoende duidelijk is, onder meer doordat het team geen expliciete wettelijke verankering kent en opereert binnen een gefragmenteerd stelsel van nationale veiligheids-, desinformatie- en mediabeleidskaders. Volgens deze auteurs bemoeilijkt dit zowel de democratische verantwoording als een systematische evaluatie van proportionaliteit en effectiviteit. Zij pleiten daarom voor een explicieter wettelijk mandaat en een duidelijkere centrale positionering van het NSOIT in het bredere overheidsbeleid rond online informatiebedreigingen.

Samenvattend kan het NSOIT worden omschreven als een nationaal team dat online informatiebedreigingen monitort als deze een risico vormen voor de nationale of openbare veiligheid. Het team komt in actie na de ministeriële aanwijzing van een high-risk information threat, en analyseert vervolgens openbaar toegankelijke online informatie. Daarbij kan het NSOIT, onder meer vanuit zijn trusted flagger-rol, schadelijke content melden bij sociale-mediaplatforms.

[46] https://bigbrotherwatch.org.uk/wp-content/uploads/2024/11/BigBrotherWatch-Briefing-on-the-National-Security-Online-Information-Team.pdf

Het NSOIT beschikt niet over een afzonderlijk wettelijk mandaat of een publiek taakdocument, maar opereert binnen bredere veiligheids- en mediakaders. Over de precieze taken, werkwijze en verantwoording van het team is weinig publieke informatie beschikbaar. Dit wordt door de Britse overheid gerechtvaardigd met een beroep op nationale veiligheid. Casussen als de onrust in Southport in 2024 illustreren het type incident waarvoor het NSOIT is bedoeld: situaties waarin mis- en desinformatie zich snel online verspreiden en bijdragen aan fysieke openbare-ordeverstoringen. Tegelijkertijd wordt vanuit civiele en academische hoek gewezen op mogelijke risico's voor transparantie, democratische verantwoording en de vrijheid van meningsuiting.

5.5 Aanpak: Prevent Duty Guidance

Wat de aanpak behelst

Prevent is een programma dat zich richt op het voorkomen van mobilisatie van jongeren voor extreem gedachtegoed en radicalisering ten aanzien van alle vormen van terrorisme, waaronder zowel jihadistisch geïnspireerd terrorisme als extreemrechts terrorisme[47]. Binnen dit programma is de Prevent Duty Guidance[47] de richtlijn waarin staat hoe publieke instellingen uitvoering moeten geven aan hun plicht om dergelijke escalatieprocessen in een vroeg stadium te signaleren en te adresseren. De Prevent Duty Guidance is van toepassing op een breed scala aan publieke organisaties, waaronder onderwijsinstellingen (zoals kinderopvang, scholen en instellingen voor vervolgonderwijs), gezondheidszorginstellingen, lokale overheden en de politie[47]. Van deze organisaties wordt verwacht dat zij aantoonbaar (*due regard*) richting geven aan deze wettelijke verplichting (Blackbourn, 2025). Dit houdt in dat zij systematisch aandacht besteden aan het inschatten van risico's, hun personeel toerusten met kennis en vaardigheden om signalen te herkennen, en beschikken over duidelijke procedures voor het intern bespreken – en indien nodig doorverwijzen – van zorgen[48].

Wanneer dergelijke zorgen aanleiding geven tot verdere beoordeling, kan een verwijzing worden gedaan naar het zogeheten Channel-programma. Meldingen worden daar besproken in een lokaal Channel-panel onder leiding van de gemeente, waaraan onder meer politie, onderwijsinstellingen, zorgorganisaties en andere relevante partners deelnemen. Dit panel beoordeelt of daadwerkelijk sprake is van een risico op escalatie c.q. radicalisering. Wanneer dat het geval is, kan een ondersteuningsplan worden aangeboden dat is gericht op het verminderen van dit risico, bijvoorbeeld via mentoring, onderwijs- of zorginterventies. Deelname aan Channel is vrijwillig voor de betrokken persoon (ouders/verzorgers in het geval van minderjarigen) en heeft een preventief karakter.[49]

Juridische grondslag en positionering van de aanpak

De Prevent Duty Guidance is juridisch verankerd in de i (CTSA) 2015[50]. Deze wet verplicht zogenoemde *specified authorities* – waaronder scholen, universiteiten, zorginstellingen, lokale

[47] https://www.gov.uk/government/publications/prevent-duty-guidance/prevent-duty-guidance-for-england-and-wales-accessible

[48] https://homeofficemedia.blog.gov.uk/2023/09/07/prevent-duty-guidance-factsheet/

[49] https://assets.publishing.service.gov.uk/media/65e5a5bd3f69457ff1035fe2/14.258_HO_Prevent+Duty+Guidance_v5d_Final_Web_1_.pdf

[50] https://www.legislation.gov.uk/ukpga/2015/6/contents

overheden en andere publieke organisaties – om *due regard* te hebben en zo te voorkomen dat mensen worden aangetrokken tot ordeverstoringen die zover kunnen gaan als het plegen van aanslagen en terrorisme. Binnen het bredere beleidskader maakt Prevent deel uit van CONTEST[51], de nationale Britse strategie voor terrorismebestrijding. CONTEST kent vier pijlers – *Prevent*, *Pursue*, *Protect* en *Prepare* – waarvan prevent expliciet is gericht op vroegtijdige interventie, ondersteuning van kwetsbare personen en het versterken van weerbaarheid binnen instellingen en gemeenschappen. De Prevent Duty Guidance vormt binnen deze structuur de operationele vertaalslag van de prevent-pijler: zij verplicht organisaties om risico's te beoordelen, signalen te melden en samen te werken met gespecialiseerde partners.

Binder en Allen (2024) en Scerri (2024) laten zien dat Prevent in de praktijk functioneert als een vroegsignalerings- en voorzorgsinstrument, uitgevoerd door niet-handhavende professionals die geen opsporings- of sanctionerende bevoegdheden hebben. De aanpak is primair normatief en organisatorisch van aard en legt verantwoordelijkheden bij publieke instellingen om risico's binnen bestaande zorg- en samenwerkingsstructuren te signaleren en aan te kaarten. Overigens wordt daarbij de rol van online (in relatie tot offline) nergens expliciet.

Bevindingen ten aanzien van Prevent Duty Guidance

Verschillende wetenschappelijke onderzoeken laten zien dat de uitvoering van de Prevent Duty Guidance in de praktijk tot structurele spanningen leidt. Lee et al. (2019) geven hiervan een overzicht in een meta-analyse van empirisch onderzoek naar de Prevent Duty in scholen. Zij laten zien dat Prevent in het onderwijs werkt met impliciete normen over 'goed burgerschap', waardoor bepaalde opvattingen en groepen – met name moslimleerlingen – sneller worden gezien als risicovol. Deze dynamiek hangt samen met zowel islamofobe interpretaties van radicalisering als met de normerende rol van Britse waarden (*fundamental British values*). Deze bevinding wordt ondersteund door Dudenhoefer (2018), die laat zien dat Prevent-verwijzingen in het onderwijs onevenredig vaak betrekking hebben op moslimleerlingen. Het probleem zit daarbij niet noodzakelijk in expliciete intenties van professionals, maar in impliciete associaties tussen islam, radicalisering en risico, die door het Prevent-kader worden versterkt. Scerri (2024) sluit hierop aan door te laten zien dat leraren dit onderdeel van Prevent vaak als ongemakkelijk ervaren: zij voelen zich verantwoordelijk voor het overbrengen van waarden, maar zijn onzeker over waar onderwijs eindigt en normering of beoordeling begint.

Het ander punt dat Lee et al. (2019) identificeren, betreft de manier waarop Prevent wordt gepresenteerd als een vorm van bescherming (*safeguarding*). Dit frame sluit aan bij bestaande structuren in het onderwijs en de zorg, maar leraren en andere medewerkers worden hierdoor niet alleen verantwoordelijk voor pedagogische begeleiding, maar ook voor het signaleren en beoordelen van potentiële risico's. Lee et al. laten zien dat dit leidt tot rolvervaging en onzekerheid over professionele grenzen. Binder en Allen (2024) bevestigen dit beeld op basis van interviews met professionals: zij beschrijven hoe de open norm van *due regard* en de nadruk op vroegsignalering ruimte laat voor professionele afweging, maar ook kan leiden tot voorzichtig of defensief handelen. Zo laat een recente evaluatie van Prevent naar aanleiding van de steekpartij in Southport zien dat de afbakening van dergelijke risico's in de praktijk complex kan zijn. Anderson (2025) concludeert dat de dader driemaal bij Prevent werd aangemeld vanwege zijn fascinatie voor extreem geweld,

[51] https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023

maar telkens buiten het programma viel omdat geen duidelijke ideologische motivatie werd vastgesteld. De evaluatie beveelt daarom aan om binnen Prevent meer aandacht te besteden aan personen die een risico vormen vanwege een fascinatie voor geweld, ook wanneer een duidelijke ideologische motivatie ontbreekt.

In de literatuur wordt daarnaast gewezen op mogelijke zogeheten *chilling effects*[52] van de Prevent-aanpak. Studies laten zien dat professionals en burgers terughoudender kunnen worden in het bespreken van gevoelige onderwerpen, zoals religie of politiek, uit vrees dat uitingen als signalen van radicalisering worden geïnterpreteerd (Open Society Justice Initiative, 2016[53]; Busher et al., 2017). Dit kan leiden tot zelfcensuur en een verminderd vertrouwen in publieke instellingen, met name in onderwijs- en zorgcontexten.

Alles bij elkaar laten deze studies zien dat de toepassing van de Prevent Duty Guidance in de praktijk met verschillende uitdagingen gepaard gaat. De aanpak richt zich op een vroege fase, waarin zorgen over extreem gedachtegoed en handelen, mogelijk leidend tot escalatie en radicalisering, worden opgepakt binnen bestaande zorgstructuren en zonder handhavende bevoegdheden. Dat maakt Prevent voor scholen en andere instellingen hanteerbaar, maar betekent ook dat professionals moeten werken met open normen en lastige afwegingen. Zoals Anderson (2025) en Blackbourn(2025) laten zien, roept dit vragen op over rolverdeling, proportionaliteit en rechtsstatelijke waarborgen. De kern van de kritiek is daarmee niet dat Prevent niet werkt, maar dat het beleid in de dagelijkse praktijk spanning oproept tussen beschermen en controleren.

[52] https://delta.tudelft.nl/article/ik-ben-verdacht-gemaakt-cvb-breek-met-repressief-beleid

[53] https://www.justiceinitiative.org/uploads/f87bd3ad-50fb-42d0-95a8-54ba85dce818/eroding-trust-20161017_0.pdf

6 Ierland

6.1 Algemeen kader handhaving Openbare Orde en veiligheid

Hoewel Ierland doorgaans wordt gekenmerkt door een relatief stabiele openbare orde, is het land voor dit onderzoek interessant vanwege de institutionele positie die het inneemt in het Europese toezicht op online platforms.

Vanaf de jaren negentig van de vorige eeuw ontwikkelde Ierland zich tot een aantrekkelijke vestigingsplaats voor internationale technologiebedrijven. Volgens de *Policy Statement on Foreign Direct Investment in Ireland* (2014)[54] richt het Ierse beleid voor directe buitenlandse investeringen zich daarbij op het bevorderen van een internationaal georiënteerde en innovatieve beroepsbevolking, op systematische investeringen in onderzoek en ontwikkeling, en op het handhaven van een concurrerend fiscaal- en ondernemingsklimaat.

Als gevolg daarvan hebben de afgelopen decennia meerdere grote technologieplatforms (waaronder Google, Meta, Microsoft, Apple, Amazon, TikTok, LinkedIn, eBay, IBM, Stripe en Workday) hun Europese hoofdkantoor in Ierland gevestigd. Hierdoor bevindt Ierland zich in een bijzondere positie als het gaat om de regulering van en het toezicht op online platforms. Ierland vervult daardoor binnen de Europese Unie een formele rol als *Digital Services Coordinator* onder de *Digital Services Act* (DSA).[55].

Dat maakt Ierland een interessant land om mee te nemen in dit onderzoek naar aanpakken voor OAOV.

6.2 OAOV: recente casuïstiek in Ierland

Hoewel het eiland Ierland een lange geschiedenis van politiek geweld en ordeverstoringen kent, met name rond het conflict in Noord-Ierland (‘*The Troubles*’) (Murphy, 2023), speelden deze gebeurtenissen zich grotendeels af buiten de huidige Republiek Ierland. Daar heeft de openbare orde zich in de twintigste eeuw in het algemeen ontwikkeld binnen een relatief stabiel en vreedzaam maatschappelijk kader, waarbij grootschalig (politiek) geweld uitzonderlijk is gebleven. Wel hebben zich in de afgelopen jaren enkele kleinschaligere incidenten voorgedaan waarin online dynamieken een rol speelden. Hieronder bespreken we een aantal van deze gevallen kort.

Op 23 november 2023 ontstonden in het centrum van Dublin rellen in de nasleep van een steekincident bij een basisschool waarbij meerdere kinderen en een volwassene gewond raakten. Terwijl de politie (*An Garda Síochána*) het incident onderzocht en een verdachte aanhield, circuleerden via sociale media al snel geruchten en onjuiste informatie over de identiteit en motieven van de dader. In de loop van de namiddag en vroege avond verzamelden zich groepen

[54] https://enterprise.gov.ie/en/publications/publication-files/forfás/policy-statement-on-foreign-direct-investment-in-ireland1.pdf

[55] https://www.cnam.ie/industry-and-professionals/online-safety-framework/digital-services-act/

mensen in het stadscentrum, waarna de situatie escaleerde tot ernstige openbare ordeverstoringen. Deze rellen gingen gepaard met brandstichting, plundering en aanvallen op de politie. Honderden *Gardaí* werden ingezet om de orde te herstellen. Tientallen agenten raakten gewond en er volgden meerdere arrestaties. In verklaringen benadrukten politie en regering dat deze voor Ierland ongekende rellen geen spontaan protest tegen het steekincident zelf vormden, maar werden aangejaagd door desinformatie en opruiende online berichtgeving, waardoor bestaande spanningen ten aanzien van migratie en nationale identiteit in korte tijd omsloegen in grootschalig geweld en wanorde[56,57].

Naast de rellen in Dublin hebben zich in de afgelopen jaren meerdere kleinere openbare-ordeverstoringen en spanningen rond migratie en asielopvang voorgedaan[58,59,60]. Deze incidenten vonden onder meer plaats bij hotels of locaties die werden (of zouden worden) gebruikt voor de huisvesting van asielzoekers. In tegenstelling tot de gebeurtenissen van november 2023 waren deze incidenten doorgaans kleinschaliger van aard. Het ging meestal om tientallen tot enkele honderden demonstranten, waarbij protesten soms gepaard gingen met confrontaties met de politie, maar zelden escaleerden tot grootschalige rellen of uitgebreide materiële schade. De verstoringen waren vaak lokaal en van beperkte duur.

Een derde type ordeverstoring deed zich voor tijdens de COVID-19-pandemie in 2020 en 2021, toen in Dublin en andere steden demonstraties plaatsvonden tegen lockdownmaatregelen en ander coronabeleid. Deze protesten hadden in de kern een politiek-protestmatig karakter en deden zich over een langere periode herhaaldelijk voor. In een aantal gevallen escaleerden de demonstraties tot confrontaties met de politie, waarbij arrestaties werden verricht en sprake was van openbare-ordeverstoringen. Tegelijkertijd bleven de schaal van het geweld en de materiële schade beperkt. De ordeverstoringen in deze periode kunnen daarmee worden getypeerd als herhaald, lokaal en relatief laag-intensief, waarbij protest en mobilisatie centraal stonden en grootschalig destructief geweld geen dominant kenmerk vormde[61,62,63].

Tot slot is naast bovenstaande incidenten in Ierland ook een vorm van ordeverstoring zichtbaar, waarbij zogenoemde *direct action*-protesten worden gericht op specifieke locaties of instellingen. Daarbij betreden kleine groepen of individuen locaties, zoals apotheken, bibliotheken of opvangvoorzieningen. Medewerkers worden rechtstreeks aangesproken over bijvoorbeeld coronamaatregelen, vaccinatie of asielopvang. Vaak is het doel deze acties te filmen en de video's

[56] https://www.irishtimes.com/crime-law/2023/11/23/dublin-stabbing-attack-live-updates-three-children-injured-chief-suspect-detained/

[57] https://www.rte.ie/news/primetime/2023/1207/1420746-how-dublins-riots-developed/

[58] https://www.rte.ie/news/regional/2024/0325/1439927-roscrea-protest/

[59] https://www.theguardian.com/world/2024/nov/21/asylum-camp-tensions-newtown-mount-kennedy-ireland

[60] https://www.thejournal.ie/protest-east-wall-refugees-asylum-seekers-5926136-Nov2022/

[61] https://www.irishtimes.com/news/crime-and-law/large-garda-presence-sustained-in-dublin-for-anti-lockdown-protests-1.4512885

[62] https://www.irishtimes.com/news/ireland/irish-news/hundreds-clash-in-violent-exchanges-at-dublin-protest-1.4377808

[63] https://www.irishexaminer.com/news/politics/arid-40235723.html

online te verspreiden. Deze acties leiden echter zelden tot massale wanorde, maar kunnen wel publieke functies verstoren en vragen oproepen over politieoptreden en bescherming van de openbare orde[64].

6.3 Kaders voor aanpak van OAOV

De politiezorg in Ierland is georganiseerd binnen één nationale politiedienst, An Garda Síochána[65] (Iers voor 'Bewakers van de Vrede'). Het is een centraal aangestuurde organisatie met landelijke verantwoordelijkheid voor handhaving van de openbare orde, criminaliteitsbestrijding en openbare veiligheid. An Garda Síochána staat onder leiding van een *Garda Commissioner*. Die legt verantwoording af aan de *Minister for Justice, Home Affairs and Migration*, een gecombineerde ministerspost binnen de Ierse regering. Voor de uitvoering van politietaken is het land opgedeeld in vier regio's, die verder zijn onderverdeeld in divisies en districten, waardoor er zowel nationale coördinatie als lokale aanwezigheid is. Binnen de nationale organisatie van An Garda Síochána zijn met name de *Garda National Crime & Security Intelligence Service* en de regionale commandostructuren (in het bijzonder de *Dublin Metropolitan Region*) relevant voor de aanpak van (online aangejaagde) ordeverstoringen.

In het kader van openbare orde en veiligheid is het *National Model for Community Policing* van relevantie. Deze aanpak beschouwt community policing niet als een afzonderlijke politietaak, maar als een organisatiebrede werkwijze en gedeelde professionele cultuur. Het betreft een benadering van openbare orde en veiligheid die nadrukkelijk inzet op samenwerking, lokale verankering en proportioneel optreden, en minder op uitsluitend repressieve of technologische interventies.[66].

Naast de politie en lokale veiligheidsstructuren speelt in Ierland ook de *Coimisiún na Meán* een belangrijke rol in het bredere stelsel rond openbare orde en veiligheid. Hoewel deze toezichthouder in naam vergelijkbaar is met het Nederlandse Commissariaat voor de Media, zijn de taken en bevoegdheden van de Coimisiún na Meán aanzienlijk breder, met name op het terrein van online platforms en digitale dienstverlening.

6.4 Aanpak: Coimisiún na Meán

Opzet en oorsprong

De naam Coimisiún na *Meán* komt uit het Iers en betekent letterlijk 'Commissie voor de Media'. Deze onafhankelijke commissie werd in maart 2023 opgericht op basis van de *Online Safety and Media Regulation Act* 2022[67]. De missie van de Coimisiún na Meán is het ontwikkelen van een bloeiend, divers, creatief, veilig en vertrouwd medialandschap in Ierland[68]. Naast de ontwikkeling van een brede en diverse mediasector in Ierland en de regulering van omroepen (tv en radio) en

[64] https://www.rte.ie/news/primetime/2023/0606/1387162-direct-action-why-has-this-new-form-of-protest-suddenly-emerged/

[65] https://www.garda.ie

[66] https://www.garda.ie/en/crime-prevention/community-engagement/community-engagement-offices/national-model-of-community-policing.pdf

[67] https://www.gov.ie/en/department-of-culture-communications-and-sport/

[68] https://www.cnam.ie/about/who-we-are/

video-on-demand-diensten is de toepassing van het *Online Safety Framework* een belangrijke taak van de Coimisiún na Meán. Daarbij gaat het om toezicht op online platforms, met bijzondere aandacht voor bescherming van kinderen en bestrijding van schadelijke of illegale inhoud[69].

De oprichting van Coimisiún na Meán vloeit direct voort uit de Online Safety and Media Regulation Act 2022 (OSMR Act 2022)[70], die in maart 2023 in werking trad[67]. Deze wet werd in Ierland ingevoerd in aansluiting op Europese Digital Services Act (DSA) waarin transparantie en verantwoordelijkheid van onlineplatforms, het beschermen van fundamentele rechten van gebruikers en het voorkomen van risico's die voortkomen uit illegale of schadelijke online-inhoud op Europees niveau worden geregeld (Turillazzi et al., 2023).

De Coimisiún na Meán beoogt onder meer een kader te bieden voor online veiligheid en gebruikersbescherming, in een veranderend medialandschap waarin sociale platforms een centrale rol in de manier waarop burgers informatie ontvangen en delen. Door de vestiging van veel grote technologie- en sociale-mediabedrijven in Ierland[71] vervult het land een centrale positie in het Europese digitale toezicht, onder meer als hoofdtoezichthouder voor de toepassing van de Digital Services Act en aanverwante EU-regelgeving.[72]

De Coimisiún na Meán is daarmee de Ierse tegenhanger van het Nederlandse Commissariaat voor de Media, maar met een ruimere bevoegdheid. De Coimisiún na Meán combineert klassiek mediatoezicht met online-platformregulering en sectorontwikkeling. In Nederland is die functie verdeeld over de Autoriteit Consument & Markt (ACM) en de Autoriteit Persoonsgegevens (AP)[73]. Waar Nederland dus verschillende toezichthouders kent voor media, digitale diensten en privacy, heeft Ierland met de Coimisiún na Meán één centrale instantie die mediatoezicht en onlineplatformregulering combineert.

De bevoegdheden van de Coimisiún na Meán zijn daarbij primair regulatoir van aard en richten zich op toezicht en handhaving ten aanzien van online platforms, via onder meer aanwijzingen, instrumenten voor toezicht en bestuurlijke sancties. In de praktijk krijgt dit vorm op de volgende manieren.

Wat de Coimisiún na Meán feitelijk doet

OAOV kunnen worden versterkt door illegale of schadelijke content, door aanbevelingssystemen die polariserende of opruiende inhoud verspreiden, en door gebrekkige meld- en interventiemechanismen. De Coimisiún na Meán adresseert vanuit haar rol voor wat betreft online-veiligheid en platformtoezicht precies deze punten. Dit doet ze op verschillende manieren: Online Safety Code, DSA-toezicht en *Terrorist Content Online Regulation*.

[69] https://www.cnam.ie/about/what-we-do/

[70] https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/html

[71] https://www.euronews.com/next/2023/02/02/the-gateway-to-the-eu-why-dublin-became-a-bustling-tech-hub

[72] https://www.gov.ie/en/department-of-the-taoiseach/press-releases/updated-national-digital-strategy-2025

[73] https://www.autoriteitpersoonsgegevens.nl/en/about-the-ap/digital-services-act-dsa

Online Safety Code

De Online Safety Code[74] is een bindend nationaal reguleringsinstrument dat door de Coimisiún na Meán is vastgesteld op grond van de Online Safety and Media Regulation Act 2022, die een wijziging van de Broadcasting Act 2009 inhield. De code richt zich op in Ierland gevestigde video sharing platforms (zoals YouTube, TikTok en Instagram) en legt verplichtingen op aan de inrichting van platformprocessen en moderatiesystemen, en kijkt minder naar specifieke casussen[75].

Zo verplicht de code platforms onder meer tot het opnemen van duidelijke regels in hun *terms of service* waarin illegale inhoud en bepaalde vormen van schadelijke content expliciet worden verboden. Het gaat bijvoorbeeld om cyberpesten, racistische of xenofobe uitingen en materiaal dat zelfbeschadiging of eetstoornissen promoot, maar ook om content die aanzet tot geweld of haat en terroristische propaganda. Platforms moeten daarnaast effectieve meld- en rapportagemechanismen beschikbaar stellen waarmee gebruikers problematische content kunnen melden. Deze meldingen moeten worden opgevolgd via transparante moderatieprocedures.

Een tweede categorie verplichtingen betreft systeem- en ontwerpmaatregelen. Platforms moeten maatregelen nemen om minderjarigen te beschermen, bijvoorbeeld via leeftijdscontroles, veiligheidsinstellingen en beperkingen op bepaalde soorten content. Ook moeten zij voorzieningen bieden die gebruikers helpen om online informatie kritisch te beoordelen, bijvoorbeeld door duidelijke uitleg over moderatieregels en mediageletterdheid.

De Coimisiún na Meán vervult binnen dit systeem drie functies: regelgever, toezichthouder en handhaver. Als regelgever stelt de organisatie de Online Safety Code vast en kan zij deze aanpassen wanneer nieuwe risico's of platformpraktijken daartoe aanleiding geven. Als toezichthouder controleert de Coimisiún of platforms hun systemen daadwerkelijk zo hebben ingericht dat zij aan de code voldoen. Ook kan ze onderzoeken beginnen als er aanwijzingen zijn dat platformontwerp of moderatiepraktijken de verspreiding van schadelijke content onvoldoende beperken. Tot slot beschikt de Coimisiún na Meán over handhavingsinstrumenten. Wanneer platforms de verplichtingen uit de code niet naleven, kan de toezichthouder een formeel onderzoek instellen en corrigerende maatregelen eisen. In ernstige of aanhoudende gevallen kunnen sancties worden opgelegd, waaronder financiële boetes. Deze nationale bevoegdheden staan naast de bevoegdheden die Ierland als EU-lidstaat heeft in het kader van de Digital Services Act, waarmee aanvullende toezicht- en sanctiemogelijkheden bestaan voor grote online platforms.

DSA-toezicht

In haar rol als *Digital Services Coordinator* (DSC) is de commissie verantwoordelijk voor de nationale uitvoering en handhaving van de Digital Services Act voor in Ierland gevestigde platforms[76,77]. In die hoedanigheid fungeert zij als het primaire aanspreekpunt voor deze platforms en houdt zij toezicht op de naleving van de DSA-verplichtingen. Daarnaast wisselen Digital Services Coordinators

[74] https://www.cnam.ie/coimisiun-na-mean-adopts-final-online-safety-code/

[75] https://www.cnam.ie/app/uploads/2024/10/Coimisiun-na-Mean_Online-Safety-Code.pdf

[76] https://www.cnam.ie/industry-and-professionals/online-safety-framework/digital-services-act/

[77] https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/

informatie over mogelijke overtredingen uit wanneer een platform in één lidstaat is gevestigd, maar diensten in meerdere lidstaten aanbiedt. In zulke gevallen kunnen andere lidstaten de Coimisiún na Meán verzoeken onderzoek te doen naar of handhavingsmaatregelen te nemen tegen platforms die in Ierland gevestigd zijn[78].

Uit het jaarlijkse activiteitenrapport[79] van de Coimisiún na Meán blijkt dat de toezichthouder in 2024 vooral werkte aan de inrichting van toezicht en samenwerking onder de DSA. In dat jaar ontving de commissie 322 klachten over mogelijke schendingen van de DSA die niet leidden tot formele onderzoeken, terwijl de nadruk lag op toezicht, informatieverzoeken aan platforms en voorbereiding op verkiezingsgerelateerde risico's.

Terrorist Content Online Regulation (EU-kader).
De *Terrorist Content Online Regulation* (TCOR)[80] vormt binnen het Europese kader een specifiek en zwaar instrument, dat relevant is in situaties waarin OAOV samenhangen met terroristische dreiging. In Ierland houdt de Coimisiún na Meán toezicht op de naleving van deze verordening door platforms en kan zij sancties opleggen bij structurele niet-naleving[81].

Bevindingen ten aanzien van de Coimisiún na Meán

In Ierse parlementaire stukken en beleidsteksten wordt online content vooral besproken in relatie tot maatschappelijke spanningen, desinformatie en de bescherming van democratische processen. Met name risico's voor verkiezingsintegriteit, vertrouwen in instituties en het publieke debat krijgen aandacht, waarbij deze problematiek niet primair wordt benaderd als een strafrechtelijk vraagstuk, maar als een bredere maatschappelijke kwetsbaarheid met implicaties voor openbare orde en veiligheid[82].

Binnen dit kader wordt de Coimisiún na Meán gepositioneerd als toezichthouder en regulator van online diensten en platforms. In haar *opening statement* benadrukt de *Online Safety Commissioner* dat de taak van de commissie bestaat uit regulering, toezicht en normstelling, en niet uit opsporing of strafrechtelijke handhaving[83]. Parlementaire analyses van het *Online Safety and Media Regulation*-kader bevestigen deze rolafbakening en plaatsen het toezicht van Coimisiún na Meán

[78] https://eur-lex.europa.eu/eli/reg/2022/2065/oj

[79] https://www.cnam.ie/app/uploads/2025/04/20250319_Art-55-DSA-report_VFinal.pdf

[80] https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online_en

[81] https://www.cnam.ie/industry-and-professionals/online-safety-framework/terrorist-content-online-regulation/

[82] Joint Committee on European Union Affairs. (2024). Report on EU elections, voting rights and disinformation. Houses of the Oireachtas.
https://data.oireachtas.ie/ie/oireachtas/committee/dail/33/joint_committee_on_european_union_affairs/reports/2024/2024-05-29_report-on-eu-elections-voting-rights-and-disinformation_en.pdf

[83] Coimisiún na Meán (2025). Opening statement by the Online Safety Commissioner, Niamh Hodnett.
https://data.oireachtas.ie/ie/oireachtas/committee/dail/34/joint_committee_on_arts_media_communications_culture_and_sport/submissions/2025/2025-11-26_opening-statement-niamh-hodnett-online-safety-commissioner-coimisiun-na-mean_en.pdf

expliciet naast – en aanvullend op – bestaande strafrechtelijke en ordehandhavende instrumenten (Oireachtas Library & Research Service, 2022a)[84].

Tegelijkertijd blijkt zowel uit de stukken[83] als het interview dat we hielden dat de Coimisiún na Meán zich nog in een opbouwfase bevindt. Uit de opening statement van de Online Safety Commissioner blijkt dat verschillende toezichtstaken van de Coimisiún na Meán, waaronder de uitvoering van Online Safety Code en het toezicht in het kader van de Digital Services Act, recent zijn ingevoerd en gefaseerd worden uitgerold. Een robuuste evaluatie is niet publiek beschikbaar.

[84] Oireachtas Library & Research Service. (2022a). Insights into the Online Safety and Media Regulation Bill: Introduction to the current legal and regulatory framework. Houses of the Oireachtas. https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2022/2022-02-22_l-rs-note-insights-into-the-osmr-bill-part-1-introduction-and-background_en.pdf

7 Frankrijk

7.1 Algemeen kader handhaving Openbare Orde en veiligheid

Anders dan in Nederland, waar de burgemeester het gezag heeft over de handhaving van de openbare orde, is deze taak in Frankrijk vooral op departementaal niveau georganiseerd en is het bestuurlijk gezag belegd bij de prefect (*préfet*)[85].

Binnen de gemeentegrenzen heeft de burgemeester weliswaar gezag over politietaken op lokaal niveau[86], maar onder toezicht van de prefect. In die rol kan de burgemeester lokale voorschriften uitvaardigen en maatregelen nemen om de openbare orde *binnen* de gemeente te beschermen, zoals het reguleren van bijeenkomsten of andere activiteiten die verstoring kunnen veroorzaken. De prefect is vertegenwoordiger van de nationale regering (ministerie van Binnenlandse Zaken) in zijn departement, en beschikt over uitgebreide bevoegdheden om maatregelen te nemen ter bescherming van de openbare orde, veiligheid en rust *over de grenzen* van gemeenten heen.

Als de openbare orde in aangrenzende gemeenten wordt bedreigd of verstoord, kan de prefect de taken van individuele burgemeesters overnemen en middelen inzetten die nodig zijn om de orde te herstellen[87]. Deze rol is cruciaal bij grootschalige demonstraties, rellen of andere ernstige verstoringen van de openbare orde. In dergelijke situaties heeft de prefect het coördinerend gezag over de inzet van nationale politie- en gendarmerie-eenheden en kan die bestuurlijke maatregelen treffen om de situatie onder controle te krijgen.

Politietaken: openbare orde en rechtshandhaving
De politietaken zijn in Frankrijk duaal georganiseerd. Naast de twee nationale korpsen – de *Police nationale* en de *Gendarmerie nationale* – beschikken veel gemeenten over een eigen *Police municipale.* Deze diensten opereren naast elkaar binnen hun eigen bevoegdheden en verantwoordelijkheden.

De Police nationale is primair verantwoordelijk in stedelijke gebieden en grote steden[88]. Ze valt onder het ministerie van Binnenlandse Zaken, dat de verschillende directies binnen de Police nationale beleidsmatig aanstuurt[89]. De Police nationale heeft verder gespecialiseerde uitvoerende

[85] https://www.prefecturedepolice.interieur.gouv.fr/

[86] Art. L. 2212-2, Code général des collectivités territoriales (CGCT).

[87] Art. L. 2215-1, CGCT: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006390225/2000-04-13.

[88] https://www.police-nationale.interieur.gouv.fr/.

[89] De belangrijkste directies met betrekking tot openbare orde en veiligheid zijn de *Direction Nationale de Sécurité Publique* (DNSP), de *Direction Nationale de la Police Judiciaire* (DNPJ), en de *Direction Nationale du Renseignements Territoriales* (DNRT). Onder de DNPJ valt onder meer het *Office anti-cybercriminalité* (OFAC), het bureau waar de platforms Pharos en Thésée zijn ondergebracht. De

elite-eenheden, zoals RAID (*recherche, assistance, intervention, dissuasion*) en BRI (*brigade de recherche et d'intervention*), die vooral bedoeld zijn voor complexe interventies bij criminele of terroristische organisaties, maar eveneens in actie kunnen komen bij grootschalige en gewelddadige openbare ordeverstoringen[90]. Ordehandhaving bij demonstraties en manifestaties is primair een taak van de oproerpolitie: de CRS (*Compagnies Républicaines de Sécurité*)[91].

In landelijke gebieden en kleine gemeenten (die meer dan 95% van Frankrijk uitmaken) is de Gendarmerie nationale de verantwoordelijke politiedienst. Ze valt formeel onder het ministerie van Defensie, maar voor haar civiele politietaken staat de Gendarmerie nationale onder het gezag van het ministerie van Binnenlandse Zaken. Dat betreft bijvoorbeeld de handhaving van de openbare orde en veiligheid, inclusief preventieve taken, verkeerscontrole en noodhulp, maar ook opsporingsonderzoek[92].

Samen met de Police nationale bemenst de Gendarmerie nationale de GIGN (*Groupe d'Intervention de la Gendarmerie Nationale*). Deze elite-eenheid functioneert vanuit een centrale post en *antennes metropolitains* (op het vasteland). De FIPN (*Force d'intervention de la police nationale*) is het centrale tactische coördinatiepunt van de elite-eenheden zoals GIGN, BRI en RAID[93].

Elke gemeente groter dan 5.000 inwoners kan een lokale politiedienst (Police municipale) inrichten. Die valt zoals gezegd onder het gezag van de burgemeester van de gemeente. De Police municipale doet geen opsporingsonderzoek en heeft beperkte bevoegdheden op het vlak van beheer van de lokale orde en veiligheid, toezicht op gemeentelijke regelgeving, veiligheid in openbare ruimtes, en verkeerscontrole. Met betrekking tot misdrijven in een gemeente rapporteert de lokale politie aan de nationale diensten, die bijgeval de aanhoudingen verrichten en het opsporingsonderzoek doen[94].

Parijs

De metropool Parijs heeft een eigen organisatiestructuur, die lokale en nationale politietaken

---

DNRT is de inlichtingendienst van de Algemene Directie van de Nationale Politie (DGPN). Het is een van de vier inlichtingendiensten van het Ministerie van Binnenlandse Zaken, naast de Algemene Directie Binnenlandse Veiligheid (DGSI), de inlichtingendienst van de Parijse politieprefectuur (DRPP) en de subdirectie operationele anticipatie (SDAO) van de Nationale Gendarmerie.

[90] https://www.police-nationale.interieur.gouv.fr/nous-decouvrir/notre-organisation/organisation/raid-recherche-assistance-intervention-dissuasion; https://www.prefecturedepolice.interieur.gouv.fr/sites/default/files/Documents/drpj_bri_plaquette%20A5_2021_bd.pdf.

[91] https://www.police-nationale.interieur.gouv.fr/nous-decouvrir/notre-organisation/organisation/direction-centrale-des-compagnies-republicaines-de-securite-dccrs.

[92] https://www.gendarmerie.interieur.gouv.fr/.

[93] https://www.police-nationale.interieur.gouv.fr/nous-rejoindre/nos-metiers/policier-de-brigade-anti-gang); https://www.legifrance.gouv.fr/download/pdf/circ?id=45250; https://snpps.fr/schema-national-des-violences-urbaines/; https://snpps.fr/wp-content/uploads/2025/08/SNVU.pdf; https://internet-signalement.gouv.fr/info/renseignement/liens-utiles; https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050957705; https://anct.gouv.fr/ressources/publication-les-violences-des-jeunes-qui-la-faute; https://rm.coe.int/1680696073; https://www.defenseurdesdroits.fr/sites/default/files/2023-07/ddd-etude-desescalade-violence-20211129.pdf; https://www.centre-europeen-securite-strategie.eu/mouvements-sociaux; https://www.jean-jaures.org/publication/apres-les-emeutes-analyses-et-points-de-vue/; https://www.justice.gouv.fr/sites/default/files/2024-11/rapport_definitif_violences_urbaines.pdf

[94] https://www.policemunicipale.fr/

verbindt, onder leiding van de politieprefect[95]. Die is verantwoordelijk voor de algemene politietaken en stadsbeveiliging (demonstraties, publieke veiligheid), maar draagt ook het gezag over gespecialiseerde opsporingsdiensten, de (regionale) inlichtingendienst (DRPP), en stuurt tevens de (regionaal gevestigde) landelijke elite-eenheden aan[96].

In tegenstelling tot de meeste andere Franse steden heeft Parijs geen lokale politie. Wel is er in 2016 een civiele handhavingsdienst opgericht: de *Direction de la Prévention, Sécurité et Protection* (DPSP). Die bestaat uit handhavers en voert lokale politietaken uit. Ook kunnen deze handhavers fungeren als hulpofficieren van de gerechtelijke politie (die de opsporingsonderzoeken doet). De burgemeester van Parijs is verantwoordelijk voor preventie en naleving van regelgeving op gemeentelijk niveau, in samenwerking met de stadsdelen en de gemeenteraad. De burgemeester heeft specifieke bevoegdheden, met name voor lokale evenementen[97]. De politieprefect coördineert echter de handhaving van de openbare orde in Parijs, indien nodig met inzet van landelijke gespecialiseerde eenheden zoals de oproerpolitie (CRS).

In het kader van strafrechtelijke vervolging na incidenten (zoals aanhoudingen tijdens rellen) is het *Ministère public* (het openbaar ministerie) verantwoordelijk voor de opsporing en vervolging van strafbare feiten. Net als in Nederland is het onderdeel van de magistratuur en niet van de politie.

7.2 Recente casuïstiek: twee typen protest

Frankrijk kent een lange traditie van publieke protesten. Demonstraties, stakingen en andere vormen van collectieve actie spelen een prominente rol in het politieke en maatschappelijke leven. Met de veelbesproken rellen in de *banlieus* van de grote Franse steden in 2005 begon een goed gedocumenteerd, nieuw soort gewelddadig protest. Dat had een nieuw vocabulaire, was gericht tegen overheid en instituties, gedreven door straatpolitieke motieven die sterk wortelden in vermeende sociaaleconomische en culturele achterstand en achterstelling (Truong, 2015; Le Goaziou & Mucchielli, 2007; Kokoreff, 2008; Jobard, 2006; Lapeyronnie, 2006; Fassin & Fassin, 2006; Roché, 2006; Mauger, 2006.

In deze traditie van zogenoemde *violences urbaines*[98] pasten in 2023 ook de Nahel Merzouk-rellen (Mohammed, 2007); Oberti & Guillaume Le Gall, 2023; Epstein, Guénot & Jobard, 2023; Marlière,

[95] In Frankrijk is sinds 2012 nog een andere *Préfecture de Police*, namelijk in de regio Bouches-de-Rhône (metropool Marseille). Deze Préfecture de Police heeft functioneel gezag over de Police nationale en de Gendarmerie nationale voor de regio Bouches-de-Rhône, maar geen eigen apparaat zoals in Parijs. https://www.bouches-du-rhone.gouv.fr/; https://www.legifrance.gouv.fr/loda/id/JORFTEXT000026498577.

[96] https://www.prefecturedepolice.interieur.gouv.fr/

[97] https://www.paris.fr/pages/organigramme-de-la-ville-de-paris-2380; https://www.police-nationale.interieur.gouv.fr/nous-decouvrir/notre-organisation/organisation/direction-centrale-des-compagnies-republicaines-de-securite-dccrs

[98] De uitdrukking 'stedelijk geweld' (violences urbaines) is omstreden. Oorspronkelijk is het Franse ministerie van Binnenlandse Zaken de term voor het eerst beleidsmatig gaan gebruiken in de nasleep van de rellen in 1990 – die hun oorsprong vonden in de dood (door de politie) van Thomas Claudio, een jongere uit een buitenwijk van Lyon. Net als het woord 'rellen' (*émeutes*), was de term niet vanzelfsprekend, omdat die allerlei beelden en verschillende – al dan niet politieke – reminiscenties opriep. Na de rellen van 2005 richtte het ministerie een aparte afdeling 'Stedelijk geweld' op binnen de Algemene Inlichtingendienst. De term werd onmiskenbaar van de politie en deze politiebenadering richtte zich op jeugdgeweld en anti-institutioneel protest. Deze nieuwe terminologie om over de rellen van deze jonge opstandelingen te spreken – het merendeel van de jongeren die in 2005 werden opgepakt was tussen de 15 en 20 jaar oud – zorgde er niet alleen voor dat het beeld van een nieuwe gevaarlijke klasse werd verankerd in de collectieve verbeelding, maar bovendien werden de rellen hierdoor gedepolitiseerd en teruggebracht tot uitbarstingen van geweld en redeloze woede, zonder woordvoerder en zonder duidelijke leuzen.

2023, p. 10-13). Die vormden in de Franse politiek een keerpunt in het denken over de online kant van protest en straatgeweld[99]. Aanleiding was de dood door politiekogels van Nahel Merzouk, een 17-jarige jongen van Marokkaans-Algerijnse afkomst uit Nanterre, nadat hij een stopteken zou hebben genegeerd. Kort na het incident circuleerden videobeelden van de schietpartij op sociale media, die de officiële verklaring van de politie aantoonbaar weerlegden. Er braken protesten en gewelddadige rellen uit, vooral gericht tegen het vermeende racisme van de politie. Relschoppers staken tussen 27 juni en 5 juli 2023 in verschillende steden voertuigen in brand, plunderden winkels en vielen publieke gebouwen aan. De Franse autoriteiten zetten duizenden agenten van politie en gendarmerie in om de orde te herstellen[100].

De Nahel Merzouk-rellen hadden een sterke politieke motivatie, vanuit ervaren achterstelling en discriminatie. Ze waren gewelddadig en onmiskenbaar online aangejaagd. De snelle verspreiding van beelden en berichten via online platforms speelde een belangrijke rol in de mobilisatie van mensen en escalatie van de onrust. Sociale media fungeerden als kanaal voor het delen van video's van het incident en van daaropvolgende confrontaties met de politie, maar ook voor oproepen om zich bij protesten of rellen aan te sluiten. Die online dynamiek droeg bij aan de snelle geografische verspreiding van onrust en de mobilisatie van jongeren die zich niet via traditionele proteststructuren organiseerden.

In de landelijke politiek leidden de Nahel Merzouk-rellen tot het bewustzijn dat bij het tegengaan van violences urbaines expliciet het aspect van online aanjagen zou moeten worden aangepakt. Dat vormde de aanleiding voor wetswijzigingen en nieuwe aanpakken (Boucher, 2023; Cahn, 2023; Marlière, 2023; Sauvadet, 2023; Wacquant, 2023)[101].

Naast deze bij uitstek (groot)stedelijke protesten en rellen is de beweging van de Gele hesjes (*Gilets jaunes*) vanaf 2018 een bekend voorbeeld van een brede volksbeweging die in heel Frankrijk de openbare orde (vreedzaam) verstoorde. De beweging was niet aan politieke partijen of vakbonden gebonden, kende geen centrale leiding, verkondigde een breed en niet per se ideologisch gekleurd palet aan eisen die waren gericht aan de centrale overheid. Aanleiding voor de Gele hesjes-beweging waren de plannen voor verhoging van de brandstofprijzen. Die leidden tot een brede volksmobilisatie met demonstraties en blokkades van wegen in heel Frankrijk. De beweging was niet alleen heel zichtbaar in de media dankzij de volkse uitstraling en de spreekwoordelijke gele hesjes, maar had ook heel concrete repercussies in de wereld van transport en logistiek in Europa.

De protestbeweging *Bloquons Tout!* (Blokkeer alles!) bezette van mei tot oktober 2025 verspreid over het land belangrijke logistieke knooppunten in steden en dorpen, of sloot die af. Dat gebeurde

[99] Aan de dood van Nahel Merzouk waren soortgelijke zaken voorafgegaan. Sinds de Police nationale in 2017 de bevoegdheid kreeg om te schieten als een bestuurder met het negeren van een stopteken de passagiers of omstanders in gevaar brengt, volgden in 2020 namelijk drie dodelijke incidenten, twee in 2021 en dertien in 2022; het betrof in alle gevallen slachtoffers met een Maghrebien-achtergrond: https://web.archive.org/web/20230630083444/https://www.publicsenat.fr/actualites/politique/refus-dobtemperer-la-porte-parole-de-la-police-nationale-annonce-138-tirs-en-2022

[100] https://web.archive.org/web/20230630083444/https://www.publicsenat.fr/actualites/politique/refus-dobtemperer-la-porte-parole-de-la-police-nationale-annonce-138-tirs-en-2022

[101] https://www.interieur.gouv.fr/documentation/rapports/analyse-des-profils-et-motivations-des-delinquants-interpelles-a-loccasion-de-lepisode-de-violences.html. Christian Mouhanna, 'L'institution policière est parvenue à convaincre le gouvernement qu'il ne tient que par elle ', *Le Monde* du 26 juillet 2023 (https://www.lemonde.fr/idees/article/2023/07/26/l-institution-policiere-est-parvenue-a-convaincre-le-gouvernement-qu-il-ne-tient-que-par-elle_6183399_3232.html).

op vreedzame wijze. Aanleidingen waren onder meer de voorgenomen bezuinigingen, de schuldencrisis waarin Frankrijk zich bevond en aangekondigde ingrepen in de sociale zekerheid. Demonstranten van Bloquons Tout! plaatsten zichzelf bewust in de traditie van de Gele hesjes en de Franse 'straatpolitiek': *boycott, désobéissance et solidarité* luidde het motto (Kaulingfreks, 2013)[102]. Uit een survey bleek dat de aanhang van Bloquons Tout! ondanks de overeenkomsten met de Gele hesjes minder gefocust was op economische onzekerheid, maar zich meer richtte op het nastreven van collectieve belangen[103].

De blokkadeacties overal in Frankrijk waren niet centraal georganiseerd, maar vooral bij de landelijke verstoringen, was er wel enige vorm van aansturing merkbaar. Volgens *Le Parisien* lag de basis van Bloquons Tout! in een burgercollectief met twintig organisatoren[104]. Dat stond los van politieke partijen en vakbonden. De beweging was volledig online aangejaagd. In mei 2025 verscheen de eerste post, die werd geplaatst door de anti-overheidsgroepering *Les Essentiels France*. Dat er online manipulatie in het spel was, kan niet worden uitgesloten[105]. Online kregen deze en vergelijkbare posts enorm bijval in juli 2025, op het moment dat de regering de voorgenomen bezuinigingen publiek maakte. Op sociale media platforms als X, TikTok, Telegram en Facebook gingen de demonstranten viraal door visuals te delen met de hashtags *#10septembre2025* en *#10septembre*[106], de datum waarop een 'algemene staking' zou moeten plaatsvinden.

Het protest was niet alleen gericht tegen de overheid. Online werd mensen ook aangeraden om grote supermarktketens als Carrefour, Auchan en warenhuizen als Amazon te boycotten, geld van de grote banken te halen, en symbolische (overheids)locaties vreedzaam te bezetten. Mensen werden opgeroepen om allerlei solidariteitsinitiatieven te ontplooien (stakingskassen, buurtraden, ondersteuning van burgerlijke ongehoorzaamheid), om zo bij te dragen aan het stoppen van de kapitalistische machinerie die onzichtbare burgers vermorzelt[107]. Doel is de totale boycot: "We betalen niet meer, we consumeren niet meer, we werken niet meer, en we houden onze kinderen thuis. Onze enige macht is een totale boycot." De algemene staking van 10 september 2025 was massaal en ongeleid. De politie greep hard in, gebruikmakend van nieuwe wetgeving en regels die

[102] https://tolunacorporate.com/fr/les-francais-et-le-mouvement-du-10-septembre-2025/.

[103] https://www.jean-jaures.org/publication/bloquons-tout-tentative-de-portrait-robot-dun-mouvement-nebuleux/.

[104] https://www.leparisien.fr/politique/un-arret-total-et-illimite-du-pays-cest-quoi-ce-mouvement-qui-appelle-a-bloquer-la-france-a-partir-du-10-septembre-22-07-2025-7VCMYN5AJRHODBHYRZKEZ3PDGQ.php.

[105] De website van de beweging is intussen verwijderd, maar liet destijds een lange lijst eisen zien, die allemaal te maken hadden met herinvesteren in publieke dienstverlening en sociale zekerheid. Extreemrechtse kopstukken affilieerden zich in de beginperiode vrijwel meteen met Bloquons Tout! Daarna waren het vooral de radicaallinkse partijen die de beweging openlijk steunen, Jean-Luc Mélenchon, leider van La France insoumise, voorop.[105] Er is intussen trouwens een nieuwe website: Indignons nous.

[106] https://x.com/jon_delorraine/status/1947325628333658248.

[107] https://x.com/SarahHRakM4/status/1946316109541442024?ref_src=twsrc%5etfw%7Ctwcamp%5etweetembed%7Ctwterm%5e1946316109541442024%7Ctwgr%5edd875508b703179be737b88b1cee3d01322fd523%7Ctwcon%5es1_&ref_url=https://www.franceinfo.fr/societe/bloquons-tout-mouvement-du-10-septembre/d-un-appel-au-boycott-a-bloquons-tout-comment-le-mouvement-du-10-septembre-a-change-de-mot-d-ordre_7461475.html.

na de Merzouk-rellen van 2023 waren ingevoerd. Ook journalisten die verslag deden werden niet gespaard. Dat leidde tot een golf van protest tegen die nieuwe wetgeving (Saqué, 2025)[108].

Deze voorbeelden illustreren hoe sociale media een cruciale rol zijn gaan spelen in de Franse traditie van grootschalig en gewelddadig protest sinds de rellen in de banlieus van 2005. Ze zijn – ongeacht de motivatie en organisatiestructuur achter het protest – van betekenis voor het agenderen, mobiliseren en opschalen van ontevreden groepen burgers, waarbij digitale communicatiekanalen fungeren als infrastructuur voor het verspreiden van oproepen, narratieven en actievormen.

7.3 Kaders voor de aanpak van OAOV

De aanpak die de Franse overheid na de Nahel Merzouk-rellen (2023) en Bloquons Tout! (2025) heeft ontwikkeld om in te grijpen bij online aangejaagde ordeverstoring en het verspreiden van desinformatie verloopt grofweg langs vier governance-strategieën:

Digitaal preventiebeleid: preventieve strategieën ontwikkelen om mensen bewust te maken van de risico's van sociale media en die risico's te beperken. Gericht op zowel jongeren als volwassenen.
Bestrijding van haatzaaiende uitlatingen: maatregelen om haatdragende en haatzaaiende uitlatingen online te identificeren en te bestrijden.
Coördinatie tussen actoren: samenwerking vanuit overheden met sociale-mediaplatforms, maatschappelijke organisaties en lokale teams.
Rekening houden met structurele oorzaken: blijven inzetten op het aanpakken van de diepere oorzaken van 'stedelijk geweld', zoals armoede, sociale uitsluiting, discriminatie, een gebrek aan toekomstperspectief en ongelijkheden, op grond van de opvatting dat sociale media bestaande dynamieken versterken.

De twee laatstgenoemde strategieën zijn generiek van aard, maar leggen de basis voor een langetermijnaanpak van de voedingsbodem van *violences urbaines* in Frankrijk. De twee andere strategieën zijn specifiek gericht tegen uitingsvormen van online aangejaagd protest. Het betreft enerzijds wetgeving die zich richt op de regulering en handhaving van online content, en anderzijds kaders die zijn gericht op het tegengaan van desinformatie en buitenlandse beïnvloeding.

De wettelijke verankering van de handhaving van de openbare orde, c.q. de aanpak van demonstraties, samenscholingen en oproer in Frankrijk, biedt geen specifiek kader waarin het online aanjagen van protest centraal staat. De *Code de la sécurité intérieure* biedt prefecten en burgemeesters de grondslag om maatregelen treffen om ordeverstoringen te voorkomen, zoals een demonstratieverbod, het tegengaan van samenscholingen, of het opleggen van beperkingen (met betrekking tot plaatsen en tijden)[109], maar online mobilisatie of verspreiding van desinformatie zijn geen expliciet deel van dit wettelijke kader. Wel wordt in Frankrijk specifieke wetgeving toegepast

[108] https://rsf.org/fr/france-la-libert%C3%A9-de-la-presse-entrav%C3%A9e-par-des-violences-polici%C3%A8res-au-cours-des-manifestations; https://rsf.org/fr/modification-du-cadre-de-protection-des-journalistes-en-manifestation-en-france-ni-la-m%C3%A9thode-ni-le; https://shs.cairn.info/magazine-socialter-2025-6-page-70?lang=fr.

[109] https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000025503132/.

voor politieoptreden bij demonstraties[110]. Ook zijn er speciale protocollen voor ordehandhaving bij violences urbaines: het *Nationaal Schema voor Stedelijk Geweld* (SNVU)[111]. Hierin wordt trouwens niet specifiek aandacht besteed aan het aanpakken van het online aanjagen van protest.

De regulering van desinformatie daarentegen is in verschillende Franse wetten vastgelegd, en heeft haar basis in specifieke uitingsdelicten die veel landen – waaronder Nederland – kennen (Van Hoboken, 2019). Specifiek met het oog op openbare ordeverstoring kan daarnaast op grond van artikel 27 van de Franse vrije perswet een hoge boete worden opgelegd voor de publicatie, verspreiding of reproductie van onwaar nieuws, als de openbare orde hierdoor (mogelijk) wordt verstoord (Couzigou, 2021, p. 103)[112]. Nieuwe wetgeving over desinformatie werd gemaakt na de Franse verkiezingen van 2017. Aanleiding was de hevige (statelijke) desinformatie diewas gericht tegen president Macron. Na zijn verkiezing kondigde hij een wet aan die de verspreiding van valse informatie rondom Franse verkiezingen moet tegengaan[113]. Op het ogenblik is dit de enige wetgeving die specifiek is gericht op *online* desinformatie die is bedoeld om de bevolking te misleiden (Couzigou, 2022).

Het is interessant dat deze wet niet primair draait om de strafbaarstelling van desinformatie, maar om een mechanisme dat de verspreiding ervan snel een halt kan toeroepen. De procedure kan door het Franse openbaar ministerie worden gestart, maar eveneens door elke belanghebbende die zichzelf ziet als slachtoffer van onware informatie die opzettelijk en geautomatiseerd is verspreid, of financieel wordt ondersteund door derde partijen, of verspreid is door bots, of een online communicatiedienst (Couzigou, 2021, p. 104). De rechter kan internetproviders of online platforms vervolgens verplichten om bepaalde content niet langer toegankelijk te maken, accounts die onware of misleidende feiten verspreiden te sluiten, of zelfs de toegang tot een website te blokkeren (Couzigou, 2021, p. 104). De wet is echter in de praktijk om verschillende redenen moeilijk toepasbaar gebleken. De rechter kan alleen verplichtingen opleggen aan online platforms of internetproviders, en een zaak kan alleen in een beperkte periode, direct gekoppeld aan een verkiezing of referendum, voor de rechter worden gebracht. De *Conseil Constitutionnel* heeft verder de reikwijdte van wat binnen dit wetsartikel als onware beweringen of verdachtmakingen moet worden gezien beperkt tot 'objectief aantoonbare onwaarheden' die een eerlijk verloop van een verkiezing of referendum kunnen beïnvloeden (Siegel & Klos, 2024, p. 688). Maar de wet lijkt wel succesvol in het opleggen van maatregelen ter bescherming van verkiezingen tegen online

[110] Bijvoorbeeld ten aanzien van controleren en (preventief) fouilleren de Loi du 10 avril 2019 'anti-casseurs' (zie: CSI (L211-..), CP (431-..), CPP (diverse bepalingen) en de Loi du 10 avril 2019 visant à renforcer et garantir le maintien de l'ordre public lors des manifestations (voor bijkomende specifieke bevoegdheden voorafgaand aan manifestaties); https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038358582.

[111] https://snpps.fr/schema-national-des-violences-urbaines/; https://www.justice.gouv.fr/rapport-danalyse-violences-urbaines-fin-juin-2023; https://www.interieur.gouv.fr/archives/actualites/communiques-de-presse/mise-a-jour-du-schema-national-du-maintien-de-lordre-snmo; Ligue des droits de l'homme: https://www.ldh-france.org/schema-national-violences-urbaines-et-guide-operationnel-des-violences-urbaines/

[112] Loi du 29 juillet 1881 sur la liberté de la presse: www.legifrance.gouv.fr/jorf/id/JORFTEXT000000877119. Deze wet wordt echter niet of nauwelijks toegepast omdat de wet ziet op de openbare orde en niet individuen als zodanig beschermt. Ook kan alleen het Franse openbaar ministerie een procedure starten, niet het slachtoffer van de desinformatie.

[113] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

desinformatiecampagnes (Couzigou 2021, p. 108-111; Couzigou 2023, p. 110-117; zie ook: Siegel & Klos, 2024).

Andere methodes die in Frankrijk zijn beproefd om de verspreiding van online desinformatie tegen te gaan, zijn de relatief stringente transparantie-eisen die aan onlineplatforms worden gesteld, zowel in de context van verkiezingen als in algemene zin (Couzigou, 2021, p. 108-110). De Franse media-autoriteit (ARCOM; vergelijkbaar met het Nederlandse Commissariaat van de Media, maar met een breder takenpakket) heeft vergaande bevoegdheden gekregen om de verspreiding van buitenlandse desinformatie via mediakanalen tegen te gaan. Twee wetten voor de aanpak van nepnieuws werden aangenomen (22 december 2018) en verleenden ARCOM en de rechter in kort geding aanvullende bevoegdheden op dit gebied[114].

Een opmerkelijke invalshoek die is verkend, onder meer met een uitvoerig debat in de Franse Senaat[115], is de discussie over direct online ingrijpen en het uitzetten van specifieke functies van platforms die bijdragen aan het mobiliseren van mensen. Het idee hierachter is dat het bevoegd gezag (de prefect) online platforms moet kunnen dwingen bepaalde functionaliteiten tijdelijk buiten bedrijf te stellen als demonstraties en protesten escaleren en de openbare orde en veiligheid dreigt te worden verstoord. Dit betreft bijvoorbeeld de functie in Snapchat waarmee zones van 'viraal gaan' op een kaart worden weergegeven, omdat mensen hierdoor naar locaties gaan waar 'iets te beleven' is. Of de functie om de locatie van vrienden realtime te volgen. WhatsApp heeft een functionaliteit waarop gebruikers video's met 'eigen kring' delen en zo laten zien waar ze zijn en wat ze doen.

Een opzienbare actie was, ten slotte, de lancering op 5 september 2025 van het Engelstalige X-account *French Response* door het ministerie van Buitenlandse Zaken. Dit account werd gepresenteerd als het 'officiële reactieaccount' van de Franse diplomatie, met als doel 'de onjuiste aanvallen op [Frankrijk] te weerleggen', zoals minister van Buitenlandse Zaken Jean-Noël Barrot verklaarde[116]. Hoewel dit initiatief kleinschalig van aard was, heeft het account bijna 200.000 volgers en kreeg het volop aandacht in de internationale media, omdat het een ietwat ludiek, ironisch en lik-op-stuk achtig antwoord is op trollen en desinformatie. Vanuit dat gezichtspunt droeg French Response ook bij aan de ontwikkeling van mediabewustzijn en -geletterdheid. Dat is overigens een expliciete strategie van de Franse overheid (Couzigou, 2023, p. 116, 119-120), die ook tot een actieve houding oproept. Burgers kunnen via overheidsplatforms als Pharos (en private initiatieven die met Pharos samenwerken) illegale, strafbare of schadelijke online inhoud (van welke soort dan ook) melden[117]. In de volgende paragrafen besteden we daar aandacht aan.

---

[114] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559; https://legalblogs.wolterskluwer.com/copyright-blog/france-arcom-a-new-regulatory-authority-to-fight-online-copyright-infringement/#:~:text=The%20Act%20creates%20'ARCOM'%20(the%20Authority%20for,authority%20with%20broad%20omissions%20and%20extensive%20powers; https://www.arcom.fr/en/internet-and-social-networks; https://www.arcom.fr/en/internet-and-social-networks#tab-link-Accesstoresources.

[115] https://www.senat.fr/rap/r23-521/r23-52113.html.

[116] https://www.lemonde.fr/international/article/2025/09/07/le-ministere-des-affaires-etrangeres-entend-lutter-contre-la-desinformation-institutionnelle-etrangere-sur-x-en-lancant-french-response_6639594_3210.html?

[117] https://www.masecurite.interieur.gouv.fr/fr/actualites/Pharos-se-modernise.

7.4 Aanpak: VIGINUM

De bestrijding van desinformatie in Frankrijk gebeurt uiteraard binnen Europese kaders, zoals de *Digital Services Act* en gezamenlijke EU-initiatieven rond online desinformatie en het versterken van de verantwoordelijkheden van *big tech*. Frankrijk voert deze EU-richtlijnen uit en werkt binnen EU-samenwerkingsverbanden aan capaciteitsopbouw en aan informatie-uitwisseling over online dreigingen[118]. Maar het heeft medio 2021 ook een intussen gerenommeerde overheidsdienst opgericht: Viginum (Bernigaud, 2023). Die is expliciet bedoeld voor de bewaking en bescherming tegen digitale buitenlandse beïnvloeding. Deze dienst functioneert binnen de structuur van de *Secrétariat général de la défense et de la sécurité* nationale (SGDSN)[119] en coördineert technische en operationele inspanningen om digitale beïnvloedingscampagnes en hybride dreigingen te monitoren.

Viginum heeft vier taken. De dienst analyseert openbaar toegankelijke content op digitale platforms (OSINT) om desinformatiecampagnes van buitenlandse (statelijke en niet-statelijke) actoren te identificeren die tot doel hebben de belangen van Frankrijk te schaden. Daarnaast ondersteunt de dienst de autoriteiten die verantwoordelijk zijn voor het correcte verloop van nationale verkiezingen met technische expertise om pogingen tot destabilisatie van het democratische proces te identificeren. Viginum onderhoudt operationele en technische contacten met haar buitenlandse tegenhangers, en ontwikkelt expertise en normstelling voor de aanpak van hybride dreigingen. De vierde taak van Viginum is het ondersteunen van de SGDSN door middel van de interbestuurlijke borging van de bestrijding van buitenlandse digitale inmenging[120].

Viginum werkt nauw samen met andere overheidsinstanties die betrokken zijn bij de bestrijding van desinformatie: het kabinet van de premier, de diplomatieke diensten, diverse afdelingen binnen het ministerie van Binnenlandse Zaken en het ministerie van Defensie. De dienst onderhoudt structurele relaties met bepaalde onafhankelijke autoriteiten, zoals ARCOM en de CNIL (Franse Autoriteit voor Gegevensbescherming, vergelijkbaar met de Nederlandse Autoriteit Persoonsgegevens)[121]. Ook staat Viginum regelmatig in contact met vertegenwoordigers van

[118] https://digital-strategy.ec.europa.eu/nl/policies/online-disinformation?

[119] Het *Sécrétariat Général de la Défense et la Sécurité Nationale* (SGDSN) is een interdepartementaal orgaan dat onder de Franse premier valt en de regeringsleider bijstaat bij het ontwerpen en uitvoeren van veiligheids- en defensiebeleid. Het SGDSN adviseert en ondersteunt het politieke besluitvormingsproces. Tot de expertisegebieden behoren alle strategische defensie- en veiligheidskwesties, zoals militaire programma's, nucleaire afschrikking, interne veiligheid als onderdeel van de nationale veiligheid, economische en energiezekerheid, terrorismebestrijding en crisisbeheersingsplannen. Het SGDSN vervult drie hoofdtaken: het monitort veiligheidsdreigingen, stelt regeringsplannen op en coördineert het crisismanagement. Daarnaast neemt het deel aan het opstellen van wetsvoorstellen en decreten met betrekking tot veiligheids- en defensieaangelegenheden, en voert het diverse operationele taken uit, variërend van veiligheidscontroles en het beheer van geclassificeerde documenten tot de bescherming van overheidscommunicatie (via het Centre de transmissions gouvernemental) en cyberbeveiliging. Een nationaal agentschap binnen SGDSN (ANSSI, *Agence nationale de la sécurité des systèmes d'information*) is specifiek verantwoordelijk voor die laatste taak. https://www.sgdsn.gouv.fr/

[120] https://www.sgdsn.gouv.fr/files/files/Publications/2025%2012%2022%20-%20AVIS%20DU%20COMITE%CC%81%20E%CC%81THIQUE%20ET%20SCIENTIFIQUE%20DE%20VIGINUM.pdf;

[121] https://www.cnil.fr/en

digitale platforms, internationale experts, specialisten uit de academische wereld en betrokkenen uit het maatschappelijk middenveld. Viginum heeft geen publiekstaak[122].

De technische teams zijn volledig geïntegreerd in de operationele afdeling en werken nauw samen met de geopolitieke, OSINT- en AI-analisten van het expertiseteam. Ze ontwikkelen en leveren tools op basis van de behoeften van de analisten. De teams hebben aanzienlijke autonomie bij het kiezen van de technische infrastructuur die het beste aansluit op de operationele vereisten. Het accent ligt op buitenlandse inmenging[123]. Ten tijde van de Franse verkiezingen van 2022 slaagde VIGINUM erin om vijf pogingen van buitenlandse inmenging te herkennen en door te geven aan overheidsinstanties (Bernigaud, 2023). De rapportages van Viginum worden in Frankrijk en in Europa als gezaghebbend en betrouwbaar beschouwd. De dienst heeft de reputatie slagvaardig, snel en van zeer hoge (technische) operationele kwaliteit te zijn.

Een ethische en wetenschappelijke commissie, die rapporteert aan de secretaris-generaal voor Defensie en Nationale Veiligheid (SGDSN), is verantwoordelijk voor het toezicht op de activiteiten van Viginum. De commissie publiceert jaarlijks een openbaar rapport[124], waarin beknopt ontwikkelingen en ambities worden geformuleerd. Deze rapporten bevatten geen operationele informatie. Hoe Viginum in de praktijk precies werkt en met welke middelen wordt zorgvuldig afgeschermd. Dat is bewust beleid.[125]

7.5 Aanpak: Pharos

Van geheel andere aard is de preventieve aanpak genaamd Pharos (*Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*)[126]. Dat is in 2009 opgezet als een platform waar burgers en overheidsinstanties illegale, strafbare of schadelijke online inhoud kunnen melden. Pharos wordt nu beheerd door het in 2023 opgerichte *Office anti-cybercriminalité* (OFAC), dat ressorteert onder de Police nationale (i.e. de Police judiciaire)[127]. Pharos en OFAC maken deel uit van het grootschalige innovatieprogramma op het gebied van cyberveiligheid dat het ministerie van

[122] https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques?utm_source=chatgpt.com.

[123] https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques?utm_source=chatgpt.com.

[124] https://www.sgdsn.gouv.fr/files/files/Viginum%20-%20rapport%20CES.pdf; https://www.sgdsn.gouv.fr/files/files/Publications/2025%2012%2022%20-%20AVIS%20DU%20COMITE%CC%81%20E%CC%81THIQUE%20ET%20SCIENTIFIQUE%20DE%20VIGINUM.pdf;

[125] Interview Viginum 20 maart 2026.

[126] https://www.masecurite.interieur.gouv.fr/fr/actualites/Pharos-se-modernise.

[127] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048458223; Organisatie OFAC: https://lannuaire.service-public.gouv.fr/gouvernement/7532cff7-fe22-4a00-9cea-c30812e444f1.

Binnenlandse Zaken in 2023 wettelijk heeft verankerd (LOPMI)[128], en hebben als belangrijkste taak het analyseren en doorgeleiden van signalen die binnenkomen[129].

Pharos is vooral gericht op het signaleren van ongewenste content en vervolgens het handhaven van wetgeving. Het is een publiek operationeel instrument, dat duidelijk maakt wat strafbare online content inhoudt. Concreet bestaat Pharos uit een openbaar webportaal waar meldingen kunnen worden gedaan [130]. Die meldingen kunnen over heel verschillende online content gaan (fraude, haat, terrorisme, geweld, opruiing, kinderporno, radicalisering, dierenmishandeling, bedreiging, et cetera). Melders vullen online een formulier in. Achter de schermen worden meldingen (geautomatiseerd) gerubriceerd, geanalyseerd en getriageerd. Dat gebeurt in drie groepen: generalisten (met overzicht over allerlei gebieden van illegale of strafbare online content), specialisten op het gebied van discriminatie en *hate speech*, en gespecialiseerde rechercheurs van de nationale politiediensten.

Pharos brengt meldingen zo centraal samen, stelt vast of het inderdaad om illegale, strafbare of schadelijke online content gaat en geleidt meldingen in dat geval door naar de bevoegde en gespecialiseerde diensten van de nationale politiediensten, die het signaal opvolgen[131]. In de praktijk gaat het dan dikwijls om OFAC, of om andere afdelingen binnen de recherche (in een bepaalde regio) als er opsporingsonderzoek dient te worden gedaan. Maar er bestaan bijvoorbeeld ook specifieke gerechtelijke eenheden, zoals de *Pôle national de lutte contre la haine en ligne* in Parijs. Die richt zich specifiek op strafrechtelijk onderzoek naar en vervolging van ernstig online haatzaaien en gerelateerde strafbare feiten[132]. Pharos kan online content snel laten verwijderen door de hostingprovider of websitebeheerder, dan wel verder opsporingsonderzoek laten beginnen. In voorkomende gevallen kan Pharos de politie ook onmiddellijk actief laten ingrijpen bij een levensbedreigende situatie. Met welke analysetools Pharos werkt, is niet publiek gemaakt.

In 2023 berichtten Franse media, onder verwijzing naar een intern rapport, dat het aantal meldingen bij Pharos bij grote incidenten piekte. Dat was bijvoorbeeld het geval rond de Nahel Merzouk rellen in juni en juli 2023, en de aanval van Hamas op Israël en Hamas op 7 oktober 2023 en de daaropvolgende oorlog. "In plaats van 4.000 meldingen per week ontvangt het platform nu 1.000 meldingen per dag", aldus het interne rapport. Dat legde veel druk op de verwerking van meldingen en op de medewerkers van Pharos. Het aantal medewerkers was na de moord op leerkracht Samuel Paty in oktober 2020 al verdrievoudigd, maar kon geen tred houden met het explosief stijgende

[128] https://www.vie-publique.fr/loi/284424-loi-24-janvier-2023-securite-lopmi-programmation-ministere-interieur; https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768.

[129] https://internet-signalement.gouv.fr/. Pharos maakt deel uit van een Frans 'ecosysteem' tegen online oplichting. Dat bestaat uit een samenhangende reeks mogelijkheden om online misstanden te melden, waaronder Pharos (illegaal of strafbaar online gedrag en/of content), Thesee (melding online scams, phishing, cyberfraude, etc.; i.p.v. melding op bureau van politie of gendarmerie: https://www.sfpf.fr/actu/thesee-plainte-arnaque), Nummer 33700 (idem als Thesee, maar dan gericht op scams, phishing via sms: https://www.sfpf.fr/actu/numero-33700-signaler-sms), Signal Spam (publiek-privaat initiatief om grootschalige spam en/of pogingen tot phishing online te melden: signal-spam.fr), Phishing Initiative (online signaleren en blokkeren van phishing sites, door Orange Cyberdéfense: phishing-initiative.fr)

[130] https://internet-signalement.gouv.fr/

[131] https://www.service-public.gouv.fr/particuliers/vosdroits/F31979.

[132] https://www.tribunal-de-paris.justice.fr/75.

aantal meldingen in 2022 en 2023[133]. In 2023 werkten er ongeveer 50 personen. Tabel 5 toont het volume van meldingen dat Pharos – volgens eigen opgave – tussen 1 januari 2023 en 1 juli 2025 heeft verwerkt. Over de doelmatigheid en doeltreffendheid van Pharos zijn geen publiek toegankelijke evaluaties bekend. De verantwoording beperkt zich tot summiere beschrijvingen bij volumetabellen.

Tabel 5: Het volume van meldingen dat Pharos, tussen 1 januari 2023 en 1 juli 2025 heeft verwerkt.

	Totaal aantal meldingen	Noodsituaties (direct ingrijpen)	Verwijdering bij de bron door websitebeheerders Kindermisbruik	Terrorisme	Verwijdering diverse (discriminerende) content door hostingproviders
2025 (6 mnd.)	109.302	509	43.994	2.814	988
2024	222.094	697	80.731	6.679	2.168
2023	211.543	713	97.703	23.113	2.229

Bron: Pharos, bilan d'activité 2023-2024-2025; https://www.masecurite.interieur.gouv.fr/fr

Bevindingen ten aanzien van Viginum en Pharos

De twee bestudeerde Franse aanpakken laten zien dat veel waarde wordt gehecht aan een sterke informatiepositie met betrekking tot de online risico's met betrekking tot online aangejaagde ordeverstoringen. Pharos richt zich op het signaleren, verzamelen en doorgeleiden van meldingen van illegale of schadelijke online content, terwijl Viginum zich richt op de analyse van bredere informatiepatronen, desinformatiecampagnes en buitenlandse beïnvloeding. Samen illustreren deze aanpakken het belang van centrale voorzieningen voor monitoring, analyse en duiding van online ontwikkelingen.

Tegelijkertijd laten beide voorbeelden zien dat dergelijke voorzieningen afhankelijk zijn van voldoende capaciteit en maatschappelijke legitimiteit. Bij Pharos roept de sterke groei van het aantal meldingen vragen op over de verwerkbaarheid en opvolging van signalen. Bij Viginum zijn personele capaciteit en financiële middelen geen issue, en er wordt met het modernste instrumentarium en een opmerkelijke mate van ruimte voor creativiteit gewerkt. Maar hier roept juist de beperkte transparantie over werkwijzen en analysemethoden vragen op over controleerbaarheid en proportionaliteit. Daarmee maakt de Franse casus zichtbaar dat investeringen in informatiepositie niet alleen technische en organisatorische vraagstukken oproepen, maar ook vragen over capaciteit, toezicht en publieke verantwoording.

[133] https://www.europe1.fr/Police-Justice/cybercriminalite-les-agents-de-Pharos-sous-un-deluge-de-signalements-et-sans-parapluie-4275423.

8 Duitsland

8.1 Algemeen kader handhaving Openbare Orde en veiligheid

De handhaving van openbare orde en veiligheid is in Duitsland federaal (landelijk) georganiseerd. Op federaal niveau is de verantwoordelijkheid belegd voor de veiligheidsstrategie, de overkoepelende wetgeving, de coördinatie van landelijke taken als de grensbewaking en de veiligheid op het spoor en in de luchtvaart, en grensoverschrijdende zware misdaad en terrorisme. De dagelijkse handhaving van de openbare orde en veiligheid is primair echter de verantwoordelijkheid van de deelstaten (*Bundesländer*).

Uitvoerend liggen die taken (binnen de deelstaten) bij twee autoriteiten: de politie en de openbare-ordediensten (*Ordnungsämter*). De politie is bevoegd bij een algemene dreiging voor de openbare veiligheid en orde waar geen andere autoriteit het gevaar kan voorkomen, en ze doet de strafrechtelijke handhaving. De openbare-ordediensten zijn gemeentelijke diensten. Zij nemen uiteenlopende taken op zich die voortvloeien uit het handhaven van de alledaagse veiligheid in de publieke ruimte, zoals verkeerscontroles, afvalverwerking en geluidsoverlast. De precieze taken en bevoegdheden van de openbare-ordediensten en de politie zijn in de afzonderlijke deelstaten verschillend geregeld, omdat de deelstaten bij wetgeving zelf kunnen beslissen hoe en door wie zij handhaving van de openbare orde en veiligheid in de gemeenten laten uitvoeren.

Er zijn vier politieautoriteiten in Duitsland. Ten eerste de deelstaatpolitie (*Landespolizei*, LPOL)[134]. De deelstaatpolitie heeft een blauwe tak, een recherche en een oproertak. In de tweede plaats is er de federale politie (*Bundespolizei*, BPOL)[135]. Die is verantwoordelijk voor de beveiliging van spoorwegen en de luchtvaart, grensbewaking en terrorismebestrijding. De derde autoriteit is het *Bundeskriminalamt* (BKA), de centrale en overkoepelende landelijke politiedienst die zich bezighoudt met de bestrijding van zware criminaliteit en de staatsveiligheid (terrorisme, georganiseerde misdaad)[136]. Ten slotte heeft Duitsland de binnenlandse veiligheidsdienst (*Verfassungsschutz*, BfV)[137], die de preventieve bescherming van de democratie en de rechtsorde tot taak heeft[138].

[134] https://www.polizei.de/Polizei/DE/Home/home_node.html.

[135] https://bundespolizei.de/#.

[136] file:///Users/HMO/Downloads/bkaGesetz.pdf.

[137] https://www.verfassungsschutz.de/DE/home/home_node.html

[138] https://www.polizei.de/Polizei/DE/Home/home_node.html; https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/heimat/mehr-respekt/polizei/unterschiedliche-einsatzkraefte-faq.html;

Wetgeving

Verstoring van de openbare orde en veiligheid is geen afzonderlijk strafbaar feit. Voor de Duitse wet geldt dat verstoring van de openbare orde en veiligheid – door middel van specifieke delicten – strafbaar kan worden gesteld als de normale loop der dingen wordt verstoord en daardoor 'gerechtvaardigde ergernis' wordt opgewekt. Te denken valt aan vernieling/beschadiging van zaken (§ 303 StGB), vernieling van bouwwerken (§ 305 StGB), verstoring van openbare bedrijven en voorzieningen (§ 316b StGB), of de verstoring van de openbare vrede (§ 125 StGB). De rechter beoordeelt dan of en in welke mate het algemeen belang is geschaad. Straffen kunnen variëren van boetes tot vrijheidsstraffen.

Openbare orde en veiligheid worden niet alleen beschermd door het strafrecht, maar ook het *Sicherheits- und Ordnungsgesetz* (SOG) en het Polizei- und Ordnungsbehördengesetz (POG) in elke deelstaat. Daarin worden de taken en bevoegdheden van respectievelijk de deelstaat en de politie ten aanzien van het handhaven van de openbare orde en veiligheid geregeld. Het *Ordnungswidrigkeitengesetz* (OWiG) gaat over handelingen die de openbare orde verstoren (overlastsituaties).

De grondwet biedt alle Duitsers ten slotte het recht om vreedzaam (onaangekondigd) te demonstreren (Art.8). De wetgevende bevoegdheid met betrekking tot het recht op vrije vergadering ligt bij de deelstaten. Beieren, Berlijn, Hessen, Nedersaksen, Noordrijn-Westfalen, Saksen, Saksen-Anhalt en Sleeswijk-Holstein hebben hiervoor hun eigen wetgevende kader aangenomen. In de andere deelstaten is het federale *Versammlungsgesetz* (*Gesetz über Versammlungen und Auszüge*) vooralsnog van toepassing. In Duitsland kan slechts inbreuk op dit recht worden gemaakt bij wijze van *ultimum remedium*, en kan een demonstratie alleen vóór of kort na aanvang worden verboden als de bijeenkomst een aantoonbare bedreiging voor de openbare veiligheid vormt. In de praktijk dient dan vrijwel altijd een concrete geweldsdreiging aan de orde te zijn.

Politie en (des)informatie

De informatiehuishouding van de Duitse politie is op federaal niveau belegd. De Centrale Informatie- en Opsporingsdienst (ZI) van het Bundeskriminalamt is verantwoordelijk voor de nationale en internationale informatie-uitwisseling. ZI beheert databanken en informatiesystemen, die de dienst samen met partners in binnen- en buitenland doorontwikkelt. ZI is bevoegd om opsporingsonderzoek te doen. Verder bevindt zich bij ZI de Centrale Informatie- en Inlichtingendienst (ZIAD). Deze dienst vormt de verbinding tussen de Duitse politie en politiediensten wereldwijd, en doet een groot deel van de internationale uitwisseling van politie-informatie. Een nieuwe, wettelijk verankerde taak van ZI is sinds 1 februari 2022 het Centrale Meldpunt voor strafbare inhoud op internet (ZMI). Hierin zijn de decentrale meldstructuren voor online haatzaaien en opruiing centraal samengebracht[139].

ZMI ontvangt meldingen met betrekking tot strafrechtelijk relevante online content via samenwerkingspartners in de strafrechtketen of van NGO's. Na een eerste controle en triage stuurt ZMI relevante meldingen door naar de bevoegde autoriteiten op deelstaatniveau. Op deze manier zorgt ZMI samen met de politiediensten van de deelstaten voor de vervolging van haatcriminaliteit

[139] https://www.bka.de/DE/KontaktAufnehmen/KontaktBesondereThemen/MeldestelleHetzeImInternet/meldestelle_node.html.

op internet. Deze samenwerking moet de toenemende verruwing van de communicatie op sociale media tegengaan, en de vervolging van plaatsers van illegale en strafbare content mogelijk maken. In 2025 verwerkte het ZMI 20.811 meldingen. Het aantal varieerde per kwartaal tussen 4.128 (Q4) en 6.241 (Q2) meldingen.

Op deelstaatniveau zijn verschillende meldpunten ingericht, zoals *HessenGegenHetze* en *REspect!*[140]. In de deelstaat Hessen treedt het parket-generaal in Frankfurt am Main ook samen met het maatschappelijk middenveld, media en wetenschap op tegen online haatzaaien en ophitsing via het gezamenlijke initatief *Keine Macht dem Haß*[141]. De Beierse regering treedt actief naar buiten met het initiatief *Justiz und Medien – konsequent gegen Haß*[142]. Het openbaar ministerie te Göttingen huisvest de *Zentralstelle zur Bekämpfung von Haßkriminalität im Internet – Niedersachsen*, dat het meldportaal *hassanzeigen.de* beheert.

Om de strafbaarheid van de meldingen adequaat vast te stellen en tegelijkertijd zo voortvarend mogelijk illegale en schadelijke content te kunnen verwijderen, staat het ZMI nauw in contact met het Centrale Contactpunt Cybercrime Nordrhein-Westfalen bij het Openbaar Ministerie in Keulen (ZAC NRW) en de Centrale instantie voor de bestrijding van internet- en cybercriminaliteit (ZIT Hessen). Deze werkwijze van ZMI, afgestemd met politie en justitie op deelstaatniveau, maakt een effectieve en consequente aanpak van online extremisme en haatzaaien mogelijk. Alle meldingen die bij ZMI binnenkomen, doorlopen dezelfde verwerkingsstappen en worden in principe meteen na binnenkomst behandeld, ongeacht of samenwerkingspartners en meldpunten een zogenoemde trusted flagger zijn (conform art. 22 van de Digital Services Act)[143]. Volgens eigen opgave heeft ZMI van juni 2021 tot eind 2025 63.138 concrete meldingen ontvangen, waarvan 85% strafrechtelijk relevant was en kon worden opgevolgd. Dan gaat het vooral over openbare oproepen tot geweld of ernstige misdrijven, bedreigingen aan het adres van personen of overheidsinstellingen, aanzetten tot haat en aantasting van de menselijke waardigheid, maar ook over propaganda voor, steun aan of bevordering van extremistische of terroristische activiteiten en andere misdrijven die relevant zijn voor de (online en offline) nationale veiligheid[144].

Naast het ZMI bestaat ook het GIZ (*Gemeinsamen Internetzentrum*), dat in 2007 werd opgericht. Het GIZ is geen zelfstandige autoriteit, maar een samenwerkings- en communicatieplatform van het Bundeskrimimalamt, het de inlichtingemdienst BfV, de *Bundesnachrichtendienst*, het *Bundesamt für den Militärischer Abschirmdienst*, en het *Generalbundesanwaltschaft*. Het GIZ heeft geen eigen leiding en is niet op basis van een specifieke wet opgericht. Elke betrokken instantie werkt binnen de eigen bevoegdheid en binnen het kader van de wetgeving die voor die instantie toepasselijk is. Deze veiligheidsinstanties van de federale overheid wisselen binnen het GIZ informatie uit (met inachtneming van het *Trennungsgebot* (scheidingsgebod) tussen politie en inlichtingendiensten) die zij hebben verkregen door observatie, evaluatie en analyse van allerlei vormen van extreme content

[140] : https://hessengegenhetze.de/hate-speech-und-extremismus-melden; https://meldestelle-respect.de/

[141] https://justizministerium.hessen.de/Buergerservice/KeineMachtdemHass

[142] https://www.bayern-gegen-hass.de/

[143] https://www.dsc.bund.de/DSC/DE/4TrustedF/start.html

[144] https://www.bka.de/DE/KontaktAufnehmen/KontaktBesondereThemen/MeldestelleHetzeImInternet/meldestelle_node.html

en radicalisering op het internet en sociale platforms. Daarnaast worden waar mogelijk taken gezamenlijk uitgevoerd en werkprocessen gecoördineerd, zoals het monitoren van internet en het gezamenlijk ontwikkelen van technische instrumenten. Het GIZ is specifiek bedoeld voor informatie-uitwisseling en coördinatie met betrekking tot islamistische en jihadistische content[145].

Verder zijn bij de mediacommissariaten in de Duitse deelstaten meldpunten of gespecialiseerde afdelingen ingericht. De mediacommissariaten houden toezicht op de radio- en televisieomroepen, controleren de naleving van de reclameregels en houden – ook ten aanzien van sociale media – toezicht op diversiteit en mediaopvoeding[146]. De aanpak die we hierna verder uitwerken, KI4Deutschland, werkt bijvoorbeeld nauw samen met de *Medienanstalt Hamburg / Schleswig-Holstein* (MA HSH).

8.2 OAOV: drie typen incidenten

In Duitsland is het aantal vernielingen van kritieke infrastructuur de laatste jaren toegenomen. Deze vernielingen komen uit links-extremistische hoek[147] en veroorzaken niet alleen aanzienlijke economische schade, maar treffen door uitval van stroom, internet en telecommunicatie of door verstoringen van het treinverkeer ook de bevolking. Voor geweldgeoriënteerde linksextremisten zijn sectoren als energie, informatietechnologie en telecommunicatie, transport en verkeer, en staat en bestuur belangrijke doelwitten. In de ogen van deze links-extremistische groepen schragen deze sectoren een repressief staatsbestel en het kapitalistische systeem. Dit type incidenten heeft in Duitsland bijgedragen aan de discussie over het monitoren van online content.

Op 9 september 2025 viel door brandstichting bij twee hoogspanningsmasten de stroom in het zuidoosten van Berlijn gedurende meerdere dagen en op grote schaal uit. Noodnummers waren beperkt bereikbaar, trams en S-Bahn vielen uit of reden met vertraging, de straatverlichting en verkeerslichten werkten niet, en omdat een warmtekrachtcentrale moest afschalen, konden veel huishoudens niet van warm water worden voorzien. Er zijn verder aanvallen gepleegd op bijvoorbeeld (bouw)voertuigen, kabelgoten, zendmasten, infrastructuur van dagbouwmijnen, of gebouwen van grote ondernemingen in de bouw en de logistiek.

Zo eiste het *Kommando Angry Birds* onder meer de brandstichting eind juli 2025 op een van de belangrijkste spoorverbindingen in Noordrijn-Westfalen op. Deze groep stelt zijn ervaringskennis ook actief beschikbaar aan anderen, zodat die zelf succesvol brand kunnen stichten. Anonieme zogenoemde *Vulkangruppen* stichten eveneens branden met aanzienlijke schade en maatschappelijke gevolgen, bijvoorbeeld op 5 maart 2024 in een stroommast vlak bij de Tesla-gigafactory in Brandenburg (*Vulkangruppe Tesla abschalten*). Op 3 januari 2026 kwam het door brandstichting bij een kabelbrug in het district Steglitz-Zehlendorf tot een grootschalige stroomuitval in het zuidwesten van Berlijn.

---

[145] Het GIZ werkt op dezelfde manier als een tweetal vergelijkbare initiatieven die al langer bestaan, namelijk het *Gemeinsames Extremismus und Terrorismusabwehrzentrum* (GETZ) en het Gemeinsames Terrorismusabwehrzentrum (GTAZ).

[146] https://www.die-medienanstalten.de/ueber-uns/landesmedienanstalten

[147] https://www.zeit.de/gesellschaft/zeitgeschehen/2026-01/politisch-motivierte-gewalttaten-2025.

De in Duitsland populaire protestcampagne *Switch off – the system of destruction* (Switch off) verbindt sinds begin 2023 antikapitalisme met klimaatpolitieke thema's en zet bewust aan tot het plegen van strafbare feiten. Interessant is dat doelgericht wordt gewerkt aan platformvorming: de online gelegenheid om de strijd 'in een gemeenschappelijke context te plaatsen'. Dat levert Switch off meer aandacht op bij een gedifferentieerde groep (potentiële) sympathisanten[148].

Deze manier van 'aandacht mobiliseren' is intussen overal ter wereld een vast onderdeel van protestrepertoires geworden. Op straat zijn er mensen met spandoeken, online gebeurt dat door anderen in een digitale ruimte met berichten en hashtags op te roepen om mee te doen. Het feit dat deze mensen niet zichtbaar zijn op straat, maakt hun manier van aandacht mobiliseren niet minder echt. Waar op straat politieke boodschappen worden gescandeerd, verspreidt een hashtag zich online razendsnel over landsgrenzen heen. Een specifiek kenmerk van online acties is dat iedereen zijn eigen draai kan geven aan de boodschap. Protest wordt zo gepersonifieerd, ook heel concreet met memes en snippets. Dat vergroot de betrokkenheid, ook onder groepen die niet in eerste instantie 'thuis' zijn bij de inhoud van het protest, maar wel actief zijn op sociale media en acties helpen viraal te gaan. Actiegroepen gebruiken dit mechanisme bewust, zeker als het gaat om grote onderwerpen waar iedereen wel iets bij voelt of er een mening over heeft (Sastramidjaja, 2025)[149].

Een derde type incident dat tot meer aandacht voor de aanpak van online aangejaagde ordeverstoring heeft geleid, is de dreiging van desinformatiecampagnes en buitenlandse inmenging. De beruchte Russische campagne *Doppelgänger* (vanaf mei 2022) liet zien dat daar vanuit het gezichtspunt van dit onderzoek twee interessante kanten aan zitten. Doppelgänger genereerde goed lijkende imitaties van gezaghebbende Westerse nieuwswebsites, die desinformatie gingen verspreiden: om verdeeldheid te zaaien, te polariseren en verkiezingen te beïnvloeden. Toen de campagne werd ontdekt, noemden diverse Europese regeringen en hun veiligheidsdiensten het een enorme bedreiging voor Westerse democratieën. De media en onderzoekers doken erbovenop en gebruikten grote woorden om het gevaar van wereldwijde desinformatiecampagnes als Doppelgänger te beschrijven. Nader onderzoek naar het fenomeen door de *Verfassungsschutz Bayern* zette echter vraagtekens bij de impact[150]. De campagne bleek in werkelijkheid lang niet zo verreikend en groot als die was voorgesteld. Media bleken de campagne belangrijker te hebben gemaakt dan die was. En belangrijker: dat zou wel eens precies de bedoeling van de campagne kunnen zijn geweest. Doppelgänger had impact, echter nauwelijks door directe blootstelling aan desinformatie, maar door de gehypete berichtgeving en alle aandacht die de discussie over het fenomeen genereerde.

Daarom is het belangrijk om bij het exposen van desinformatie op internet of sociale media niet alleen hard bewijs te hebben en dat bewijs ook te delen met de bredere (academische) onderzoeksgemeenschap, maar vooral ook twee wezenlijke vragen te stellen: in welke mate blaast *exposure* nepnieuws nieuw leven in? En ondermijnt dat juist niet het publieke vertrouwen in overheden en media? Het klakkeloos herhalen van mogelijk al te simpele oorzaak-gevolg

[148] https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/linksextremismus/angriffe-von-linksextremisten-auf-kritis.html.

[149] https://www.frankfurter-hefte.de/artikel/politischer-protest-im-internet-und-auf-der-strasse-2665/.

[150] https://www.verfassungsschutz.bayern.de/mam/anlagen/baylfv_vollanalyse_doppelgaenger.pdf.

redeneringen en politieke uitspraken is koren op de molen van desinformatie- en beïnvloedingscampagnes. Dat maakt ze disruptief. Daarom moeten journalistieke verhalen en onderzoeksteksten over desinformatie altijd van context worden voorzien, en moeten claims over het succes van desinformatiecampagnes nooit zonder harde bewijzen worden gepresenteerd. En dat is precies zoals het bij alle media-aandacht voor Doppelgänger niet ging[151].

Sinds augustus 2023 is de beïnvloedingscampagne Storm-1516 actief, met een technologisch vernuft en op een schaal die Doppelgänger ver achter zich laat. Duitse, Franse en Britse media worden geïmiteerd, kunstmatige intelligentie maakt geloofwaardige meertalige content mogelijk, en *burner accounts, deepfakes en typosquats* worden gebruikt om de grens tussen nep en echt diffuus te maken. In de kern zijn dit geen aanvallen meer op instituties, maar op de verstandhouding tussen overheid en samenleving. Onderzoek van het Franse Viginum onderstreepte deze conclusie[152]. *Target hardening* is daarom een van de verdedigingslinies, maar minstens zo relevant is de versterking van digitale geletterdheid, mediabewustzijn, het herkennen van door AI gemaakte *fake content* en met name het snel delen van betrouwbare informatie hierover binnen én tussen Europese landen.

De twee Duitse aanpakken die we hierna bespreken, sluiten aan bij de aandacht voor en urgentie van bescherming van burgers tegen antidemocratische, extremistische en haatzaaiende narratieven.

8.3 Aanpak: KI4Demokratie

De eerste aanpak is KI4Demokratie: een op AI gebaseerde monitoring van rechtsextremistische narratieven en netwerken op openbare sociale media. Het betreft een privé-initiatief, ondersteund door een commercieel bedrijf in Hamburg. Het initiatief kreeg na een LinkedIn-oproep in 2023, toen het (re)migratiedebat in Duitsland leidde tot felle demonstraties, zó veel bijval dat het als netwerk van vrijwilligers AI-tools begon te ontwikkelen om grote aantallen posts te kunnen screenen. De bedoeling hierachter was om: (i) de manier waarop extreemrechtse individuen online communiceren en *mainstreamen* transparant te maken; (ii) te analyseren wie de knooppunten en *heartbeats* vormen in de netwerken waarbinnen die posts circuleren; (iii) de steunnetwerken achter het extreemrechtse vertoog te identificeren; en (iv) de aard en stabiliteit van de narratieven vast te stellen (met het oog op interventies). KI4Demokratie is sinds medio 2025 operationeel en wil democratische organisaties en instellingen, de wetenschap en de journalistiek ondersteunen en voorzien van betrouwbare informatie.[153].

KI4Demokratie is een AI-platform dat dagelijks grote hoeveelheden Duitstalige openbare online data inkoopt en screent met behulp van een thesaurus van 500 zoekwoorden. Verschillende machine learning-modellen identificeren extreemrechtse narratieven, herkennen daarin trends, en maken netwerkanalyses. Het platform maakt onder meer gebruik van sentimentanalyse, hatespeech-detectie, topic modelling, netwerkanalyse en -visualisatie, en factchecking. De

[151] https://www.foreignaffairs.com/russian-federation/dont-hype-disinformation-threat.

[152] https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

[153] https://ki-fuer-demokratie.de/. Interview initiatiefnemer d.d. 1 april 2026.

uitkomsten van deze analyses worden met een dashboardfunctie toegankelijk gemaakt voor gebruikers. KI4Demokratie verzamelt informatie, maar publiceert zelf geen informatie die herleidbaar is naar personen of specifieke groepen. De gebruikte technieken en protocollen worden beschreven in een wetenschappelijke publicatie (Garrido Veliz et al., 2025)[154]. Het initiatief geeft openheid over ethische afwegingen, beperkingen en juridische waarborgen. Ook legt het initiatief verantwoording af over gegevensbescherming (privacywetgeving, GDPR). Over de eerste ervaringen die zijn opgedaan, is inmiddels gepubliceerd (Garrido Veriz et al., 2025).

KI4Demokratie is een onafhankelijk, landelijk initiatief *('Wir agieren als parteiunabhängige Initiative'*) en is niet verbonden met overheids- of politieorganisaties. Wel wordt samengewerkt met de Medienanstalt Hamburg / Schleswig-Holstein (MA HSH), die vanuit zijn taakstelling om toezicht te houden op sociale media actief gebruik maakt van de informatie die KI4Demokratie toegankelijk maakt. Of politiediensten ook gebruik maken van deze informatie is formeel niet bekend, maar volgens de initiatiefnemer ligt het voor de hand dat de MA HSH illegale en strafbare content doorzet naar het ZMI van het BKA. KI4Demokratie werkt samen met verschillende (particuliere) partners op technologisch, communicatief, marketing en onderzoeksgebied. Een overzicht hiervan is op de website van het initiatief te vinden. Vanuit wetenschap, journalistiek, ngo's en bedrijfsleven bestaat er belangstelling voor de techniek en de informatie van KI4Demokratie. Maar volgens de initiatiefnemer kan de overheid moeilijk uit de voeten met systematische monitoring van extreemrechtse uitlatingen op sociale media en online platforms, omdat die focus de neutraliteit van de overheid in het geding brengt[155].

Garrido Veliz et al. (2025) constateerden onder meer dat het model bij specifieke gebeurtenissen (zoals het steekincident in Aschaffenberg in januari 2025) goed werkt. Tegelijkertijd staat de enorme hoeveelheid gescande data op gespannen voet met wat qua personele capaciteit en beperkte financiële ruimte aan analyses kan worden uitgevoerd. De initiatiefnemer onderstreept dezelfde beperkingen. Ook geven Garrido Veliz en collega's (2025) aan dat het moeilijk is om directe feedback te krijgen van (potentiële) gebruikers – een belangrijke voorwaarde om het model te verbeteren. Daarnaast levert de toegankelijkheid van AI-taalmodellen die zijn getraind in de Duitse taal beperkingen op. Er zijn er niet veel en de beschikbare taalmodellen zijn onvoldoende doorontwikkeld of getraind. Dat is met name van belang voor het *fact-checking framework*. Er lagen ten tijde van het onderzoek bovendien nog uitdagingen in het nauwkeurig onderscheiden van legitiem discours en daadwerkelijk extremistische inhoud. Er is een risico op vals-positieven. Ook de interpretatie van de gegevens in het dashboard door de gebruikers is een aandachtspunt, aldus de onderzoekers. Er is immers toch een zekere deskundigheid nodig is om de betreffende gegevens goed te interpreteren. Gebruik van het dashboard vraagt om een strikte procedure (*curated ingress*) om misbruik voor antidemocratische doelen te voorkomen (Garrido Veriz et al., 2025)[156].

[154] https://arxiv.org/pdf/2506.09947v2.

[155] https://ki-fuer-demokratie.de/. Interview initiatiefnemer, 1 april 2026.

[156] https://arxiv.org/pdf/2506.09947v2.

8.4 Aanpak: Landelijke actiedagen tegen strafbare haat-posts

De tweede aanpak zijn de Landelijke actiedagen tegen strafbare haat-posts. Veel van deze *Haßpostings* (hate speech, belediging, opruiing en antisemitisme) worden via sociale media verspreid. Politiek is vrijwel iedereen in Duitsland het er wel over eens dat politie en justitie daar hard tegen moeten optreden. Uit deze overweging zijn landelijke actiedagen voortgekomen, onder coördinatie van eerst het ministerie van Binnenlandse Zaken en later het BKA. De politiediensten in de deelstaten voeren de acties uit, bij strafvervolging in samenwerking met het openbare ministerie in de deelstaten (*Staatsanwaltschaft)*. Indirect zijn ook de online platforms betrokken, evenals partijen die websites hosten In 2025 vond de *Aktionstag gegen Haßpostings* voor de twaalfde keer plaats in alle deelstaten[157]. Het unanieme signaal: het online verspreiden van haatuitingen is strafbaar en krijgt daadwerkelijk opvolging om normbesef te versterken.

Concreet betekent dit een reeks van bijna 200 gecoördineerde politieacties, die in heel Duitsland gelijktijdig worden uitgevoerd in de deelstaten. Daarbij horen huiszoekingen, verhoren van verdachten, inbeslagnames van hardware (computers, harde schijven, telefoons), inzet van IT- en (cyber)forensische afdelingen en digitale recherche en analyses van online posts (sociale media-monitoring, IP-tracering, loggegevensanalyse, en data-analyse om verdachten te identificeren)[158].

De politie heeft de bevoegdheid om huiszoekingen, inbeslagnames en verhoren uit te voeren bij verdenking van strafbare feiten, op basis van rechterlijke toestemming (StPO, art. 102–110). De openbare aanklagers kunnen strafvervolging instellen, met name op grond van het aanzetten tot haat (StGB art. 130) en aanverwante bepalingen gericht tegen haatzaaien, bedreiging en belediging[159]. Verder kan de politie in het kader van opsporingsonderzoek – in gerechtelijke context en onder toezicht van de aanklager – gegevens bij onlineplatforms opvragen of vorderen[160]. Het *Netzwerkdurchsetzungsgesetz* (NetzDG) verplicht platforms om *offensichtlich rechtswidrige Inhalte* snel te verwijderen en periodiek transparantierapporten te publiceren[161]. Als een zaak internationale aspecten heeft, worden Europese opsporingsinstrumenten en eventueel Europol / Eurojust ingezet. Tegelijkertijd mogen de acties van politie en justitie niet in strijd zijn met de Duitse grondwet en het internationaal recht. Privacy, bescherming van persoonsgegevens (AGV) en uitingsvrijheid blijven gewaarborgd.

---

[157] https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/11/aktionstag-hassposting.html; https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/241112_PM_Aktionstag_Hasskriminalit%C3%A4t.html https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/250625_StrafbareHasspostings.html.

[158] https://www.zeit.de/politik/deutschland/2025-06/polizeiaktion-bundesweit-hass-hetze-internet.

[159] Zie ook: https://dserver.bundestag.de/btd/21/010/2101056.pdf.

[160] https://www.gesetze-im-internet.de/. Op grond van het Telekomgesetz (TKG, art.171–173), dat de telecommarkt reguleert, gericht op eerlijke concurrentie, consumentenbescherming en netwerkuitbreiding; en het Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG). Deze wet bundelt sinds 1 december 2021 de privacyregels voor telecommunicatie en digitale diensten (zoals websites) en regelt strikte toestemming voor cookies en tracking, ter aanvulling op de AVG, in afstemming met de European Digital Services Act.

[161] https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html.

In de praktijk is er landelijk, in de deelstaten en lokaal veel (media-)aandacht voor de landelijke actiedagen en het bestrijden van *strafbaren Haßpostings*. Overigens organiseerde de politie in 2024 ook expliciet een landelijke *Aktionstag gegen antisemitische Haßkriminalität*, om antisemitisme op de agenda te houden[162]. Deze initiatieven krijgen over het algemeen breed bijval, maar er worden ook kritische noten gekraakt. De actiedagen zouden vooral symbolisch zijn. De structurele capaciteit van politie en justitie om online haat te bestrijden is onvoldoende. Critici wijzen ook op mogelijke selectiviteit. De nadruk wordt gelegd op extreme gevallen van – meestal rechtsextremistische – content, terwijl meer subtiele maar evengoed schadelijke content onopgemerkt blijft. Er blijft ten slotte altijd grijs gebied tussen wat strafbaar is en wat onder uitingsvrijheid vallen kan. Daar moeten politie en justitie zorgvuldig in opereren.

Bevindingen ten aanzien van KI4Demokratie en de Landelijke actiedagen tegen haatpostings
De Duitse aanpakken verbinden online signalen aan een concreet handelingsperspectief. Zowel KI4Demokratie als de landelijke actiedagen tegen haat-posts zijn gericht op het beter herkennen en adresseren van online uitingen die kunnen bijdragen aan maatschappelijke spanningen of verstoringen van de openbare orde.

Waar KI4Demokratie nadruk legt op analyse, monitoring en duiding van online ontwikkelingen, met een specifiek accent op rechtsextremistische narratieven, richten de Actiedagen zich op zichtbare handhaving van online uitingen die strafbaar kunnen worden gesteld. Tijdens de Actiedagen werken politie en justitie op allerlei niveaus samen, indirect ook met internetproviders en platforms. De bedoeling is om via (sociale) media expliciet te maken dat haat-posts niet worden getolereerd. KI4Demokratie is daarentegen een onafhankelijk particulier initiatief, dat nauw samenwerkt met het commissariaat voor de media (Medienanstalt) in Hamburg / Schleswig-Holstein, dat bij de politie aangifte doet van mogelijk strafbare rechtsextremistische uitingen online. KI4Demokratie treedt niet actief naar buiten, maar presenteert zijn werkwijze en bevindingen via expertisenetwerken en expertbijeenkomsten.

Knelpunt in beide gevallen is dat het interpreteren van online signalen complex is, ook met geavanceerde AI zoals KI4Demokratie die gebruikt. Handhavingsacties vergen veel capaciteit, de frequentie van de Actiedagen is laag. Het structurele effect van beide aanpakken is moeilijk vast te stellen. Van de Actiedagen zijn geen evaluaties voorhanden, terwijl KI4Demokratie voor een robuuste evaluatie nog te kort actief is.

162 https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/241112_PM_Aktionstag_Hasskriminalit%C3%A4t.html.

9 Conclusie

In dit hoofdstuk beantwoorden we eerst de vraag hoe online aangejaagde ordeverstoringen zich in de praktijk manifesteren (vraag 1). Daarna gaan we in op welke aanpakken landen hanteren en hoe deze functioneren (vraag 2). We eindigen dit hoofdstuk met een aantal overkoepelende bevindingen. Deze vormen de opmaat naar het antwoord op de vraag welke elementen uit de onderzochte buitenlandse aanpakken relevant zijn voor de Nederlandse context (vraag 3). Dat antwoord formuleren we in een aantal lessen.

9.1 De aard van OAOV

Op de vraag hoe online aangejaagde openbare-ordeverstoringen zich in de praktijk manifesteren, laat het onderzoek geen eenduidig antwoord zien. Achter de term gaat een breed scala aan situaties schuil, waarin online en offline dynamieken onontwarbaar met elkaar zijn verweven. Die variatie hangt samen met de eigenschappen van online platforms en sociale media. Zij maken het mogelijk dat informatie zich snel en op grote schaal verspreidt, vaak buiten traditionele structuren om, en bieden ruimte voor anonimiteit, losse netwerkvorming, en spontaan en wisselend leiderschap. Algoritmen versterken bovendien emotioneel geladen boodschappen. Daardoor kan mobilisatie sneller, diffuser en minder voorspelbaar verlopen, en krijgt de online dimensie in verschillende situaties een andere rol: organiserend, versterkend of escalerend, soms ook dempend en sturend.

Tegen deze achtergrond laat de analyse in hoofdstuk 2 zien dat online aangejaagde ordeverstoringen het best kunnen worden begrepen als een gelaagd fenomeen, waarin telkens andere combinaties voorkomen van drie dimensies: motivatie en thematiek, de wijze van mobilisatie, de actievorm en het verloop ervan. Incidenten verschillen omdat mensen verschillende redenen en gewoonten hebben om zich te mobiliseren. Niet iedereen komt op dezelfde manier en met dezelfde intensiteit voor dezelfde dingen in actie. Incidenten verschillen ook omdat mensen in verschillende, elkaar deels overlappende (online) netwerken zitten, met eigen manieren van communiceren en informatie consumeren. Incidenten verschillen ten slotte ook omdat mensen zich op verschillende manieren gedragen als ze de straat op gaan. Kortom, we hebben met een uiterst veelvormig en beweeglijk fenomeen van doen.

Terugkerende verschijningsvormen

Hoewel de praktijk sterk gevarieerd is, zijn er wel terugkerende patronen te onderscheiden in de manieren waarop OAOV zich voordoen. Deze patronen zijn niet strikt afgebakend, maar bieden wel houvast om de variatie te ordenen.

Een eerste type verstoringen betreft ideologisch gedreven mobilisaties, waarin politieke, maatschappelijke of normatieve overtuigingen centraal staan. Het gaat bijvoorbeeld om protesten rond klimaat, ongelijkheid of migratie, waarbij online communicatie wordt gebruikt om issues te agenderen en te framen, en ook om mensen te organiseren, informeren en mobiliseren. Dat manifestateert zich op uiteenlopende manieren, van vreedzame demonstraties tot meer ontregelende of confronterende actievormen, waarbij fysiek en verbaal geweld aan de orde kan zijn maar dat lang niet altijd is.

Een tweede type bestaat uit incidenten die worden aangejaagd door geruchten, desinformatie of morele verontwaardiging. In deze gevallen speelt online verspreiding van (al dan niet onjuiste)

informatie of desinformatie een centrale rol in het creëren van urgentie, dreiging of legitimatie om in actie te komen. Zulke dynamieken kunnen leiden tot snelle escalatie, vooral wanneer online frames ertoe leiden dat groepen tegenover elkaar komen te staan of dat gevoelens van onrecht, onmacht en achterstelling worden versterkt. Dikwijls gaat dit type verstoringen gepaard met (grootschalige) verbale en fysieke agressie.

Een derde type betreft opportunistische of door influencers aangejaagde samenkomsten, zoals influencer-gedreven mobilisaties en online hypes. Het kan hierbij ook gaan om complotdenkers die hun ideeën of verdenkingen online verspreiden en oproepen tot concrete acties tegen mensen of objecten. Bij dit type ontbreekt doorgaans een inhoudelijk of ideologisch programma, en zelfs als dat er wel is (zoals bij complotnarratieven) ontstaat de ordeverstoring vooral door de snelheid, schaal en onvoorspelbaarheid waarmee grote groepen mensen zich verzamelen en in actie komen.

Daarnaast zijn er specifieke vormen van openbare ordeverstoring waarin groepsdynamiek, rivaliteit of situationele factoren centraal staan, zoals bij hooliganisme, vechtgroepen of uitgaansgerelateerde incidenten. Ook hier speelt online communicatie een rol in het mobiliseren of coördineren van groepen, maar ligt het motief om in actie te komen vooral in die bestaande sociale relaties en interacties.

Tot slot zijn er situaties waarin online communicatie bijdraagt aan paniek, onzekerheid of plotselinge samenkomsten, zonder dat sprake is van duidelijke organisatie of de intentie om actief te mobiliseren. In zulke gevallen kan de snelle verspreiding van waarschuwingen, geruchten of tegenstrijdige informatie direct invloed hebben op het gedrag van grote groepen mensen in de publieke ruimte.

In de praktijk komen combinaties van deze verschijningsvormen voor, soms zelfs bij één en hetzelfde incident. Wat begint als een vreedzaam protest of een online hype, kan door interactie tussen deelnemers, omstanders en autoriteiten alsnog escaleren tot een openbare ordeverstoring.

9.2 Aanpakken van OAOV

In hoofdstuk 3 hebben we een groot aantal interventies geordend in vier typen aanpakken. Die indeling diende als analytisch kader voor de landenstudies. Om de tweede deelvraag in dit onderzoek te kunnen beantwoorden, keren we in deze paragraaf terug naar deze vier typen aanpakken: welke aanpakken hanteren verschillende landen om online aangejaagde openbare-ordeverstoringen te signaleren, te voorkomen en te beheersen, en hoe functioneren deze in de praktijk? Het doel is daarbij niet om de typologie opnieuw te beschrijven, maar om de belangrijkste bevindingen uit de landenstudies per type aanpak samen te brengen en te vergelijken.

Cluster 1. Preventieve en maatschappelijke aanpakken

Deze aanpakken (Tabel 6) richten zich op het voorkomen van escalatie door versterking van weerbaarheid en focus op maatschappelijke dynamiek. Ze grijpen vroeg in en werken via netwerken van publieke en maatschappelijke actoren. Deze aanpakken zijn afhankelijk van samenwerking, vertrouwen en institutionele inbedding. Het effect is indirect en moeilijk meetbaar.

Tabel 6: Mogelijkheden en issues van Preventieve en maatschappelijke aanpakken.

Aanpak (land)	Omschrijving / mechanisme	Mogelijkheden en issues
Prevent Duty Guidance (VK)	Wettelijke plicht voor publieke instellingen om signalen van radicalisering te herkennen en te delen	+ Vroegsignalering via brede netwerken – Spanningen met vertrouwen en professionele autonomie
Psychological Defence Agency – MPF (Zweden)	Versterkt maatschappelijke weerbaarheid tegen desinformatie via kennis, communicatie en coördinatie	+ Structurele versterking informatie-weerbaarheid – Effect indirect en moeilijk meetbaar

Cluster 2. Regulerende en toezichthoudende aanpakken
Deze aanpakken (Tabel 7) richten zich op het stellen en handhaven van regels voor de online omgeving, met name voor platforms. Ze werken vooral randvoorwaardelijk door de online context waarin mobilisatie kan plaatsvinden te beïnvloeden. In Ierland is deze aanpak doorontwikkeld. Ook in Duitsland spelen mediatoezichthouders in toenemende mate een rol bij het reguleren van online content, de providers en de platforms. Deze aanpakken worden steeds meer gekaderd in Europese wetgeving.

Tabel 7: Mogelijkheden en issues van regulerende en toezichthoudende aanpakken.

Aanpak (land)	Omschrijving / mechanisme	Mogelijkheden en issues
Coimisiún na Meán (Ierland)	Onafhankelijke toezichthouder die via Digital Safety Act en Online Safety Code platformverantwoordelijkheid afdwingt	+ Structurele beïnvloeding van online ecosysteem – Indirect effect op concrete ordeverstoringen

Cluster 3. Informatie- en intelligencegerichte aanpakken
Deze aanpakken (

Tabel 8) richten zich op het verkrijgen en duiden van informatie over online dynamiek, vaak vlak vóór of tijdens escalatie. Ze vormen in de praktijk een cruciale schakel: ze maken het mogelijk om patronen te herkennen, dreigingen te duiden en gericht te handelen.

Tabel 8: Mogelijkheden en issues van informatie- en intelligencegerichte aanpakken.

Aanpak (land)	Omschrijving / mechanisme	Mogelijkheden en issues
VIGINUM (Frankrijk)	Analyseert en detecteert buitenlandse desinformatiecampagnes en online beïnvloeding	+ Strategisch inzicht in informatiebedreigingen – Niet transparant
NSOIT (VK)	Monitoring en duiding van high-risk information threats voor overheid	+ Snelle duiding van online dynamiek – Niet transparant; mogelijk disproportioneel
KI4Demokratie (Duitsland)	Ondersteunt analyse van online haat, desinformatie en democratische bedreigingen	+ Koppelt technologie en analyse – Interpretatie en operationalisering blijven lastig

Cluster 4. Handhavings- en repressieve aanpakken

Deze aanpakken (Tabel 9) richten zich op het direct ingrijpen en sanctioneren van strafbaar gedrag. Ze zijn het meest zichtbaar en concreet, maar ook sterk afhankelijk van timing, bewijspositie en maatschappelijke acceptatie. In de landenstudies blijkt dat zij noodzakelijk zijn voor normhandhaving, maar op zichzelf onvoldoende zijn om onderliggende dynamiek te beïnvloeden.

Tabel 9: Mogelijkheden en issues van handhavings- en repressieve aanpakken.

Aanpak (land)	Omschrijving / mechanisme	Mogelijkheden en issues
Landelijke actiedagen tegen haatpostings (Duitsland)	Gecoördineerde opsporingsacties tegen strafbare online uitingen	+ Zichtbare handhaving en afschrikking – Symbolisch en vergt veel opvolgingscapaciteit (die er niet is)
PHAROS (Frankrijk)	Meld- en analysetool die illegale online content doorgeleidt naar opsporing en vervolging	+ Versterkt opsporingsketen en meldbereidheid – Afhankelijk van meldingen en opvolgingscapaciteit (die ontbreekt)

9.3 Overkoepelende bevindingen

Een belangrijke overkoepelende bevinding is dat online aangejaagde ordeverstoring in geen van de onderzochte landen als een louter digitaal probleem wordt benaderd. Overal en in alle aanpakken gaat het om een fenomeen in *The Onlife* (Floridi, 2015): online dynamiek – desinformatie, geruchten, algoritmische versterking, influencer-mobilisatie, platformfunctionaliteiten of netwerken die (al dan niet geautomatiseerd) ongewenst ideeëngoed verspreiden – gaat samen met bestaande maatschappelijke spanningen, identitaire tegenstellingen, wantrouwen jegens instituties en overheden of concrete incidenten op straat, en conditioneert die over en weer. Effectieve aanpakken dienen daarom integraal en systeemgericht te zijn. Ze richten zich op zowel de content als de platforms, alsook op de maatschappelijke en bestuurlijke context waarbinnen OAOV plaatsvinden.

Een tweede overkoepelende bevinding is dat innovatieve aanpakken zich meestal niet aan de uitersten van het continuüm bevinden. Ze vormen veeleer een gelaagde combinatie van preventie, vroegsignalering, platforminteractie en – pas in laatste instantie – repressie. Alle landen laten zien dat investeringen in maatschappelijke weerbaarheid tegen desinformatie conceptueel veelbelovend zijn, ook al ontbreken de empirische bewijzen vooralsnog. Dat geldt bijvoorbeeld voor het Zweedse Psychological Defence Agency en het Franse VIGINUM, terwijl Ierland illustreert dat systeemtoezicht door een nieuwe variant op een mediacommissariaat, de Coimisiún na Meán, aanvullend kan functioneren als preventieve laag onder klassieke openbare ordehandhaving. Duitsland laat zien dat meldstructuren, data-analyse en interinstitutionele coördinatie bruikbaar kunnen zijn om strafbare online dynamiek vroeg te herkennen, terwijl het Verenigd Koninkrijk onderstreept dat community based samenwerking en vroegsignalering waardevol zijn, mits zij voldoende rechtsstatelijk zijn ingebed.

Hieruit volgt dan ook – zoals recent onderzoek heeft onderstreept (Swart et al., 2025) – dat inzet op repressieve instrumenten die de individuele integriteit van burgers of hun demonstratierecht beperken, al dan niet met wettelijk verankerde bevoegdheden, weinig effect sorteert. Het actuele wettelijk kader om demonstraties en openbare ordeverstoringen te reguleren volstaat, ondanks de *convening power* van sociale media en online platforms en de belangrijke invloed van desinformatie die langs die weg wordt verspreid en gemobiliseerd. Een eenzijdig georiënteerde repressieve of technisch-instrumentele reflex draagt bovendien niet bij aan begrip over en weer, en veroorzaakt mogelijk legitimiteitsproblemen en maatschappelijke tegenreacties. Recent onderzoek onder Britse klimaatactivisten suggereert dat repressie bij reeds betrokken activisten juist kan bijdragen aan verdere mobilisatie en de bereidheid om meer confronterende actievormen te gebruiken (Davies-Rommetveit et al., 2026).

Dat geldt mutatis mutandis ook voor monitoring zonder duidelijk mandaat, externe controle of heldere afbakening, zoals de discussie rond de NSOIT in het Verenigd Koninkrijk laat zien. Gebrek aan transparantie leidt tot zorgen over *mission creep*, *chilling effects* en indirecte beperking van meningsuiting[52]. Ook recent Nederlands onderzoek naar burgerperspectieven op online toezicht laat zien dat burgers bevoegdheden op het gebied van monitoring vooral accepteren als die gericht en tijdelijk zijn, en als ze aan een concrete dreiging zijn gekoppeld. Weerstand ontstaat met name wanneer burgers vrezen dat sprake is van structurele monitoring, onduidelijke grenzen of

onvoldoende controle op het gebruik van gegevens (Bantema, 2025)[163]. Voorlopig lijkt het erop dat de *silver bullet* nog ontbreekt, maar dat de koers een zorgvuldig uitgebalanceerde en meerlagige aanpak is die bestaat uit weerbaarheid, regulering, samenwerking, intelligence en begrensde repressie.

[163] https://www.websitevoordepolitie.nl/content/uploads/2026/05/BANTEMA-Burgerperspectieven-op-wetsvoorstel-gegevensvergaring-openbare-orde-WEBSITE.pdf

10 Acht lessen voor Nederland

Om antwoord te geven op de derde en laatste deelvraag hebben we op basis van de bevindingen uit de landenstudies acht lessen voor Nederland geformuleerd. Deze lessen zijn vervolgens besproken in een online expertsessie met deskundigen uit wetenschap, beleid en praktijk. De deelnemers brachten gezamenlijk expertise in op het gebied van openbare orde en veiligheid, digitalisering, cybersafety, online gedrag, data-analyse, platformregulering, vrijheid van meningsuiting, strafrecht en lokaal bestuur. Tijdens de sessie zijn de bevindingen uit het onderzoek en de lessen die we daaruit hebben getrokken getoetst op herkenbaarheid, relevantie en toepasbaarheid in de Nederlandse context. Daarnaast is besproken welke kansen, risico's, dilemma's en randvoorwaarden de experts zagen bij de verdere ontwikkeling van beleid en instrumentarium. De uitkomsten van deze expertsessie zijn gebruikt om de lessen aan te scherpen en nader te duiden.

Les 1. Online is onderdeel van de openbare orde

Neem online communicatie standaard mee in de analyse van openbare-ordeverstoringen.
Mensen gebruiken sociale media en online platforms om te communiceren, te coördineren, te mobiliseren, te organiseren, te versnellen, intenser te maken, te verspreiden en betekenis te geven. De onderzochte voorbeelden laten zien dat online en offline processen zó nauw met elkaar verweven zijn geraakt, dat het onderscheid tussen 'online aangejaagde' en 'gewone' openbare-ordeverstoringen in de praktijk vaak weinig houvast biedt. Voor de analyse van en handhaving bij incidenten is het daarom niet de vraag óf online communicatie een rol speelt het meest relevant, maar de vraag hóe dat gebeurt en met welke gevolgen.

Les 2. Stem de aanpak af op het type incident

Effectieve interventies vragen om een goede match tussen de aard van het incident en de aard van de aanpak.
De onderzochte incidenten verschillen sterk in motieven, betrokken netwerken, actievormen, snelheid van escalatie, en de rol van online communicatie. Daardoor verschilt ook welke interventies kansrijk zijn. Een aanpak die past bij langdurige maatschappelijke spanningen vraagt iets anders dan een reactie (die op zichzelf ook weer een effect heeft) op een plotselinge online hype, een geruchtencampagne of een aangekondigde protestactie. De opgave is daarom om typen incidenten en typen aanpakken systematisch met elkaar te verbinden: welke combinatie van interventies past bij welke online-offlinedynamiek, op welk moment en met welk doel?

Deze afstemming begint al in de signaleringsfase, wanneer professionals op straat en bij digitale recherche tekenen van onrust waarnemen. De combinatie van structurele achtergrondkenmerken en specifieke, incidentele of lokale factoren bepaalt namelijk de aard en impact van een incident, en daarmee welke combinatie van interventies het meest passend is. Even belangrijk is het om in de na(zorg)fase van incidenten de tijd te nemen om terug te kijken, en te analyseren of de ingezette interventies het beoogde effect hebben gehad.

Les 3. Zorg voor een breed repertoire aan aanpakken

Omdat online aangejaagde openbare-ordeverstoringen uiteenlopende vormen aannemen, is op nationaal niveau een breed repertoire aan samenhangende interventies nodig.
Geen van de onderzochte landen beschikt over één uniforme aanpak. Alle landen combineren verschillende typen interventies: preventieve en maatschappelijke aanpakken, regulering en toezicht, informatie- en intelligencegerichte aanpakken, en handhaving en vervolging. Dat brede repertoire is nodig, omdat het speelveld varieert van geruchtenvorming en online mobilisatie tot platformverantwoordelijkheid, maatschappelijke spanningen en strafbare feiten. Effectief beleid vraagt daarom niet om één nieuwe oplossing, maar om samenhang tussen verschillende instrumenten, duidelijke verantwoordelijkheden en het vermogen om per situatie de juiste combinatie te kiezen. In de onderzochte landen lijkt die samenhang tussen aanpakken echter goeddeels te ontbreken.

Les 4. Grondrechten zijn het uitgangspunt

De aanpak van openbare-ordeverstoringen begint niet bij de vraag hoe kan worden ingegrepen, maar bij de bescherming van fundamentele rechten en vrijheden.
Demonstraties, protesten, bijeenkomsten en online uitingen vallen in beginsel binnen de democratische rechtsorde, ook wanneer zij confronterend, ontregelend of hinderlijk zijn. Het beschermen van grondrechten vormt daarom het uitgangspunt van overheidsoptreden. Tegelijkertijd kunnen situaties ontstaan waarin sprake is van geweld, strafbare feiten of ernstige risico's voor de openbare orde, waardoor optreden noodzakelijk wordt.

De landenstudies laten zien dat voorstellen voor ruimere bevoegdheden op het gebied van monitoring, regulering en handhaving vaak gepaard gaan met discussie over noodzaak, proportionaliteit en grondrechten. Ook laten de onderzochte voorbeelden zien dat interventies zelf gevolgen kunnen hebben voor gedrag en maatschappelijke verhoudingen. Monitoring kan leiden tot zorgen over privacy en chilling effects, terwijl repressief optreden onder omstandigheden juist kan bijdragen aan wantrouwen, verdere mobilisatie of escalatie. De uitdaging ligt daarom niet alleen in de vraag óf de overheid kan optreden, maar ook in welke gevolgen verschillende vormen van optreden hebben voor gedrag, vertrouwen en maatschappelijke verhoudingen.

Les 5. Ontwikkel en evalueer preventieve aanpakken

Het voorkomen van escalatie begint niet tijdens een incident, maar in de periode daarvoor.
Verschillende landen gaan ervan uit dat openbare-ordeverstoringen voortkomen uit bredere maatschappelijke spanningen, wantrouwen, polarisatie, geruchtenvorming of gevoelens van uitsluiting. Hoewel deze factoren op zichzelf niet noodzakelijk problematisch of strafbaar zijn, kunnen zij wel de voedingsbodem vormen voor openbare-ordeverstoringen. Daarom zetten de landen in op uiteenlopende vormen van preventie, zoals mediageletterdheid, lokale samenwerking, ondersteuning van professionals en maatschappelijke weerbaarheid. Daarbij richt de aandacht zich niet alleen op individuele burgers, maar ook op gemeenschappen, lokale netwerken, maatschappelijke organisaties en de relatie tussen overheid en samenleving.

Tegelijkertijd laat het onderzoek zien dat nog beperkt bekend is welke preventieve interventies onder welke omstandigheden daadwerkelijk effectief zijn. Daarom is het van belang om preventieve aanpakken niet alleen te ontwikkelen, maar ook systematisch te monitoren en te evalueren. Juist op dit punt bestaat een belangrijke kennislacune: robuust onderbouwde evaluatieve kennis ontbreekt in vrijwel alle onderzochte landen. Daardoor is vaak onduidelijk welke interventies

daadwerkelijk bijdragen aan het voorkomen of beperken van openbare-ordeverstoringen in The Onlife.

Les 6: Werk structureel samen

De aanpak van openbare-ordeverstoringen vraagt om structurele samenwerking tussen partijen die betrokken zijn bij signalering, duiding, preventie en handhaving.
Openbare-ordeverstoringen waarin online communicatie een rol speelt, raken verschillende domeinen tegelijk. Geen enkele partij heeft afzonderlijk volledig zicht op online signalen, lokale spanningen, platformmechanismen en mogelijke risico's voor de openbare orde. Politie, bestuur, justitie, toezichthouders, onderwijs, zorg, maatschappelijke organisaties, media en platforms beschikken elk over verschillende vormen van kennis, bevoegdheden en informatie, maar ook over uiteenlopende werk- en verantwoordingsculturen. Meer inzicht over en weer in wat partijen doen en hoe ze dat doen zou samenwerking ten goede komen.

Samenwerking is niet alleen van belang tijdens acute incidenten, maar ook in de voorbereiding daarop en in de nazorgfase na een incident. Online signalen krijgen pas betekenis in samenhang met kennis over lokale situaties, maatschappelijke spanningen, groepen, gebeurtenissen en fysieke locaties. Binnen verschillende aanpakken wordt gewerkt met structurele samenwerkingsverbanden, preventienetwerken en vaste contactstructuren tussen betrokken organisaties.

In de praktijk wordt de vigerende privacywetgeving in Europa en Nederland dikwijls aangewezen als een belemmering voor samenwerking in de vorm van uitwisseling en verwerking van persoonsgegevens en privacygevoelige informatie. Dat geldt vooral als het gaat over samenwerking tussen de domeinen veiligheid, zorg en sociaal. De wetgeving wordt echter ten onrechte als belemmering gezien. Binnen de AVG (en onderliggende wetgeving) is erg veel mogelijk, op voorwaarde dat de overkoepelende doelstelling om gegevens uit te wisselen en te verwerken doeltreffend is geformuleerd. Frustratie over de AVG komt doorgaans voort uit bestuurlijke terughoudendheid. Het belang van privacy-expertise die uitlegt hoe zorgvuldig met gevoelige gegevens om kan worden gegaan valt niet te onderschatten.

Les 7: Reguleer platforms en spreek hen aan op hun verantwoordelijkheid

Platforms zijn niet alleen doorgeefluiken, maar beïnvloeden actief hoe informatie zich verspreidt en hoe online mobilisatie en escalatie verlopen. Daarom dragen ook zij verantwoordelijkheid voor de aanpak van openbare-ordeverstoringen.
Verschillende landen richten hun aanpak niet alleen op burgers en groepen, maar ook op platforms en online infrastructuren. Daarbij gaat het bijvoorbeeld om platformtoezicht, meldstructuren, trusted flaggers, het verwijderen van strafbare inhoud en regelgeving zoals de Digital Services Act. De achterliggende gedachte is dat verantwoordelijkheid niet uitsluitend ligt bij individuele gebruikers, maar ook bij de digitale omgevingen waarin informatie wordt verspreid.

De onderzochte voorbeelden laten zien dat overheden, toezichthouders en strafrechtelijke ketens platforms daarom steeds nadrukkelijker aanspreken op hun rol in informatieverspreiding, online mobilisatie en de openbare orde. Tegelijkertijd blijft de effectiviteit van deze aanpak afhankelijk van duidelijke juridische kaders, internationale samenwerking en de bereidheid van platforms om mee te werken.

Les 8. Creëer een lerende praktijk

Investeer niet alleen in nieuwe aanpakken, maar ook in het vermogen om daarvan te leren. De onderzochte landen zetten in op uiteenlopende vormen van monitoring, platformtoezicht, maatschappelijke weerbaarheid, samenwerking en handhaving. Tegelijkertijd is over de werking, effectiviteit en mogelijke (neven)effecten van veel van deze aanpakken nog relatief weinig bekend. Dat geldt in het bijzonder voor preventieve interventies en maatregelen gericht op weerbaarheid, mediageletterdheid en online beïnvloeding.

Ook laat het onderzoek zien dat interventies zelf onderdeel kunnen worden van de dynamiek die zij proberen te beïnvloeden. Monitoring, communicatie, ingrepen bij platforms of handhaving kunnen bijdragen aan de-escalatie, maar in sommige situaties ook leiden tot wantrouwen, verplaatsing van communicatie of verdere escalatie. Effectief beleid vraagt daarom niet alleen om optreden, maar ook om het systematisch volgen, evalueren en bijstellen van interventies.

Dit onderzoek benadrukt daarmee het belang van een lerende praktijk, waarin kennisontwikkeling, monitoring en evaluatie niet losstaan van beleid en uitvoering, maar onderdeel zijn van een continue feedbackloop tussen incidenten, interventies en opgedane ervaringen. Naast versterking van evaluatieonderzoek en verdere verdieping van de relatie tussen online dynamieken en offline sociale voedingsbodems (zie les 2), vraagt ook de rechtsstatelijke inbedding van interventies om meer aandacht. Met name waar publiek-private samenwerking, platformsignalering en gegevensuitwisseling plaatsvinden, is meer empirische kennis nodig over proportionaliteit, transparantie en de bescherming van grondrechten.

Gezien het grensoverschrijdende karakter van online platforms, pogingen tot beïnvloeding en de diversiteit aan mogelijke aanpakken ligt het bovendien voor de hand om de internationale kennisuitwisseling verder te versterken. Een Europees kennisnetwerk of een periodieke conferentie over de aanpak van openbare-ordeverstoringen zouden hiervoor geschikte instrumenten kunnen zijn. Nederland zou hierin een voortrekkersrol kunnen vervullen.

Bijlage 1 Begeleidingscommissie en expertsessie

Begeleidingscommissie

Dit onderzoek is begeleid door een begeleidingscommissie die heeft meegedacht over de uitvoering van het onderzoek en de interpretatie van de bevindingen. De begeleidingscommissie bestond uit:

prof.dr. Henk Kummeling (Universiteit Utrecht) - Voorzitter
dr. Hedy Greijdanus (Rijksuniversiteit Groningen)
mr. drs. Shanti Rewti (Ministerie van Justitie en Veiligheid)
dr. Saskia Baas (WODC)

Expertsessie

Ter toetsing en aanscherping van de lessen voor Nederland is een online expertsessie gehouden. Tijdens deze sessie zijn de voorlopige bevindingen en lessen uit het onderzoek besproken met deskundigen uit wetenschap, beleid en praktijk. Aan de expertsessie namen deel:

dr. Willem Bantema (NHL Stenden)
prof. dr. Ana Isabel Barros (Tilburg University / Politieacademie)
Merel Driessen MA (Erasmus Universiteit Rotterdam)
mr. Lotte Houwing (Bits of Freedom)
dr. Michael Klos (Universiteit Leiden)
drs. Martijn Verhagen (Gemeente Amsterdam)

Colofon

Generatieve AI-toepassingen, waaronder ChatGPT, zijn in verschillende fasen van dit onderzoek gebruikt als ondersteunend hulpmiddel. De resultaten zijn steeds door de onderzoekers beoordeeld, geverifieerd en waar nodig aangepast. Alle keuzes, analyses, bevindingen en conclusies zijn voor rekening en verantwoordelijkheid van de auteurs.

De eindredactie van dit rapport is verzorgd door Patrick van den Hurk.

Referenties

Abidin, C. (2021). Mapping Internet Celebrity on TikTok: Exploring Attention Economies and Visibility Labours. *Cultural Science Journal, 12*(1), 77–103.

Al Jazeera. (2022). Sweden suspects "foreign actors" behind riots over Quran burning. https://www.aljazeera.com/news/2022/4/20/sweden-believes-foreign-actors-behind-riots-over-quran-burning

Amnesty International. (2013). *Policing assemblies*. In *Use of force: Guidelines for the implementation of the UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials* (pp. 101–126). Amnesty International.

Anderson, D. (2025). *Lessons for Prevent: Report of the Independent Prevent Commissioner following the Southport attack and the murder of Sir David Amess MP*. Independent Prevent Commissioner. https://assets.publishing.service.gov.uk/media/68907502486754ec2887839f/Lessons_for_Prevent_13_July.pdf

Associated Press. (2022, February 17). *Sweden hits out at "disinformation" on child kidnappings*. AP News. https://apnews.com/article/politics-sweden-government-social-services-kidnapping-e55c6196609d102bfe079d7c40c9ed7b

Associated Press. (2022, April 18). *Sweden links riots to criminal gangs that target police*. NPR. https://www.npr.org/2022/04/18/1093289012/riots-in-sweden

BBC News. (2020, August 30). *Protest against Koran-burning turns violent in Sweden*. BBC News. https://www.bbc.com/news/world-europe-53959492

Berglund, O. J. (2023). Disruptive protest, civil disobedience & direct action. *Politics*. Advance online publication. https://doi.org/10.1177/02633957231176999

Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication & Society, 15*(5), 739–768. https://doi.org/10.1080/1369118X.2012.670661

Bernigaud, A. (2023). *Defending the vote: France acts to combat foreign disinformation, 2021–2022*. Trustees of Princeton University.

Bierens, J., Jaasma, B., Perenboom, J., & Bitter, C. (2023). *Advies online aangejaagde ordeverstoringen*. Pels Rijcken.

Binder, J., & Reid, A. (2024). *Prevent duty, safeguarding and agency*. Nottingham Trent University. https://www.ntu.ac.uk/__data/assets/pdf_file/0034/2526883/Prevent-duty,-safeguarding-and-agency-NTU-report.pdf

Birchall, C., & Knight, P. (2025). *Report on conspiracy theories in the online environment and the counter-disinformation ecosystem in the UK*. REDACT. https://doi.org/10.71535/EFBFF8E9-83FF-48C8-96CD-A3382D42B4FD

Blackbourn, J. (2025). Administrative justice and decision-making under the Prevent and Channel duties. *Public Law*. Advance online publication. https://durham-repository.worktribe.com/OutputFile/3671694

Boucher, M. (2023). *La nébuleuse du pouvoir d'agir: L'empowerment des quartiers populaires à l'épreuve des pacificateurs et entrepreneurs de colères*. Champ social.

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp. 47–66). Routledge.

Busher, J., Choudhury, T., Thomas, P., & Harris, G. (2017). *What the Prevent duty means for schools and colleges in England: An analysis of educationalists' experiences*. Durham University, University of Huddersfield, and Coventry University. https://eprints.hud.ac.uk/id/eprint/32349/

Cachet, A., Daemen, H., Noppe, R., Ringeling, A., & Schaap, L. (2002). *Buitenlandse burgemeesters bekeken*. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. https://www.kennisopenbaarbestuur.nl/site/binaries/site-content/collections/documents/2004/01/01/buitenlandse-burgemeesters-bekeken/buitenlandse-burgemeesters-bekeken.pdf

Clark, C. (2023). Public order policing in the UK. In B. Bürger, T. D. Herold, & R. Lee (Eds.), *Public order policing* (pp. 247–270). Springer.

Commissie Project X Haren (2013). *De weg naar Haren. De rol van jongeren, sociale media, massamedia en autoriteiten bij de mobilisatie voor Project X Haren, (Deelrapport 2)*. [te raadplegen via ris.utwente.nl/ws/portalfiles/portal/5142026/de-weg-naar-haren-commissie-project-haren.pdf.]

Couzigou, I. (2021). The French legislation against digital information manipulation in electoral campaigns: A scope limited by freedom of expression. *Election Law Journal, 20*(1).

Couzigou, I. (2022). The empowerment of platform users to tackle digital disinformation: The example of the French legislation. In I. Kalpokas & J. Kalpokiene (Eds.), *Intelligent and autonomous: Transforming values in the face of technology* (Vol. 390). Brill.

Davies-Rommetveit, S., Douch, J., Gardner, P., Sach, A. A., Thomas-Walters, L., & Tausch, N. (2026). Emotional responses to state repression predict collective climate action intentions. *Nature Climate Change, [volume(issue)]*, 1–7. https://doi.org/[DOI]

Den Heyer, G. (2019). *Police response to riots: Case studies from France, London, Ferguson, and Baltimore*. Springer Nature. https://doi.org/10.1007/978-3-030-31810-9

Donson, F., Chesters, G., & Welsh, I. (2004). Rebellion, repression and the riot: The impact of anti-terrorism legislation on policing dissent. *Sociology, 38*(1), 57–76. https://doi.org/10.1177/0038038504039354

De Veen, L., Eysink Smeets, M., & Moors, H. (2024). *Fenomeenkaart online aangejaagde ordeverstoringen*. CCV & EMMA.

Dudenhoefer, A. L. (2018). Resisting radicalisation: A critical analysis of the UK Prevent Duty. *Journal for Deradicalization*, (14), 153–191.

Epstein, R., Guenot, M., & Jobard, F. (2024). Émeutes urbaines, sciences sociales et action publique: Mouvements et stagnations dans la politique de la ville et les politiques de sécurité. *Zilsel: Science, technique, société, 13*, 11–22. https://doi.org/10.3917/zil.013.0011

Evans, S. (2013). Stockholm riots throw spotlight on Swedish inequality. *BBC News*. https://www.bbc.com/news/world-europe-22650267

Eysink Smeets, M., Baetens, T., De Veen, L., & Moors, H. (2024). *Literatuurstudie: Burgerparticipatie bij online aangejaagde openbare ordeverstoringen (OAOV)*. EMMA.

Eysink Smeets, M., Moors, H., De Veen, L., & Koelink, M. (2025). *Bloemen op de begraafplaats*. Sdu / Politie en Wetenschap.

Fassin, D., & Fassin, E. (Eds.). (2006). *De la question sociale à la question raciale*. La Découverte.

Floridi, L. (Ed.). (2015). *The Onlife manifesto: Being human in a hyperconnected era*. Springer. https://doi.org/10.1007/978-3-319-04093-6_21

Garrido Veliz, R. A., Schaland, T. N., Bergmoser, S., Horwege, F., Bansal, S., Nahar, R., Semmann, M., Forthmann, J., & Yimam, S. M. (2025). *KI4Demokratie: An AI-based platform for monitoring and fostering democratic discourse*. arXiv. https://arxiv.org/pdf/2506.09947v2

Greijdanus, H., Bartelds, A., Postma, L., & De Vries, S. (2023). *Interventies in de cyclus van online aangejaagd geweld: Inzichten uit een literatuurreview*. Rijksuniversiteit Groningen & NHL Stenden.

Greijdanus, H., de Matos Fernandes, C. A., Turner-Zwinkels, F., Honari, A., Roos, C. A., Rosenbusch, H., & Postmes, T. (2020). The psychology of online activism and social movements: Relations between online and offline collective action. *Current Opinion in Psychology, 35*, 49–54. https://doi.org/10.1016/j.copsyc.2020.03.003

Government Offices of Sweden. (2025). *The Swedish model of government administration*. https://www.government.se/how-sweden-is-governed/the-swedish-model-of-government-administration/

Government Offices of Sweden. (n.d.). *Swedish Psychological Defence Agency*. Retrieved November 24, 2025, from https://www.government.se/government-agencies/swedish-psychological-defence-agency/

Hagström, P. (2022). *Utredaren: "Jag har inte fördelat ansvar och skuld"*. *Polistidningen*. https://polistidningen.se/2022/12/utredaren-jag-har-inte-fordelat-ansvar-och-skuld/

Homrighausen, A. (2024). Påskuppploppen 2022: *Ett underrättelsemisslyckande?* Lund University. https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9144168&fileOId=9144170

Hutter, S., & Borbáth, E. (2019). Challenges from left and right: The long-term dynamics of protest and electoral politics in Western Europe. *European Societies, 21*(4), 487–512. https://doi.org/10.1080/14616696.2018.1494299

Jarynowski, A., & Rostami, A. (2013). *Reading Stockholm riots 2013 in social media by text-mining*. *arXiv*. https://arxiv.org/abs/1310.1249

Lee, J., Elwick, A., & Kazim, R. (2019). The impact of the Prevent Duty on schools: A review of the evidence. *British Educational Research Journal, 45*(4), 821–837. https://doi.org/10.1002/berj.3527

Jobard, F. (2006). Sociologie politique de la 'racaille'. In H. Lagrange & M. Oberti (Eds.), *Émeutes urbaines et protestations: Une singularité française*. Presses de Sciences Po.

Jong, W., Dückers, M. L. A., & Van der Velden, P. G. (2016). Crisis leadership by mayors: A qualitative content analysis of newspapers and social media on the MH17 disaster. *Journal of Contingencies and Crisis Management, 24*(4), 286–295. https://doi.org/10.1111/1468-5973.12124

Jusko, T., & Weihe, M. (2024). Football hooliganism as a socio-political phenomenon: Motivation and social work interventions. *Journal of Education, Health and Sport, 14*(1), 119–130. https://doi.org/10.12775/JEHS.2024.14.01.010

Karlsson, I., Karlsson Haikio, T., Malm, M., & Orden, H. (2026). *Visual disinformation and visual literacy*. Lund University Psychological Defence Research Institute. https://lup.lub.lu.se/search/files/240017208/Visual_Disinformation_and_Visual_Literacy.pdf

Kaulingfreks, F. (2013). *Making trouble: Disruptive interventions of urban youth as unruly politics*. Radboud Universiteit.

Knutsson, J., & Holgersson, S. (2023). *Granskning av Polismyndighetens utvärdering av polisinsatsen under påskuppploppen 2022*. Polisforskningsstiftelsen. https://polisforskning.se/ws/media-library/f64ad3283917472993f3155682425af0/pm-om-polismyndighetens-utvardering-av-paskuppploppen.pdf

Kokoreff, M. (2008). *Sociologie des émeutes*. Payot.

Kozlowski, A., & Tofvesson, M. (2024, May 7). Combatting disinformation by state agencies: The case of the Swedish Psychological Defence Agency. *New Eastern Europe*. https://neweasterneurope.eu/2024/05/07/combatting-disinformation-by-state-agencies-the-case-of-the-swedish-psychological-defence-agency/

Kumar, A. (2025). *Submission of written evidence to the Science, Innovation and Technology Committee inquiry on social media, misinformation and harmful algorithms (UK Parliament)*. https://research.gold.ac.uk/id/eprint/38208/1/download%20%283%29.pdf

Lapeyronnie, D. (2006). Révolte primitive dans les banlieues françaises. *Déviance et Société, 30*(4), 431–448. https://doi.org/10.3917/ds.304.0431

Le Goaziou, V., & Mucchielli, L. (Eds.). (2007). *Quand les banlieues brûlent… Retour sur les émeutes de novembre 2005*. La Découverte.

Lund University. (n.d.). *Lund University Psychological Defence Research Institute (Forskningsinstitutet för psykologiskt försvar)*. https://www.psychologicaldefence.lu.se/about-institute

Marlière, E. (2023). *Les quartiers (im)populaires ne sont pas des déserts politiques*. Le Bord de l'Eau.

Marlière, E. (2023). Quarante ans de révoltes urbaines. *Esprit*, (11), 10–13.

Mauger, G. (2006). *L'émeute de novembre 2005: Une révolte protopolitique*. Éditions du Croquant.

Ministry of Justice. (2023). *Action against terrorist material online*. https://www.government.se/press-releases/2023/01/action-against-terrorist-material-online/

Mohammed, M. (2007). Les voies de la colère: « Violences urbaines » ou révolte d'ordre « politique » ? L'exemple des Hautes-Noues à Villiers-sur-Marne. *Sociologos*, (2). https://doi.org/10.4000/socio-logos.352

Moors, H., Baetens, T., Dijkstra, P., Maessen, J., Vegte, H., Wijngaart, M., & Willemsen, K. (2020). *Het gebeurt: Over sociale onrust in de Schilderswijk*. https://doi.org/10.13140/RG.2.2.13113.03680

Moors, H., Klarenbeek, L., Berger, E., Dückers, M., Duin, M., Kist, G., Luesink, M., Schijvenaars, T., Wijngaart, M., Maessen, J., & Broekmans, V. (2022). *Avondklokrellen: Lokale dynamiek in een mondiale crisis. Analyse van de voedingsbodem van de ordeverstoringen in vier Noord-Brabantse steden*. https://doi.org/10.13140/RG.2.2.35206.45128

Moors, H. (2023). Protest in Coronatijd. Kijken naar maatschappelijke onrust en rellen. In *Cahiers Politiestudies*, 67, 215-248.
https://www.researchgate.net/publication/376595553_Protest_in_Coronatijd

Murphy, J. (2023). Policing and peace in Northern Ireland: Change, conflict, and community confidence. In R. Wilford & A. Aughey (Eds.), *The Routledge handbook of the Northern Ireland conflict and peace* (pp. 324–337). Routledge. https://doi.org/10.4324/9781003224372-28

Naber, C. (2022, 18 april). Zweedse politie linkt geweld rond campagne Deense 'koranverbrander' aan criminele bendes. *Algemeen Dagblad*. https://www.ad.nl/buitenland/zweedse-politie-linkt-geweld-rond-campagne-deense-koranverbrander-aan-criminele-bendes~a68bcc759/

Nationale ombudsman. (2018). *Demonstreren, een schurend grondrecht?* (Rapport 2018/015). https://research.rug.nl/files/77302389/2018_015_RAPPORT_Demonstreren_een_schurend_grondrecht.pdf

Nationale ombudsman. (2026). *Sta voor protest! Een onderzoek naar de mate waarin de overheid het demonstratierecht behoorlijk beschermt en faciliteert*.
https://www.nationaleombudsman.nl/system/files/onderzoek/20260043-sta-voor-protest.pdf

Oberti, M., & Le Gall, M. G. (2023). Les territoires des émeutes: La ségrégation urbaine au cœur des violences. *La Vie des Idées*. https://laviedesidees.fr/Les-territoires-des-emeutes

Oksanen, P. (2023). History as a battlefield: Russia's information war against Finland. *World Literature Today, 97*(4). https://doi.org/10.1353/wlt.2023.a901373

Pamment, J., & Tsurtsumia, D. (2025). *Beyond Operation Doppelgänger*. Lund University Psychological Defence Research Institute.
https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelg%C3%A4nger.pdf

Pamment, J., & Isaksson, E. (2024). *Psychological defence: Concepts and principles for the 2020s*. Swedish Psychological Defence Agency. https://mpf.se/psychological-defence-agency/publications/archive/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s

Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fållhed, A. (2024). *Countering information influence activities: A handbook for journalists*. Swedish Psychological Defence Agency.
https://mpf.se/download/18.5ed1a83718d2a5fd639d524/1706648817558/countering-information-influence-activities-a-handbook-for-journalists.pdf

Pamment, J., Falkheimer, J., & Isaksson, E. (2023). *Malign foreign interference and information influence on video game platforms: Understanding the adversarial playbook*. Swedish Psychological Defence Agency. https://mpf.se/psychological-defence-agency/publications/archive/2023-12-01-malign-foreign-interference-and-information-influence-on-video-game-platforms-understanding-the-adversarial-playbook

Polisen. (2026). *The Swedish Police Authority*. https://polisen.se/en/the-swedish-police/the-swedish-police-authority/

Postma, L., De Boer, D., & Bantema, W. (2025). *Schuldig tot het tegendeel bewezen is? Een evaluatie van de (online) aanpak van een gemeente en politie naar aanleiding van online onrust*. Thorbecke Academie.

Psychological Defence Agency. (2023). *Don't be fooled: A handbook to help you recognise and deal with disinformation, misleading information, and propaganda*. Swedish Psychological Defence Agency.

Ranstorp, M., & Ahlerup, L. (2024). *The LVU campaign: The disinformation campaign against Swedish social services: Disinformation, conspiracy theories and domestic-international links related to malign influence activities by non-state actors.* Swedish Defence University. https://fhs.diva-portal.org/smash/get/diva2:1874819/FULLTEXT01.pdf

Sveriges Riksdag. (2025). *Polislag (1984:387)*. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/polislag-1984387_sfs-1984-387/

Roché, S. (2006). *Le frisson de l'émeute: Violences urbaines et banlieues*. Seuil.

Roorda, B., Swart, N., Bekkering, J., & Winter, H. (2026, 5 mei). Een rapport op de plank? Conclusies WODC-onderzoek naar demonstratierecht vinden weinig gehoor bij kabinetten-Schoof en -Jetten. *Montesquieu Instituut*. https://www.montesquieu-instituut.nl/column/202605/een-rapport-op-de-plank-conclusies-wodc-onderzoek-naar-demonstratierecht-vinden

Saqué, S. (2025). Qui a peur des mouvements sociaux? *Socialter, 72*(6), 70–71.

Sastramidjaja, Y. M. (2025). Connective spaces of radical hope: Rhizomatic youth struggles for viable futures in Southeast Asia. *Journal of Youth Studies, 28*(6), 867–884. https://doi.org/10.1080/13676261.2025.2556927

Sauvadet, T. (2023). *Voyoucratie et travail social: Enquêtes dans les quartiers de la politique de la ville*. Éditions du Croquant.

Scerri, D. (2024). An educational response to the "Prevent Duty" in England and Wales. *Critical Studies on Terrorism, 17*(2), 304–328. https://doi.org/10.1080/17539153.2024.2319886

Schierup, C. U., Ålund, A., & Kings, L. (2014). Reading the Stockholm riots: A moment for social justice? *Race & Class, 55*(3), 1–21. https://doi.org/10.1177/0306396813509191

Seger, E., Perry, H., & Hancock, J. (2025). *Epistemic security 2029: Fortifying the UK's information supply chain to tackle the democratic emergency*. Demos. https://demos.co.uk/wp-content/uploads/2025/02/Epistemic-Security-2029_accessible.pdf

Sharp, G. (2010). *From dictatorship to democracy: A conceptual framework for liberation* (4th ed.). Albert Einstein Institution.

Siegel, I., & Klos, M. (2024). Straffe desinformatiewetgeving? Bedenkingen vanuit Franse en Europese Unie-wetgeving. *Ars Aequi, 73*(7/8), 682–691. https://scholarlypublications.universiteitleiden.nl/access/item%3A4082154/view

Suliman, A. (2022, January 6). Sweden sets up Psychological Defence Agency to fight fake news, foreign interference. The Washington Post.

Sveriges Radio. (2014). *Riot report: Police methods raised tension in Husby*. https://www.sverigesradio.se/artikel/5861906

Sveriges Radio. (2022). *Police union calls for independent review of how riots were handled*. https://www.sverigesradio.se/artikel/police-union-calls-for-independent-review-of-how-riots-were-handled

Swart, N. J. L., Roorda, B., Bekkering, C. V. J., Zuidberg, N. S., Krol, E., Winter, H. B., & Bemelmans, J. H. B. (2025). *Het recht om te demonstreren in de democratische rechtsstaat*. Rijksuniversiteit Groningen.

Swedish Ministry of Defence. (2023). *Increased spread of disinformation directed towards Sweden*. https://www.government.se/press-releases/2023/07/disinformation/

Toft, A. (2024). "But it's really about …" Norwegian media coverage of the Qur'an burnings in Sweden and Norway in April 2022. *Temenos: Nordic Journal for the Study of Religion, 60*(1), 105–129. https://doi.org/10.33356/temenos.136707

Truong, F. (2015). Retour sur les raisons de la colère: La mort, les "conneries" et la haine, dix ans après. *Agora débats/jeunesses, 70*(2), 47–58.

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The Digital Services Act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology, 15*(1), 83–106. https://doi.org/10.1080/17579961.2023.2184136

Uhnoo, S., & Hansen Löfstrand, C. (2018). Voluntary policing in Sweden: Media reports of contemporary forms of police–citizen partnerships. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 19*(1), 41–60. https://doi.org/10.1080/14043858.2018.1439635

Van der Linden, S. (2023) *Foolproof. Why we fall for misinformation and how to build immunity*, Harper Collins, London

Van Hoboken, J., Appelman, N., Fathaigh, R. O., Leerssen, P., McGonagle, T., Van Eijk, N., & Helberger, N. (2019). *Het juridisch kader voor de verspreiding van desinformatie via internetdiensten en de regulering van politieke advertenties*. IViR.

Van Rijsingen, H., & Bomers, L. (2013). Rellen in Stockholm: Wat is er aan de hand in Zweden? *EenVandaag*. https://eenvandaag.avrotros.nl/artikelen/rellen-in-stockholm-wat-is-er-aan-de-hand-in-zweden-45969

Van Vark, A. (2025) *Separation and immersion : the changing role of the armed forces in Northwestern liberal democracies,* doctoral thesis Universiteit Leiden

Vergani, M., Giovannetti, A., Liao, K., Li, X., Ng, S., & Goodhardt, D. (2026). *The 2024 UK riots: Tracing the path from online activity to offline mobilisation*. Deakin University. https://dro.deakin.edu.au/articles/report/The_2024_UK_Riots_Tracing_the_Path_from_Online_Activity_to_Offline_Mobilisation/31975392

Verma, A., Sear, R., Restrepo, N. J., & Johnson, N. F. (2025). *City riots fed by transnational and trans-topic web-of-influence* [Preprint]. *arXiv*. https://arxiv.org/abs/2502.17331

Vugts, P. (2025). Vredeseenheid bewaakt met zachte hand de orde tijdens demonstraties: "Sfeer nog steeds gemoedelijk, iedereen in de olie". *Het Parool*. https://www.parool.nl/misdaad/vredeseenheid-bewaakt-met-zachte-hand-de-orde-tijdens-demonstraties-sfeer-nog-steeds-gemoedelijk-iedereen-in-de-olie~b4a54851/

Wacquant, L. (2023). *Misère de l'ethnographie de la misère*. Raisons d'agir.

Walgrave, S., Van Laer, J., Verhulst, J., & Wouters, R. (2010). Why people protest: Comparing demonstrators' motives across issues and nations. In M. Giugni & M. T. Grasso (Eds.), *The diversity of protest: Comparative perspectives on political participation by social movement participants* (pp. 13–34). Wiley-Blackwell. https://medialibrary.uantwerpen.be/oldcontent/container2608/files/Walgrave%20et%20al_%20(2010)_%20Why%20people%20protest.pdf

Winter, H., Boxum, C., Cazemier, J., Drouen, T., & Roest, S. (2025). *Internationale verkenning bevoegdheden online gegevensvergaring politie bij (dreigende) openbare ordeverstoringen*. Pro Facto.

Wolsink, J. & Ferwerda, H. (2022). *Het fenomeen vechtafspraken, vier jaar later*. Sdu.

think. do. connect.

E:M+MA.
Wijnhaven 88
2511 GA Den Haag
070 - 87 00 460
info@emma.nl
www.emma.nl
Volg ons op LinkedIn