



Hoe online extremistische broedkamers een nieuwe generatie van geweld kweken

Augustus 2025



Van meme tot moord

Hoe online extremistische broedkamers
een nieuwe generatie van geweld kweken

Auteurs:

Gerben Bakker, Thijs van Aken, Philippe van Pappelendam
en Julie Jeuken

Met medewerking van:

“Mary” (onafhankelijk OSINT-deskundige, actief voor
Capitol Terrorists Exposers); Team Strategieontwikkeling
Nederlandse politie; Verschillende politiemedewerkers en
OSINT-deskundigen die omwille van hun heimelijke functie
en/of taakstelling ongenoemd blijven; Paul Sinning.

Cover foto gemaakt met AI.

Augustus 2025

Dit onderzoek is verricht door HCSS in opdracht van de
Nederlandse politie. Het onderzoek voor dit rapport is
afgerond in augustus 2025. Gebeurtenissen of ontwikkelingen
die plaatsvonden in de periode tussen afronding en publicatie
zijn niet van invloed geweest op de bevindingen.

© *The Hague* Centre for Strategic Studies behoudt zich alle
rechten voor. Geen enkel onderdeel van dit rapport mag
gereproduceerd of gepubliceerd worden in welke vorm
dan ook, in print, microfilm, fotografie, of op enig andere
manier zonder voorafgaande schriftelijke toestemming van
HCSS. De rechten van alle foto's zijn voor behouden aan hun
respectievelijke eigenaars.

Inhoudsopgave

Take-aways	IV
Managementsamenvatting	V
1. Inleiding	1
1.1. Doel en onderzoeksvraag	2
1.2. Aanpak	3
1.3. Definities	3
2. Online extremisme: Een eigenstandige generatie?	5
2.1. Rapoports vier golventheorie	5
2.2. De vijfde golf van gewelddadig extremisme: de 'Digitale Golf'?	6
3. Omvang en aantrekkingskracht van het online ecosysteem	8
3.1. De structuur van online ecosystemen	8
3.2. De onderlinge verwevenheid van extremistische biotopen	10
3.3. Beperkt zicht op de omvang	13
3.4. Wat we wél kunnen zeggen over de omvang en het bereik	15
3.5. De aantrekkings- en verstrikkingskracht van online omgevingen	16
4. Trends en online extremistische ecosystemen	20
4.1. Meme-propaganda	20
4.2. Ideologische hybridisatie	22
4.3. Gamificatie van extremisme: 'fun' als vehikel voor geweldsideologie	23
4.4. Nihilistische en misantropische geweldsverheerlijking	25
4.5. Manifesten en digitaal martelaarschap	26
4.6. 'Hybrid net activism' en 'leaderless resistance'	27
5. Implicaties voor de maatschappelijke stabiliteit in Nederland	30
5.1. Online geïnspireerd terrorisme en extremistisch geweld	30
5.2. Druk op de democratische rechtsorde	36
5.3. Sporen van vervloeiing met statelijke actoren	40
6. Strategische aandachtspunten	42
6.1. Naar een betere kennispositie	42
6.2. Naar meer politieke focus en wettelijke bewegingsruimte	44
6.3. Naar een adaptieve preventie en aanpak	46

Take-aways

Online extremisme is geen margeverschijnsel, maar een steeds duidelijker beginpunt voor hoe we naar extremisme moeten kijken. De digitale ruimte voor extremisme is dynamisch, groeiend, en biedt vrijwel onbegrensde mogelijkheden om te radicaliseren. Langzaam maar zeker lijkt deze ruimte ook een ander profiel van extremistisch ouderschap op te leveren (en tevens slachtofferschap): jong en digitaal mobiel, internationaal communicerend, ideologisch diffuus, opgegroeid in digitale biotopen met vaak zeer extreme content. We moeten er rekening mee houden dat geweld vaker vanuit deze online biotopen ontstaat.

De verjonging in digitale extremistische netwerken is zichtbaar en zorgwekkend. Een deel van de jongste generaties wordt blootgesteld aan extreem haatdragende, gewelddadige en antidemocratische content. Eenmaal in actieve kanalen opgenomen, vinden versnelde groepsdynamische processen plaats van radicalisering, grooming en desensitisering die (langdurige) mentale schade veroorzaken en een nieuwe risicogroep kunnen baren.

Doelgerichte extremistische voetafruk op het mainstream politieke en publieke domein vormt een risico voor onze rechtorde. Extremistische groepen zijn strategisch uit op normalisering van geweld of ultraradicalen standpunten in de politieke en publieke ruimte. Er liggen lijnen van online cellen naar aangejaagde fysieke (flits-)protesten of ordeverstoringen. Ook zijn er sporen van statelijke inmenging, maar de precieze aard daarvan is onvoldoende in beeld. Over het geheel genomen zijn deze invloedsrelaties even gevaarlijk als complex als ze niet worden onderzocht en in de gaten gehouden.

Zogenaamd 'Nihilistisch Gewelddadig Extremisme' staat nog slecht op het netvlies van zowel de samenleving als de veiligheidssector. De afgelopen jaren heeft zich een ultragewelddadig niche-netwerk kunnen ontwikkelen op Discord en Telegram, dat door de eigen leden ook wel wordt aangeduid met de term 'COM'. (Zeer) jonge leden worden voor deze netwerken gegroomd en (vaak) op basis van sextortion door andere leden aangezet tot geweld, afpersing van andere leden of –incidenteel— zelfmoord. Een beter zicht op deze netwerken is nodig vanuit het oogpunt van preventie, deradicalisering en bescherming van (Nederlandse) kinderen en jongeren die hierbij betrokken kunnen raken.

Het relatieve aandeel veroordeelden voor terroristische misdrijven dat online inspiratie vindt, groeit. Ook al zijn definitieve conclusies lastig door een gefragmenteerd gegevensbeeld: Op basis van analyse van de Nederlandse veroordeelden voor terroristische misdrijven over de afgelopen tien jaar zien we de voorzichtige ontwikkeling dat de digitale wereld een nadrukkelijker rol begint te spelen, evenals de aanwezigheid van mentale gevoeligheden zoals psychologische stoornissen of trauma's. Dit soort onderzoek naar de preciezere rol van digitale radicalisering verdient voortzetting en verdieping.

Er ontbreekt in Nederland belangrijke kennis over online extremistische ecosystemen. Er zijn in Nederland onvoldoende monitoringinitiatieven van online extremistische groepen en dynamiek. Dit lijkt te maken met een gebrek aan bewustzijn en urgentiegevoel, en met de angst om de erg strikte Nederlandse privacy-normen te breken. Het gevolg is dat we slecht in beeld hebben hoe omvangrijk online netwerken zijn, wat het Nederlandse aandeel is, en hoeveel reikwijdte en impact ze hebben.

Zonder de (op)waardering van OSINT-deskundigheid en investering in OSINT-capaciteit komen we in Nederland nergens. Preventie en opsporing van online extremisme vergt specialistische kennis en inspanning. Het kost tijd en vraagt expertiseopbouw om subculturen, hun memes en taal te begrijpen en toegang te krijgen tot de meer verborgen extremistische netwerken. Zowel binnen de overheidsveiligheidssector als daarbuiten moet worden gebouwd aan een sterke OSINT onderzoeksinfrastructuur om mee te kunnen blijven bewegen met de steeds complexere dynamiek van digitale netwerken.

Management-samenvatting

Online extremisme is geen margeverschijnsel, eerder een steeds meer leidend verschijnsel. Aanslagen lijken soms uit het niets te komen, gepleegd door soms zeer jonge, snel geradicaliseerde daders die buiten de blik van opsporingsinstanties bleven. De snelle dynamiek en het aanpassingsvermogen van online groepen is zorgwekkend. Het domein van haatdragende, (extreem) gewelddadige content blijkt bovendien hardnekkig. In extremistische kanalen (maar juist ook in alle openheid op mainstream platformen) vindt een zorgwekkende normalisering plaats van extreem geweld en antidemocratische denkbeelden. De impact op de samenleving werkt dan ook door op meerdere punten.

Top concerns. Voor de nabije toekomst levert de verkenning enkele *top concerns* op:

1. *Meer kans op online geïnspireerd extremistisch geweld.* Extremistische geweldpleging is vaker geworteld in digitale radicaliseringsprocessen. Zo ontstaat een ander profiel van terroristisch en extremistisch daderschap (en tevens slachtofferschap): jong en digitaal mobiel, internationaal communicerend, ideologisch diffuus, opgegroeid in digitale biotopen met vaak zeer extreme content. We moeten er rekening mee houden dat geweld vaker vanuit deze online biotopen ontstaat.
2. *Beschadiging van jongeren.* Een deel van de jongste generaties wordt voortdurend blootgesteld aan haatdragende, gewelddadige en antidemocratische content. Het gaat om jongeren, tieners, soms zelfs kinderen die om allerlei redenen worden aangetrokken tot kanalen. Eenmaal in de meest extreme kanalen opgenomen, vinden mogelijk processen van radicalisering, grooming en desensitisering plaats die (langdurige) mentale schade veroorzaken en een nieuwe risicogroep baren.
3. *Weinig greep op de impact op de democratische rechtsorde.* De impact van online extremisme op de maatschappelijke stabiliteit is aanwezig maar hebben we slecht in beeld. Technologische condities versnellen de verspreiding. Extremistische content loopt op allerlei manieren over naar het mainstream politieke en publieke domein. Er liggen lijnen van online cellen naar fysieke (flits-)protesten. Ook zijn er sporen van statelijke inmenging maar de precieze aard daarvan hebben we nauwelijks in beeld.

Omvang van het online extremistische ecosysteem. Online extremisme manifesteert zich niet in overzichtelijke ideologische blokken, maar in een gefragmenteerd web van open en gesloten netwerken. Deze bestaan uit talloze biotopen, zoals de manosfeer, islamogram, Siege, de manosfeer of bijvoorbeeld ecofascistische niches, die deels overlappen. Onder wisselende namen duiken ze op en verdwijnen weer. De structuur lijkt op een dynamisch-adaptief ecosysteem. Dit maakt het ook erg ingewikkeld om overzicht te genereren. Ook praktische zaken staan daarbij in de weg. Versleutelde communicatie, vluchtige platformstructuren, moeilijk te doorgronden memes, in-grouptaal en technische barrières (zoals gesloten API's) zorgen ervoor dat het extremistisch verkeer moeilijk te monitoren is. Dat laat onverlet dat sommige studies een hele hoge verspreidingsgraad laten zien. Extreem gewelddadige kanalen, waarop executies en misbruikfilmpjes worden gedeeld, hebben soms wel honderden tot duizenden leden.

Aantrekkings- en verstrikkingskracht. Jongeren, tieners, en soms kinderen van 8 tot 12 jaar raken verstrikt in extreem gewelddadige biotopen. De aantrekkingskracht is deels psychologisch: ze lijken sociaal geïsoleerde jongeren te voorzien in de behoefte aan identiteit, sociale erkenning, status en een verklarend wereldbeeld. De ‘verstrikkingskracht’ is gebaseerd op – vaak doelgerichte groepstactieken van – love bombing en groomingtactieken, door desensitisering door frequente blootstelling aan extreem gewelddadig materiaal. Zorgwekkend is met name het gebrek aan zicht op jongeren die verstrikt raken in digitale subculturen, meestal zonder dat ouders daar ook maar enige notie van hebben.

Trends in uitingsvormen en kenmerken. Online extremisme is niet ‘slechts’ een vorm van radicalisering met digitale middelen. Juist de diffuse, cynische en visueel verpakte uitingen maken online extremisme tot een eigenstandige motor van radicalisering en destabilisatie. Specifieke kenmerken maken de verspreiding en impact zeer succesvol en onttrokken aan de blikken van outsiders.

- *Memes en meme-propaganda.* Internethaat weet zich te verpakken in een cynische beeldcultuur. Dit heeft meerdere functies die vaak een strategisch doel dienen, zoals groomen, provoceren of mainstreaming (het verzachtend verpakken van steeds extremere denkbeelden die daardoor eenvoudiger verspreid raken).
- *Gehybridiseerde ideologie.* In de online wereld vloeien ideologieën samen tot hybride overtuigingen die zich niets aantrekken van oude politieke scheidslijnen. Een gebruiker kan tegelijk misogyn, ecologisch en antisemitisch zijn, zonder zichzelf ooit als ‘extremist’ te beschouwen. Het resultaat is een grillige en moeilijk te voorspellen mix van radicale sentimenten.
- *Gegamificeerd geweld.* Geweldsideologie krijgt een speels jasje op gaming platforms. Gamificatie verlaagt de morele last, door bijvoorbeeld te refereren aan een puntenscore als het gaat om werkelijke moord. Ook dienen game platforms soms als trainings- of rekruteringsomgeving.
- *Nihilistische geweldsverheerlijking.* In bepaalde subculturen is geweld geen middel, maar het doel op zich. Hier bloeit een nihilisme en een sadisme dat zich uitdrukt in het delen van de meest extreme content en een grooming- en chantagesystematiek waarbij jongeren worden gedreven tot moord, seksueel kindermisbruik of zelfmoord.
- *Manifesten en digitaal martelaarschap.* Extremisten zijn steeds vaker ook de maker van obscure manuscripten waarin quasi-intellectuele wereldbeelden en rechtvaardigingen voor geweld worden gegeven. Morbide geweldshandleidingen of e-zines blijven eindeloos op het internet rondzwerven en gaan bovendien gelden als documenten van martelaarschap nadat er aanslagen gepleegd zijn.
- *Hybrid net activism.* Iedereen is uitvoerder, niemand is leider. Online extremisme volgt geen bevelslijnen maar netwerken van symbolen, inside jokes en gedeelde frustraties. Juist door de afwezigheid van structuur ontstaat een krachtig, quasi-zelforganiserend geheel dat zich ultrasnel en tegelijk moeilijk beheersbaar kan mobiliseren in de offline wereld.

Strategisch aandachtspunt #1: Naar een betere kennispositie. Online extremisme vereist dat beleidsmakers een andere manier van kijken ontwikkelen. Klassieke categorisering matchen niet meer met de vloeibare en veranderlijke kenmerken van digitale extremistische ecosystemen. Daarom moet worden ingezet op meer mogelijkheden voor monitoring en kennisopbouw om de structuur van het ecosysteem, de taal, de patronen en de effecten beter te leren begrijpen. Deze kennisopbouw vereist samenwerking met digitale platforms, investering in de ontwikkeling van analyse-instrumentatie, de inzet van OSINT-methoden, de betrokkenheid van OSINT-experts (ook buiten de politie), en het opbouwen van een ‘mee-ademend’ referentiekader van extremistische symboliek. Geautomatiseerde monitoring en moderatie

zijn nodig maar niet zaligmakend. Kennisontwikkeling moet gepaard gaan met interpretatie en infiltratie door specialisten. Investeren in dit type menselijke capaciteit is dan ook van zeer groot belang.

Strategisch aandachtspunt #2: Naar meer politieke focus en wettelijke bewegingsruimte.

De opkomst van online extremisme vraagt om een beleidsblik die bereid is om de digitale dreiging als beginpunt te nemen en niet als een zijdelingse uitingsvorm. Wet- en regelgeving moeten bewegingsruimte bieden. Daarbij dient men alert te blijven op de balans tussen ingrijpen en rechtsstatelijkheid. Op Europees niveau vereist dit inzet op digitale soevereiniteit. In de Nederlandse wettelijke context moet kritisch worden beoordeeld in hoeverre wettelijke kaders volstaan. Privacybescherming heeft geleid tot een extreme huiver voor gegevensverwerking wat strategische kennisopbouw belemmert. Hostingpartijen worden nog steeds stevig beschermd. De wetgever staat voor de opgave om een werkbaar evenwicht te vinden.

Strategisch aandachtspunt #3: Naar een adaptieve preventie en aanpak.

De effectieve aanpak vereist naast klassieke opsporing mogelijk fundamenteel andere benaderingswijzen. Omdat de dynamiek snel, vloeibaar en organisch is, is een adaptieve respons nodig, inspeliend op de aantrekkingskracht en de groepsdynamische processen. Dit vraagt om grondige kennis van groepen en hun subteksten. Ook de sociale omgeving speelt een sleutelrol: digitale weerbaarheid begint aan de keukentafel of in de klas, waar internetgedrag bespreekbaar moet worden gemaakt. Dit vergt een maatschappelijke bewustwordingsagenda die niet alleen voor de rekening komt van de overheid. Daarnaast verdienen online contranarratieven erkenning als remmende kracht. Al deze zaken beginnen echter bij kennis en OSINT-specialisten die deze kennis kunnen ontginnen en begrip hierover kunnen verspreiden.

1. Inleiding

Online extremisme is geen margeverschijnsel maar steeds meer een leidend verschijnsel. Steeds vaker lezen we over extremistische jonge daders die schijnbaar vanuit het niets aanslagen plegen en daarbij online manifesten achterlaten of hun daden zelfs live-streamen. We horen dat jongeren soms vereenzaamd raken en hun heil zoeken in gesloten online gemeenschappen en slachtoffer worden van grooming. Wat er precies gebeurt in deze online omgevingen blijft obscuur voor velen die de taal en mores van internetcultuur niet begrijpen. Dat is een probleem. Want de risico's zijn groeiende, terwijl de kennis erover sterk achterblijft.

Extremisme werd gewoonlijk benaderd als een fenomeen dat te maken had met 'papieren' ideologieën en fysieke organisaties en cellen zoals Islamitische Staat (IS) of de vroegere Rote Armee Fraktion (RAF). Deze kijk is nog steeds relevant, maar de digitale werkelijkheid opende een eigen dimensie van extremisme met een veel onoverzichtelijker en 'messy' dynamiek. Online zien we grilligere en versnelde radicaliseringsprocessen, en een alarmerende verjonging van daders en slachtoffers. Ook de taal en de vorm van communicatie weerspiegelt de uniciteit van internetcultuur met eigen gedragseffecten en tactieken. Het internet is bovendien zijn onschuld allang voorbij. Geweld blijkt te kunnen opbloeien uit een giftige cocktail van meme-propaganda, blootstelling aan *gore* content, uitgegroeide frustraties over de fysieke realiteit, een barrage aan complotgedachten en desinformatie, in combinatie met een hogere vatbaarheid door psychische problemen of empathische onvolwassenheid.

In deze strategische verkenning claimen we dat online extremisme geen margeverschijnsel is en reële risico's met zich meebrengt. Deze risico's hangen samen met enkele belangwekkende trends die wijzen op versnelling en versterkte hang naar extreem geweld. We brengen deze trends in beeld en verkennen de mogelijke implicaties op basis van signalen. Onderweg wordt daarbij steeds duidelijker dat online extremisme serieuze aandacht verdient maar ook een specialistische aandacht die een beter begrip veronderstelt van de eigentijdse werking van internetcultuur en -gedrag.

Ook gelet op de aanpak verdient online extremisme in de toekomst een sterker ontwikkeld onderzoeksveld naar de typologie, de ecologie en de psychologische gedragspatronen die er gelden. Met dat begrip ontstaat er ook meer kans om extreem toxische omgevingen te verstoren en te voorkomen dat kwetsbare jongeren afglijden in subculturen die onuitwisbare voetafdrukken achterlaten. Processen van signalering en opsporing zullen mogelijk een draai moeten maken. Het wettelijk kader zal beter moeten 'mee-ademen' met de dynamiek. Professionals in de contraterrorisme en terrorismeketen zijn vaak 'opgevoed' in de tijd van relatief duidelijk aanwijsbare terroristische organisaties. Die ervaring en die kijk moeten we niet naar de prullenbak verwijzen. Maar online speelt er van alles door elkaar en gelden er wetmatigheden die specialistische kennis en interventies behoeven.

We constateren dat er in het veiligheidsdomein pas hier en daar bewustzijn ontstaat over hoe omvangrijk en invloedrijk online extremistische ecosystemen zijn. Voor velen die niet bekend zijn met eigentijdse internetcultuur is het ver weg. Maar met het oog op de risico's kunnen we ons geen schouderophalen permitteren. Het is in onze ogen belangrijk dat het onderwerp steviger op de agenda komt te staan en dat meer mensen met deze werelden bekend raken.

1.1. Doel en onderzoeksvraag

Het doel van deze strategische verkenning is om de rol en ontwikkeling van online extremisme als relatief eigenstandige factor voor eigentijds (terroristisch) geweld te begrijpen en te duiden. Om dit doel te bereiken beantwoorden we in deze analyse de volgende onderzoeksvraag:

“Zien we, onder invloed van online ecosystemen, een nieuw type golf van extremistisch geweld opkomen, en zo ja, welke krachten zetten deze ontwikkeling in, welke trends en aanwijzingen wijzen dan die kant op, en wat zijn de implicaties daarvan voor de Nederlandse maatschappelijke stabiliteit?”

Onder deze vraagstelling ligt de hypothese dat de dominante rol van online ecosystemen sterk bijdraagt aan een veranderend beeld van (terroristisch) geweld tegen de democratische rechtsorde. We veronderstellen dat er aanwijsbare trends en verbanden bestaan tussen uitingen van extremistisch en terroristisch geweld en de rol van internetcultuur als facilitator en incubator voor radicalisering.

Voor wie is dit paper? Dit paper is opgesteld als een strategische verkenning binnen het kader van het Strategisch Monitor Politie programma. De studie heeft als doel om de politie en bredere veiligheidssector te voorzien van inzichten die raken aan (risico's voor) de maatschappelijke stabiliteit. De verdiepende analyse is tevens van waarde voor beleidsmakers en onderzoekers die zich bezighouden met (online) radicalisering en extremistische netwerken.

Hoe kwam dit paper tot stand? Deze verkenning kwam tot stand op basis van een combinatie van bronnen. Naast raadpleging van literatuur, beleidsdocumenten en relevante rapportages zijn digitale bronnen, waaronder beeldmateriaal en chat exports, geanalyseerd. Ter verdieping zijn achtergrondgesprekken gevoerd met OSINT-specialisten en deskundigen uit de opsporingspraktijk.

1.2. Aanpak

De analyse is als volgt gestructureerd:

- **Stap 1. Een nieuwe generatie extremistisch geweld?** We bespreken op een conceptuele manier waarom online extremisme mogelijk een eigen generatie van extremisme beschrijft.
- **Stap 2. De omvang en aantrekkingskracht van het 'web van haat.'** Wat is er te zeggen over de omvang en aantrekkingskracht van extremistische online ecosystemen?
- **Stap 3. Trends en online extremistische ecosystemen.** Welke trends laten zien dat online extremistische ecosystemen gekenmerkt wordt door actuele uitingsvormen van geweld?
- **Stap 4. Implicaties voor de maatschappelijke stabiliteit.** Wat betekenen de besproken bevindingen als het gaat om de impact voor de maatschappelijke stabiliteit?
- **Stap 5. Strategische aandachtspunten.** Welke strategische richtingen zijn nodig om naar deze nieuwe ontwikkelingen te kunnen accommoderen?

1.3. Definities

Online geïnspireerd extremistisch geweld en terrorisme. Het is belangrijk om onderscheid te maken tussen (online) extremisme, extremistisch geweld en terrorisme. Tegelijkertijd veronderstellen we in deze analyse dat online extremisme en terrorisme soms in elkaars verlengde liggen. Centraal in deze verkenning staat niet het terrorisme als de uitkomst van (online) radicaliseringsprocessen, maar de performatieve werking van de digitale wereld als factor in extremistisch geweld en terrorisme. Online geïnspireerd terrorisme lijkt bijvoorbeeld toch iets anders dan terroristische cellen die het internet gebruiken om elkaar te emailen of appen.¹ Zoals we eerder benadrukten: online extremisme is een opzichzelfstaande kracht met, in sommige gevallen, uiterste terroristische geweldsconsequenties.²

Online extremisme in overlap met digitale haat. Online radicalisering en extremisme kunnen uitmonden in een terroristische daad, maar dit is lang niet de enige uitingsvorm in het bredere repertoire van extremisme. Vaak manifesteert extremisme zich in minder fysieke gedragingen: trollen, doxxing, intimidatie, haatmisdrijven, en vooral digitale haatuitingen.³ Zo hebben diverse vormen van extremisme in Nederland uiteindelijk geen terroristische impact, maar dragen ze wel bij aan de uitholling van de democratische rechtsorde.⁴

Een probleem is dat binnen de online sfeer het onderscheid tussen extremistische uitingen, digitale haat en daadwerkelijk strafbare uitspraken bijzonder diffuus is. Veel verwerpelijke content valt onder de noemer 'awful but lawful': kwetsend maar niet per se vervolgbaar. Hoewel er in het strafrecht ruimte bestaat om haatmisdrijven, bevinden uitingen zich vaak (en ook bewust) onder de drempel om als haatmisdrijf te kunnen worden vastgepind. Dit wordt

¹ Ware, J., *The Third Generation of Online Radicalization*, 2023.

² In een voorgaande analyse definiëren we geweld aan de hand van een synthese van wetenschappelijke definities als "het opzettelijk gebruik van fysieke kracht of macht, hetzij dreigend of daadwerkelijk, tegen zichzelf, een andere persoon, een groep of een gemeenschap, dat resulteert in of mogelijk resulteert in letsel, dood, psychologische schade, ontwikkelingsachterstanden of deprivatie." Van belang is dat geweld, ook zeker vanuit extremistische hoek, kan verwijzen naar zowel fysieke als niet-fysieke schade die wordt toegebracht. Opzettelijkheid blijft in deze definitie echter altijd een criterium. Zie ook, voor een uitgebreide analyse van geweld: HCSS, *Geweld aan de horizon: Trends omtrent geweld en maatschappelijke stabiliteit*, 2024. NCTV, *Dreigingsbeeld Terrorismen Nederland*, December 2024.

³ Schuurman, B., *Non-Involvement in Terrorist Violence, Perspectives on Terrorism*, 14(6), 2020.

⁴ HCSS, *Geweld aan de horizon: Trends omtrent geweld en maatschappelijke stabiliteit*, 2024. NCTV, *Dreigingsbeeld Terrorismen Nederland*, December 2024.

ook wel 'borderline content' genoemd. Die vaagheid, versterkt door kenmerken als anonimiteit, maakt het lastig om greep te krijgen op wat er gezegd wordt en hoe schadelijk dan wel vervolgbaar dat is. Hoewel deze verkenning zich dus focust op extremisme, gaat de aandacht ook uit naar de bredere voedingsbodem van haatuitingen en hoe deze een overstap biedt naar extremere biotopen.

Onderstaande definities worden gedragen door de auteurs en zijn een synthese van verschillende wetenschappelijke definities of definities in rapportages:

Extremisme: Een radicalisme gebaseerd op antidemocratische en intolerante denkbeelden die oproepen tot maatschappelijke of politieke verandering. Hoewel extremistische denkbeelden het gebruik van geweld verheerlijken, maken extremisten gebruik van zowel gewelddadige als niet-gewelddadige middelen.

Online extremisme: digitaal radicalisme waarbij extremistische denkbeelden, gericht tegen de democratische rechtsorde of maatschappelijke fundamentele waarden, zich ontwikkelen, verspreiden en verankeren binnen digitale omgevingen. Het internet fungeert als netwerkdomein waarin radicalisering wordt gefaciliteerd, versneld en gelegitimeerd, vaak buiten zicht van toezicht of tegenspraak.

Extremistisch geweld: De gewelddadige uitingsvorm van een extremistisch radicaliseringsproces. Extremistisch geweld kan bestaan uit (kleinschalige) geweldsincidenten en haatmisdrijven. Hoewel extremistisch geweld de vorm kan aannemen van terrorisme, uit extremisme zich ook in andere geweldsvormen.

Terrorisme: Een specifieke vorm van extremistisch geweld. Terrorismen is een tactiek van doelbewuste geweldsdaden tegen voornamelijk burgers, met als doel het veroorzaken van bredere propagandistische en psychologische effecten in de samenleving.

Online haat: Online haat, in relatie tot extremisme, verwijst naar zogenaamde 'borderline content'. Deze term wordt door de overheid gebruikt voor de aanduiding van (legale) online content 'dat geen strikt terroristisch karakter kent en zelfs niet altijd hoeft te leiden tot geweld, maar wel de veiligheid van burgers en instituties ondermijnt, bijvoorbeeld doordat het aanzet tot haat of opruiing of omdat de content extremistisch gedachtengoed normaliseert.'

Online radicalisering: Het proces waarin een individu zich extremistische denkbeelden of tactieken eigen maakt. Verschillende factoren op individueel-, groeps- en structuurniveau beïnvloeden dit proces. Radicalisering op het internet kenmerkt zich door meer geïndividualiseerde trajecten, ideologische hybriditeit (zie H4.2) en een post-organisatorisch karakter (zie H4.6).

2. Online extremisme: Een eigenstandige generatie?

Moeten we online extremisme beschouwen als een nieuwe generatie die wordt voortgebracht? In dit hoofdstuk verkennen we de ruimte voor de erkenning van online extremisme als een eigenstandig macroconcept.

2.1. Rapoports vier golventheorie

De vraag of we aan de vooravond staan van een nieuwe generatie extremistisch geweld roept de klassiek geworden theorie van David C. Rapoport in herinnering. In zijn 'vier golven-model' beschreef Rapoport hoe terroristische bewegingen zich sinds het einde van de negentiende eeuw ontwikkelden langs opeenvolgende historische stadia op basis van onderscheidende kenmerken. Elke golf duurde volgens Rapoport bij benadering veertig jaar, de tijd waarin in een generatie kon opkomen en weer aan relevantie kon inboeten.⁵ In dat licht is het relevant om te bezien of de digitale dimensie kan worden begrepen als het begin van een vijfde golf. De conceptuele perspectieven die in dit hoofdstuk worden besproken, bouwen voort op deze (speculatieve) gedachte.⁶⁷

⁵ Rapoport, D.C., *The Fourth Wave: September 11 in the History of Terrorism*, *Current History*, 100(650), 2001.

⁶ De vier golven-theorie van Rapoport is niet zonder kritiek. Zo dreigen groeperingen en daden die niet binnen een dominante golf passen uit het beeld te verdwijnen. Ook laat de nadruk op het globale en universele karakter van terrorisme weinig ruimte voor lokale oorzaken van extremistisch geweld. Daarnaast is het onduidelijk wanneer een golf dan echt is afgelopen en hoe dit kan worden gemeten. Desondanks biedt de theorie een handvat om duiding te geven aan opvallende en dominante ontwikkelingen op het gebied van terrorisme en extremisme.

⁷ Rapoport, D.C., *Terrorism*, *Encyclopedia of Violence, Peace, & Conflict*, 2022.

Figuur 1. De vier golven van modern terrorisme



2.2. De vijfde golf van gewelddadig extremisme: de 'Digitale Golf'?

Sinds Rapoports viergolventheorie speculeren academici over een vijfde golf, waarvan de periode 2020-2025 de beginfase zou markeren. De opkomst van de digitale samenleving wordt daarbij vaak als drijvende kracht gezien. Het internet speelt in deze 'Digitale golf' een cruciale rol in het faciliteren van een sterk geïndividualiseerd radicaliseringsproces, een waarin niet per definitie een enkele ideologie centraal staat.⁸ De vijfde golf van gewelddadig extremisme is daarmee een product van een veranderende tijdsgeest waarin individualiteit en identiteit ook meer naar de voorgrond treden.⁹ Ook de coronacrisis wordt aangemerkt als katalysator voor de blijvende versmelting van het digitale en het extremistische.¹⁰ In de traditie van Rapoport veronderstellen wij dat deze nieuwe Digitale golf is ontstaan en een unieke online extremistische cultuur faciliteert. Een aantal kenmerken zullen in dit rapport de revue passeren:

- *Hybridisatie van ideologie.* In de online extremistische cultuur bestaat een versmelting van diverse ideologieën en subculturen. Hoewel 'verzuilde' vormen van extremisme en terrorisme blijven bestaan (denk bijvoorbeeld aan IS of 'boomer' neonazi groepen), is de realiteit online een stuk vloeibaarder en onoverzichtelijker.¹¹ Online 'opgevoede' daders

⁸ Simon, D.D. & Jenkins, B.M., *Lone Wolf Terrorism: Understanding the Growing Threat*, 2013, pp. 25-34.

⁹ Kinvall, C. & Mitzen, J., *Anxiety, fear, and ontological security in world politics: thinking with and beyond Giddens*, *International Theory*, 12, 2020.

¹⁰ Colseatt, R. & Renard, T., *What the Zeitgeist can Tell us About the Future of Terrorism*, ICCT, 2022.

¹¹ Collins, J., *A New Wave of Terrorism? A Comparative Analysis of the Rise of Far-Right Terrorism*, *Perspectives on Terrorism*, 15(6), 2021; Bjørge, T., *Introduction to the Special Section on Anti-Government Extremism*, *Perspectives on Terrorism*, 17(1), 2023; Ribeiro M.H., e.a., *The Evolution of the Manosphere Across the Web*, 2021.

van extremistisch geweld lijken veel minder vaak een eenduidige ideologie te volgen, maar vormen een collage van individuele overtuigingen op basis van allerlei elementen en grieven (zie H3.2).¹² In hoofdstuk 4.2 spreken we uitgebreider over deze ideologische hybridisatie.

- *Post-organisatorische netwerken met eigen taal en gedrag dynamieken.* Online, 'post-organisatorische netwerken' zijn fluïde en strategisch gedecentraliseerd. Online groepen volgen vaak een eigen logica van aantrekking en verstriking gebaseerd op internetspecifieke communicatie en tactieken (zie H4.1).
- *Onbegrensde contentverspreiding via manifesten en virale content.* Digitale manifesten, filmpjes van executies, haatpropaganda en oproepen tot geweld vermenigvuldigen zich razendsnel met een wereldwijd bereik. Kenmerkend zijn meme-propaganda, gamificatie en 'nihilistische geweldsverheerlijking' (zie H4). Online extremisme is in staat mondiale narratieven te trechteren naar lokale impact.

Samenvattend biedt het model van Rapoport een (imperfecte) springplank om een nieuw(?) maar vooral eigenstandig perspectief op extremistische manifestaties in te ruimen. Onze benadering is daarbij niet wetenschappelijk maar vooral 'heuristisch' bedoeld. Het denken in termen van een eigenstandig digitaal extremistisch perspectief schept de voorwaarden om specifieke, belangwekkende kenmerken voor de toekomst scherper te ontwaren, zoals versnelling, hybridisatie, esthetisering en gamificatie, die het karakter van gewelddadig extremisme mogelijk ingrijpend veranderen, of dat al doen.

Figuur 2. De Digitale Golf van gewelddadig extremisme



¹² Gartenstein-Ross, D., e.a., *Composite Violent Extremism: Conceptualizing Attackers Who Increasingly Challenge Traditional Categories of Terrorism*, *Studies in Conflict & Terrorism*, 2023, p. 14.

3. Omvang en aantrekkingskracht van het online ecosysteem

Extremistische online ecosystemen vormen een complex en gelaagd verschijnsel¹³ waarvan de contouren steeds beter zichtbaar worden, maar waarvan de exacte omvang en groei lastig vast te stellen blijven. Dit hoofdstuk schetst achtereenvolgens de structuur, omvang en aantrekkingskracht van het ecosysteem van online extremisme.

3.1. De structuur van online ecosystemen

Als we nadenken over online extremisme volstaat het niet om te denken in duidelijk afgebakende ideologische 'kaartenbakken' van rechts-extremisme, jihadisme, enzovoort. Net zoals een biologisch ecosysteem moet ook het online extremistisch ecosysteem worden beschreven langs diverse niveaus van dynamische interactie.¹⁴ Traditionele ideologische stromingen vormen in het ecosysteem van online extremisme diffuse biotopen waarin een verscheidenheid aan subculturen eigen identiteiten en denkbeelden ontwikkelen.

Cellen en gemeenschappen zijn de 'basiseenheden' van digitale extremistische ecosystemen, bestaande uit websites, kleinere chatgroepen, besloten kanalen, enzovoort. Ze ontstaan vaak organisch door contentdeling en (culturele) nichevorming. Vanuit het oogpunt van opsporing zijn deze cellen ook sterk afgeschermd waardoor infiltratie vaak noodzakelijk is. Bijvoorbeeld:

- Fora of messageboards zoals 4chan, 8kun, of websites zoals de neonazistische blog The Daily Stormer.
- Besloten groepen of kanalen op platformen zoals Telegram of Discord. Denk bijvoorbeeld aan accelerationistische Telegram-kanalen, The Base of Atomwaffen Division.

¹³ Een verwijzing naar dit rapport: AIVD, [Een web van haat: De online grip van extremisme en terrorisme op minderjarigen](#), 2025.

¹⁴ Stephane Baele e.a., [Uncovering the Far-Right Online Ecosystem: An Analytical Framework and Research Agenda](#), 2020.

Ecosystemen zijn clusters van biotopen die ideologisch, thematisch of cultureel verwant zijn. Deze verbonden netwerken functioneren als een atmosfeer: losser georganiseerd, maar essentieel voor de verspreiding en normalisering van extremistische denkbeelden. Op dit niveau vinden we ook kruislingse platform interacties. Dit netwerk is veranderlijk en kent vage grenzen: sommige gemeenschappen bewegen zich op het snijvlak van meerdere biotopen in soms verschillende ecosystemen, bijvoorbeeld tussen alt-right en Incel-netwerken (zie H3.2). Door deze hybride structuren is het ecosysteem van online extremisme flexibel, adaptief en lastig volledig te isoleren of te ontmantelen. Bijvoorbeeld:

- De 'manosfeer' — een ecosysteem van pick-up artists, men's rights activists en anti-feministische influencers die mannelijkheid herdefiniëren in vijandige termen ten opzichte van vrouwen, feminisme en sociale gelijkheid.
- De 'incelosfeer' — een online biotoop welke onderdeel is van de manosfeer, en waarin personen zich identificeren als 'involuntary celibates' (Incels), en waarin seksuele frustratie wordt verbonden met misogynie en frustratie over maatschappelijke normen rond gender en relaties.
- 'Platform based' netwerken – zoals clusters van kanalen op Telegram waartussen veel zijdelingse uitwisseling bestaat omdat ze dezelfde ideologische basis delen, zoals het Terrorgram en Islamogram netwerk.

Het wisselend analytisch perspectief op online uitingen heeft forse invloed op wat we waarnemen en problematiseren. Kijken we naar individuen in extremistische privékanalen en groepen, dan zien we een duidelijk te onderscheiden *smalle dreiging* van online extremisme. Gemarkeerde groepen en kanalen kunnen worden geïnfilterd en gevolgd, hoewel infiltratie van afgeschermd kanalen onder sommige omstandigheden bewerkelijk kan blijken. Uitspraken op persoonlijke titel maken vervolging eenvoudiger. Analyseren we op het niveau van (sub-)biotopen, dan krijgen we een massaal en diffuus beeld van uitlatingen, gepolariseerde discussies en meme-cultuur. Hier communiceren honderdduizenden gebruikers tegelijk en op vaak grote sociale afstand; het overzicht over wie wat zegt verdwijnt. Anonimiteit speelt bovendien een belangrijke rol. Proxies, VPN's en burner email accounts maken internetgebruikers lastiger te traceren. Troll-accounts verschijnen en verdwijnen. Memes en viral filmpjes bevatten dubbelzinnige boodschappen. Op abstracter niveau ontstaat een ander type cumulatieve dreiging: de complexiteit en beweeglijkheid van het online extremistische landschap maakt dat de bredere effecten op de radicalisering van jonge generaties en de bredere maatschappelijke beeldvorming lastig te peilen zijn. Uiteindelijk moet online extremisme op verschillende niveaus worden begrepen: zonder inzicht in 'intieme' online radicalisering missen we dreigingsdetectie van de kans op terroristisch en extremistisch geweld, terwijl zonder zicht op brede biotopen de onderliggende sociale normalisering van extremistische ideeën onzichtbaar blijft.

3.2. De onderlinge verwevenheid van extremistische biotopen

In het flexibele en veranderlijke ecosysteem van online extremisme radicaliseren individuen niet zozeer in een brede ideologische bewegingen, maar vaker in meer gefocuste subculturen. Extremistische bewegingen zoals Incels, eco-fascisten of accelerationisten concentreren zich rondom een bijzondere identiteit en specifieke particuliere grieven.¹⁵ Hoewel deze biotopen over het algemeen voortkomen uit één bepaald extremistisch gedachtegoed, staan ze nauw in contact en vertonen ze overlap met andere biotopen in het online extremistische ecosysteem. Daarbij wisselen gebruikers niet alleen specifieke uitingsvormen en tactieken uit, maar bevinden ze zich ook in toenemende mate tussen de verschillende biotopen en ecosystemen.

De flexibele en open structuur van het internet draagt daarmee bij aan een toename van personen die niet radicaliseren in een eenduidig extremistisch gedachtegoed, maar in een mix van narratieven en tactieken afkomstig van diverse, soms tegenstrijdige ideologieën. Deze diffuse vorm van online extremisme beantwoordt aan enkele grondoorzaken van radicalisering die niet politiek van aard zijn, maar voortkomen uit individuele behoeften aan erkenning en een vereenvoudigd verklarend wereldbeeld (zie H3.4).¹⁶ De grieven van deze kwetsbare individuen zijn hierdoor makkelijk overdraagbaar naar een verscheidenheid aan extremistische denkbeelden die kunnen voorzien in deze behoeftes. De vaak gedeelde aanwezigheid van complotdenken en anti-establishment sentimenten bij extremistische stromingen vergemakkelijkt deze ideologische vermenging.¹⁷

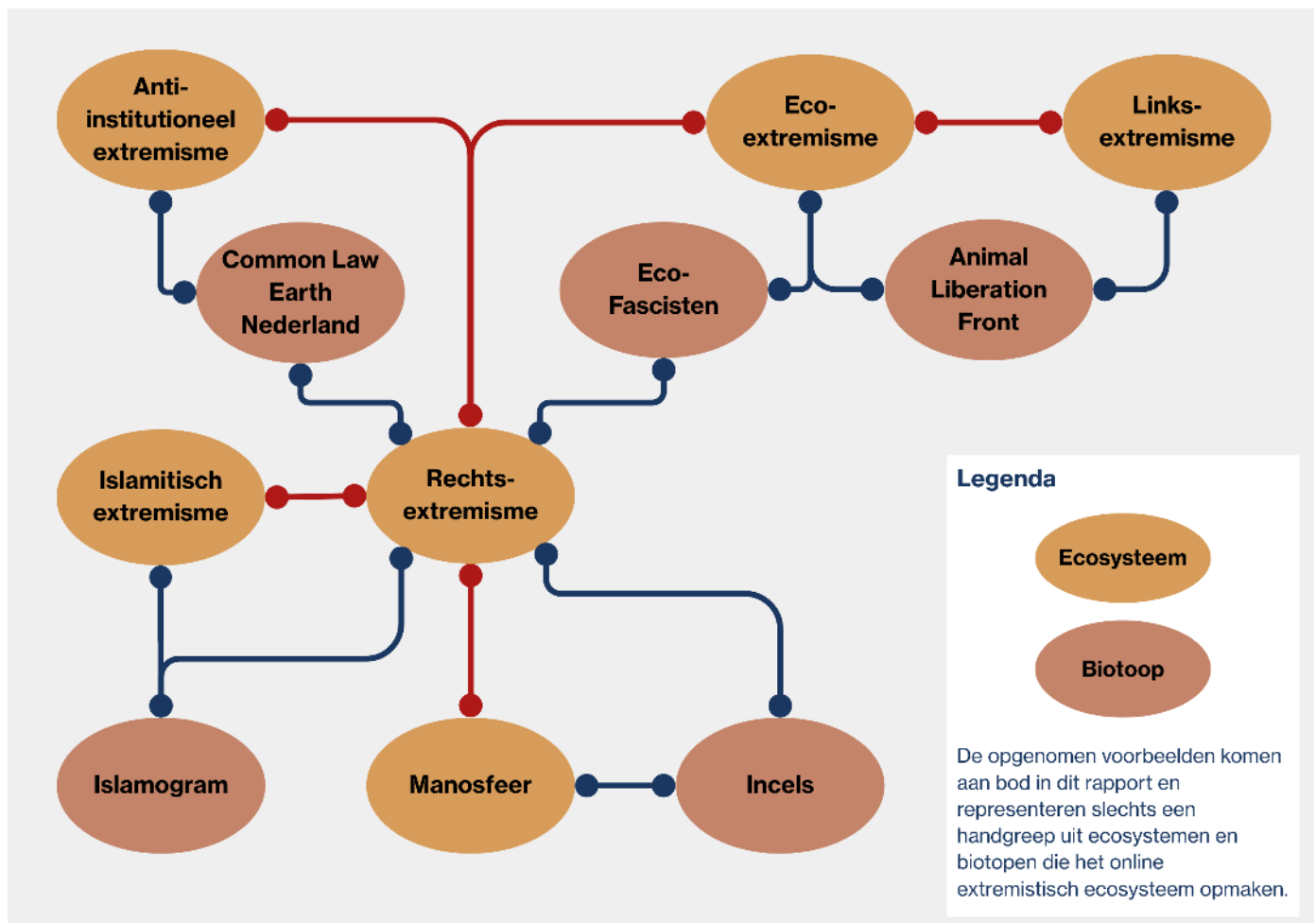
Het gevolg voor online extremisme en radicalisering is daarmee tweeledig. Ten eerste zien extremistische ecosystemen een diversiteit aan interacterende biotopen die elk hun eigen niche, identiteit en dynamiek van radicalisering kennen. Aan de andere kant bewegen sommige individuen flexibel tussen deze biotopen of creëren ze een eigen extremistisch wereldbeeld dat elementen uit verschillende subculturen combineert. Onderstaande figuur geeft een schematische impressie van de dwarsverbanden tussen online extremistische ecosystemen en het hybride karakter van extremisme online. Na de figuur volgt een nadere toelichting van enkele van deze dwarsverbanden, in het bijzonder de interactie tussen het rechts-extremistische ecosysteem en de Manosfeer, eco-fascisten en de zogenoemde TikTok-jihad.

¹⁵ Accelerationisme verwijst volgens de NCTV naar “het rechts-extremistische gedachtegoed waarbij het creëren of versnellen van chaos wordt nagestreefd, om zo een rassenoorlog en de vervanging van de democratie door een witte etnostaat te bespoedigen”. NCTV, *Definities gebruikt in het Dreigingsbeeld Terrorisme Nederland*, 2025. De term eco-fascisme wordt later in deze paragraaf toegelicht. In de definitie van de NCTV blijft onvermeld dat de term accelerationism verweven is met de neoreactionaire ‘Dark Enlightenment’-filosofie, onder andere ontwikkeld door Britse filosoof Nick Land.

¹⁶ Frank Bekkers, e.a., *Maatschappelijke Ontgoocheling van de Middenklasse*, HCSS, 2023, pp. 14-26.

¹⁷ Jamie Bartlett & Carl Miller, *The power of unreason*, DEMOS, 2010.

Figuur 3. Schematische impressie ecosysteem van online extremisme



Misogynie als verbindende factor tussen de Manosfeer en rechts-extremistische biotopen.

In de Manosfeer vermengen antifeministische en patriarchale overtuigingen zich met gewelddadig extremisme. Een overzichtsstudie identificeert deze misogynie als gedeeld kenmerk dat verschillende uitingen van rechts-extremistisch gedachtengoed verbindt met ideologieën van mannelijke suprematie zoals die te vinden zijn in de Manosfeer.¹⁸ In rechts-extremistische kringen komen misogynie en patriarchale denkbeelden voort uit een conservatief wereldbeeld waarin vrouwen ondergeschikt zijn aan de man en traditionele genderrollen de norm zijn. Mannelijke suprematie, aan de andere kant, gaat vaak gepaard met schoonheidsidealen voor mannen en vrouwen die gegrond zijn in racistische overtuigingen van witte dominantie. Misogynie en patriarchale denkbeelden functioneren zo als verbindend element dat beweging tussen de Manosfeer en rechts-extremistische milieus vergemakkelijkt.

Een recente uiting van deze dwarsverbanden is de mainstreaming van de Manosfeer door zogenaamde 'masculinity influencers' die een patriarchaal wereldbeeld verbinden met rechts-extremistische denkbeelden. Bijvoorbeeld de opkomst van sociale media influencer Andrew Tate staat symbool voor de reikwijdte en de verspreiding van mannelijke suprematie en misogynie en racistische denkbeelden onder jonge mannen en tieners. In zijn content, sinds 2022 verbannen van reguliere sociale media, benadrukt hij het idee dat mannen in de

¹⁸ Robin O'Hanlon, e.a., *Misogynistic Extremism: A Scoping Review*, *Trauma, Violence, & Abuse*, 25(2), 2023.

samenleving hun positie verkrijgen door het continue bewijzen van hun heteroseksualiteit en dominantie over vrouwen.¹⁹ De vijfvoudige moord door Elliot Rodger in 2014 wordt gezien als een van de eerste gewelddadige uitingen van de Manosfeer, specifiek de Incel-gemeenschap, en is sindsdien een inspiratiebron voor anderen gebleken.²⁰ De extremistische uitwassen van de Manosfeer – en diens interactie met recht-extremistische biotopen – vormen daarmee een toenemende geweldsdreiging tegen vrouwen.²¹

Ecofascisten: op de nexus tussen eco-extremisme en rechts-extremisme. De antikapitalistische denkbeelden van dierenrechtenbewegingen, klimaatactivisten en eco-extremisten overlappen traditioneel met sentimenten die ook te vinden zijn binnen het link-extremistische ecosysteem. Binnen deze overlap opereren groepen als het Animal Liberation Front en Earth Liberation Front, die met name buiten Nederland vernielingen en sabotage plegen aan infrastructuur en bedrijven.²² Maar ook rechts-extremisten vertonen ideologische raakvlakken met eco-extremisten en klimaatactivisten die pleiten tegen de ecologische uitwassen van de moderne tijd. In hun streven naar maatschappelijke ineenstorting, verwerpen zij industrialisatie, urbanisatie, intensieve landbouw en materialisme. Clubs als The Green Brigade doen dit naar eigen zeggen vanuit een geromantiseerd verleden waarin homogene bevolkingsgroepen in harmonie leven met de natuurlijke orde. Deze natuurlijke orde omvat niet alleen harmonie met de natuur, maar ook traditionele genderrollen en een hiërarchische ordening tussen etnische groepen die het uitsluiten en deporteren van niet-westerse bevolkingsgroepen legitimeert. Dit ecofascisme combineert ecologische narratieven met racistische en autoritaire elementen die ook te vinden zijn in ander rechts-extremistisch gedachtengoed.²³ Op Telegram richt ecofascistische content zich op een breder publiek binnen het rechts-extremisme door ecologische motieven te combineren met thema's van witte suprematie en misogynie. Daarnaast illustreren berichten die het 'linkse' Animal Liberation Front steunen hoe ecofascisten een zekere ideologische flexibiliteit vertonen die hen in staat stelt om voor hen relevante inhoud uit andere online biotopen te benutten.²⁴

Ecofascistische dreiging tegen Eurovisie Songfestival in Nederland. In juli 2025 onthulde een Luxemburgse rechtszaak dat het Eurovisie Songfestival, door Nederland georganiseerd in 2020, het beoogde doelwit was van een terroristische aanslag. Het brein hierachter was Alexander H., lid van rechts-extremistische, accelerationistische groepering The Base en het ecofascistische The Green Brigade, een afsplitsing van The Base. Deze laatste groepering combineert het streven naar een homogene witte etnostaat met milieubescherming, met als doel het behoud van de planeet voor de eigen ethnische groep. In voorbereiding op de aanslag was Alexander H. via digitale kanalen in contact met een Nederlandse minderjarige verdachte, onder andere over het infiltreren van de beveiliging van het Songfestival. Eerder werd Alexander H. in verband gebracht met brandstichting bij een Zweedse nertsenfokkerij in 2019.

¹⁹ Craig Haslop e.a., *Mainstreaming the Manosphere's Misogyny Through Affective Homosocial Currencies: Exploring How Teen Boys Navigate the Andrew Tate Effect*, *Social Media + Society*, 10(1), 2024.

²⁰ Taisto Witt, 'If I cannot have it, I will do everything I can to destroy it.' The canonization of Elliot Rodger: 'Incel' masculinities, secular sainthood, and justifications of ideological violence, *Social Identities*, 26(5), 2020.

²¹ Robin O'Hanlon, *Misogynistic Extremism: A Scoping Review*, *Trauma, Violence, & Abuse*, 25(2), 2024.

²² J.R. da Silva, *The Eco-Terrorist Wave*, *Behavioral Sciences of Terrorism and Political Aggression*, 12(3), 2019.

²³ Kristy Campion, *Defining Ecofascism: Historical Foundations and Contemporary Interpretations in the Extreme Right*, *Terrorism and Political Violence*, 35(4), 2023.

²⁴ Brian Hughes, e.a., *Ecofascism: An Examination of the Far-Right/Ecology Nexus in the Online Space*, *Terrorism and Political Violence*, 34(5), 2022.

TikTok-jihad en de online convergentie tussen jihadistische en rechts-extremistische content. Het gebruik van sociale media als platform voor propaganda en rekrutering gaat volgens gesproken experts gepaard met een verjonging van geradicaliseerde individuen in het islamitisch extremisme. Met name sinds de aanval van Hamas op Israël op 7 oktober 2023 is er een aanzienlijke toename te zien van extremistische content op onder andere TikTok.²⁵ Hier prediken zogenaamde 'TikTok imams' religieus-extremistische boodschappen, waarin zij het martelaarschap verheerlijken en kwetsbare jongeren een gevoel van identiteit en betekenis bieden.²⁶ Een deel van deze jongeren maakt hierbij gebruik van inhoud en esthetiek die normaal gesproken te vinden is in alt-right en rechts-extremistische milieus. Zogenaamde 'Islamogrammers' gebruiken rechts-extremistische symboliek en beeldtaal om zich af te zetten tegen de liberale democratie, feminisme en multiculturalisme. Daarbij combineren ze jihadistische symboliek met visuele elementen uit populaire cultuur en meme-cultuur.²⁷ Binnen afgeschermden kanalen op Telegram en Discord circuleert daarnaast Nazipropaganda en laten jonge salafisten zich positief uit over nazi-Duitsland en de Holocaust. Gen-Z salafisten hebben zo een eigen subcultuur gecreëerd waarin zij, geïnspireerd door ideologische tegenpolen, een eigen visuele taal en identiteit ontwikkelen.²⁸ De convergentie van jihadistische en rechts-extremistische inhoud en symboliek is illustratief voor het vloeibare en hybride karakter van de online extremistische cultuur.

3.3. Beperkt zicht op de omvang

Hoewel online extremisme steeds beter wordt onderzocht, blijft het zicht op de werkelijke omvang van het 'web van haat' beperkt en gefragmenteerd. Dit heeft een aantal redenen:

- *Grote verscheidenheid aan uitingsvormen.* Het alt-tech domein is een netwerk van alternatieve, gedecentraliseerde platformen ontstaan zoals Gab, Truth, Parler en Odysee waar weinig tot geen contentmoderatie plaatsvindt.²⁹ Ook X, het voormalige Twitter platform overgekocht door Elon Musk, kent geringe moderatie. Dit houdt verband met de vrije meningsuiting-doctrines die sterk hebben kunnen wortelschieten in de neoreactionaire kringen van tech-CEO's in de VS. De brede beschikbaarheid aan alternatieve platforms maakt het verhuizen eenvoudig. Alt-tech platformen maken samenwerking in het kader van opsporing bewerkelijk of onmogelijk.
- *Gecodeerde communicatie.* Binnen online biotopen circuleren ideeën niet zelden via memes (ironische en vaak dubbelzinnige beelden) en dogwhistles (signalen, gebaren of begrippen met een extremistische dubbelbetekenis) die alleen in-group worden herkend. De werkelijke hoeveelheid extremistische content blijft hierdoor snel een *dark number*. De talloze memes en video's zijn bovendien lastig juridisch te classificeren omdat de boodschap als legaal uitgelegd kan worden.
- *'Dehashing' en automatisch gegenereerde content.* Geautomatiseerde herkenning van haatcontent gebeurt voor een deel op basis van zogenaamde 'gehashte content.'

²⁵ AIVD, *Jaarverslag 2023*, 2023, pp. 12-14.

²⁶ NOS, *Man (24) uit Venray aangehouden op verdenking van terrorisme*, 2025.

²⁷ Shitposting is een specifieke vorm van online gedrag waarin 'trollen' absurde, chaotische of zinloze memes en andere berichten posten op reguliere en alternatieve sociale media (zie H4.1).

²⁸ Moustafa Ayad, *Islamogram: Salafism and Alt-Right Online Subcultures*, *Institute for Strategic Dialogue*, 2021.

²⁹ Deplatforming verwijst naar het verwijderen of beperken van gebruikers of sociale media. Vaak is dit in reactie op schendingen van communityrichtlijnen of servicevoorwaarden, bijvoorbeeld door het verspreiden van extremistische content.

Het aanleggen van hash-databases is een manier om op basis van een set unieke herkenbare eigenschappen (zeg – digitale vingerafdrukken) haatdragende of extremistische content te detecteren. Deze vorm van herkenning is niet 'fool-proof.' Zonder menselijke beoordeling ontstaan al snel blinde vlekken. Bovendien kan het proces worden gesaboteerd. Users kunnen memes licht aanpassen om de hashherkenning te omzeilen. Ook is het mogelijk om op basis van AI eindeloze variaties op een thema te maken en te verspreiden. Ook in relatie tot de Nederlandse context gelden de voornoemde bezwaren. In Nederland wordt door de NCTV en de politie bijvoorbeeld gebouwd aan een zogenaamde 'symbolenbank'. Dat is op zichzelf genomen nuttig, maar de toekomstbestendigheid van dergelijke databases vergt permanente aandacht en onderhoud.

- *Begrensde bevoegdheden.* Toezichhoudende instanties stuiten op juridische en technische barrières wanneer zij digitale netwerken, communicatiekanalen of servers willen onderzoeken. Hun bevoegdheden zijn vaak begrensd door nationale wetgeving, terwijl de infrastructuur waarop ze toezicht willen houden zich over landsgrenzen uitstrekt. Dit maakt hen afhankelijk van de bereidheid tot samenwerking van internationale platformen en hostingdiensten – een bereidheid die lang niet vanzelfsprekend is. In sommige gevallen beroepen deze partijen zich op privacywetgeving, commerciële belangen of technische onmogelijkheid, waardoor toezicht en interventie ernstig worden bemoeilijkt.
- *Afgeschermd API's.* Steeds meer grote platformen beperken de toegang tot hun Application Programming Interfaces (API's). Deze vormen de belangrijkste toegangspoort voor onderzoekers om systematisch grote hoeveelheden data te analyseren. Platformen zoals X (voorheen Twitter), Reddit, en Facebook hebben hun API-beleid voornamelijk gewijzigd vanwege commerciële heroriëntatie, druk van gebruikers over privacy, of om controle over contentanalyse in eigen huis te houden. In sommige gevallen worden API's alleen nog tegen hoge kosten of met zware restricties beschikbaar gesteld. Dit belemmert niet alleen academisch onderzoek, maar onderstreept ook de overheidsafhankelijkheid voor het vestigen van een informatiebeeld.

Kortom, het 'web van haat' is uitgebreid en in beweging, maar ons zicht erop blijft onvermijdelijk gefragmenteerd en afhankelijk van de lens waarmee we kijken. Een diepgaand begrip van online extremisme vraagt daarom om verschillende analysemethoden tegelijkertijd. Ook valt de afhankelijkheid van het toezicht op van technische detectiesystemen en (buitenlandse) internetdienstverleners.

IS-Khorasan herkent de privacybescherming van Nederland als voordeel.

De Nederlandse wetgeving is sterk verankerd in de bescherming van burgerrechten en stelt strikte eisen aan het verzamelen, opslaan en inzien van digitale communicatie en persoonsgegevens. In combinatie met een hoge mate van juridische controle op opsporingsbevoegdheden creëert dit een omgeving waarin heimelijke communicatie relatief beschermd kan plaatsvinden. Extremistische actoren beschouwen Nederland hierdoor soms als een veilige haven. Zeker als gegevens worden opgeslagen op bulletproof hostingdiensten. In een 'quickscan' in het online engelstalig propaganda-magazine 'Khorasan', gepubliceerd door IS-K (de regionale tak van de Islamitische Staat, actief in en rond Afghanistan), wordt Nederland bijvoorbeeld strategisch opgemerkt als omgeving waarin de hoogste privacy-normen gelden. Platforms en fora die gebruikmaken van Nederlandse hosting worden zo door deze jihadistische groep in 2025 gewaarmerkt als het veiligst en meest geschikt voor online communicatie.

3.4. Wat we wél kunnen zeggen over de omvang en het bereik

De schaal en zichtbaarheid van online extremistische content blijkt vaak veel groter dan algemeen wordt aangenomen. Steekproeven en moderatierapportages zijn begrensd in wat ze kunnen meten. Ook is het vrijwel onmogelijk om online interactiegegevens geografisch te isoleren waardoor het precieze Nederlandse beeld onmogelijk vast te stellen is. Onderstaande cijfers illustreren echter dat we al snel moeten denken aan grote aantallen en interacties per analysegeval.

- *Transparantierapportages van grote platforms* – geven een beeld van het aantal posts dat werd verwijderd wegens haatcontent of terrorismepropaganda. Facebook rapporteerde dat het in één kwartaal actie ondernam op bijna 15 miljoen posts met terroristische inhoud.³⁰ Als het gaat om berichten van haatzaaien werden rond de 5 à 6 miljoen items verwijderd.³¹ Twitter, vóór de rebranding tot X, meldde in 2018 schorsing van ruim 166.000 accounts wegens terrorisme-gerelateerd extremisme.³² Dergelijke aantallen verwijzen alleen nog maar wat actief wordt opgespoord.
- *Steekproef rechts-extremisme in Nieuw-Zeeland*. In een nationale case study werden ruim 600.000 extremistische berichten in een jaar verzameld van 315 (voorondersteld) binnenlandse accounts.³³ De in totaal 600.000 gedetecteerde berichten riepen 8 miljoen publieke interacties op: 5,1 miljoen likes of upvotes, 1,68 miljoen reacties en discussies, 945.000 reposts, en 1,3 miljoen videoweergaven.
- *Steekproef Australisch rechts-extremisme op Gab*. Australische onderzoekers verzamelden data van 40 accounts in Australië tussen januari en september 2020.³⁴ De groep accounts was verantwoordelijk voor 45.404 posts in een half jaar. Drie accounts waren goed voor 75% van de totale output.
- *Verspreiding terroristische content, zoals aanslagvideo's*. Het Britse Tech Against Terrorism identificeerde in zijn TCAP-rapportage (Terrorist Content Analytics Platform) tussen februari 2021 en november 2023 ca. 3.000 unieke locaties met extreemrechtse terroristische inhoud, variërend van live-aanslagvideo's tot manifesten.³⁵ Deze items werden aangetroffen op ten minste 130 verschillende platforms. Gemiddeld detecteert TCAP maandelijks ruim 100 nieuwe items.
- *Steekproef antisemitisme op Reddit en Twitter*. In de week van 18 tot 25 augustus 2021 detecteerde de Anti Defamation League circa 27.400 antisemitische tweets op Twitter, afkomstig uit een steekproef van 1% van alle Engelstalige tweets (de cijfers werden geëxtrapoleerd naar het gehele platform).³⁶ De totale potentiële zichtbaarheid werd geschat op 130 miljoen Twitter-gebruikers. Op Reddit werden in dezelfde week 1.924 tot 2.043 antisemitische comments vastgesteld, uit een totaal van circa 40 miljoen Engelstalige Reddit-reacties.
- *Indicatieve groepsomvang van extremistische of terroristische nichegroepen*. In een achtergrondartikel door Der Spiegel werd duidelijk dat ook zogenaamde nihilistisch

³⁰ Statista Research Department, Facebook terrorist content deletion per quarter 2024, 2025.

³¹ Statista Research Department, Facebook hate speech removal per quarter 2024, 2025.

³² Reuters, Twitter suspended 166,153 accounts for terrorism content in H2 2018, 2019.

³³ Milo Comerford, e.a., Understanding the New Zealand Online Extremist Ecosystem, Institute for Strategic Dialogue, 2021.

³⁴ Cécile Guerin, e.a., A Snapshot of Far-Right Activity on Gab in Australia, Institute for Strategic Dialogue, 2021.

³⁵ Tech Against Terrorism, Mapping Far-Right Terrorist Propaganda Online, 2024.

³⁶ ADL, How Platforms Rate on Hate: Measuring Antisemitism and Adequacy of Enforcement Across Reddit and Twitter, 2021.

gewelddadige extremistische groepen (NGE's – zie ook kader op pagina 28) de meest extreem gewelddadige nihilistische nichegroepen soms duizenden leden hebben. Voordat de groep 764 recentelijk opgeheven werd, had deze groep rond de 8000 leden.³⁷ Bij Nederlandse accelerationistische Telegramkanalen van bijvoorbeeld The Base spreken we doorgaans over tientallen leden. Uiteindelijk zijn er geen harde uitspraken te doen over hoe groot kanalen gemiddeld genomen zijn. Ook komen dezelfde personen soms terug in verschillende groepen waardoor het aantal unieke deelnemers in het bredere ecosysteem misschien minder groot is dan gedacht.

Specifiek voor de Nederlandse context is maar een beperkt aantal publieke bronnen voorhanden waarin prevalentie en verspreiding van extremistische content concreet worden:

- *Haat op RTL-kanalen.* Een analyse van RTL in 2024 van 210.000 Instagram-reacties op Instagram-pagina's van RTL-kanalen toonde dat 1 op de 10 reacties een haatreactie was.³⁸ De haat bleek vaker gericht tegen vrouwen of LHBTQ'ers. Uit de analyse bleek bovendien dat maar een kleine groep daders (ca. 1 procent) disproportioneel bijdroeg aan de haatcontent.
- *Fenomeenanalyse NCTV.* In Nederland publiceerde de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in mei 2024 de fenomeenanalyse 'Memes als online wapen.' Hierin wordt beschreven hoe extremistische groepen en individuen gebruikmaken van memes als laagdrempelig communicatiemiddel om hun boodschap te verspreiden. In het rapport worden echter geen indicaties gegeven over prevalentie of bereik.
- *Meldingen ATKM.* In Nederland is sinds 2023 de Autoriteit Online Terroristisch en Kinderpornografisch Materiaal (ATKM) opgericht om haatcontent te signaleren en offline te halen. Exacte cijfers voor detectie van terroristisch, extremistisch en kinderpornografisch materiaal zijn niet (publiekelijk) voorhanden. Maar er is aangekondigd dat het ATKM in 2025 rapporteert.³⁹
- *Analyse AIVD.* De brochure 'Een web van haat', door de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) waarschuwt voor de problematische effecten van extremistische online content in Nederland.⁴⁰ De analyse is gebaseerd op interne observaties en casuïstiek. Daarbij benoemt de AIVD hoe propaganda zich verspreidt. Maar het beeld is indicatief en bevat geen monitoringgegevens.

3.5. De aantrekkings- en verstrikkingskracht van online omgevingen

Digitale gemeenschappen bieden anonieme en tamelijk vrijblijvende verbindingen die aantrekkelijk zijn. Online kan men makkelijk instappen op groepen en kanalen zonder sociale hordes te nemen.⁴¹ Daarna voltrekken zich echter dikwijls processen die mensen snel dieper in het spreekwoordelijke moeras zuigen. Er zijn gevallen van aanslagplegers die in minder dan enkele maanden online geradicaliseerd bleken. We schetsen hieronder (zonder de bedoeling

³⁷ Der Spiegel, [Sadisten-Netzwerk um »White Tiger«: Wie ein FBI-Agent an der Hamburger Polizei verzweifelte](#), 2025.

³⁸ RTL, Broadcast Magazine, [Data-onderzoek RTL toont zorgwekkende cijfers online haat](#), 2024.

³⁹ De Tweede Kamer, Kamerbrief 29 754 nr. 735 aangaande Terrorismebestrijding, 2025.

⁴⁰ AIVD, [Een web van haat - De online grip van extremisme en terrorisme op minderjarigen](#), 2025.

⁴¹ ICSR, [Online Radicalisation: The Net or the Netizen?](#), 2013.

uitputtend te zijn) enkele belangwekkende factoren van aantrekking en verstrikking in de context van digitale interactie. We delen enkele indicatieve inzichten en observaties, geen empirisch geverifieerde wetenschappelijke bevindingen.

- *Laagdrempelige online participatie.* Een belangrijke aantrekkingsfactor is de laagdrempeligheid door onder meer de mogelijkheid tot (aanvankelijke of gedeeltelijke) anonimiteit. Zeker in het eerste contact spelen de lage sociale investering en de toegang een belangrijke rol om koudwatervrees voor ongemakkelijke denkbeelden of situaties weg te kunnen nemen.⁴² Anonimiteit versterkt tevens het proces van ideologische escalatie. Mølmen stelt dat anonimiteit een dynamiek creëert waarin gebruikers elkaar ideologisch overbieden wat de hermetische sfeer in de groep versterkt.⁴³
- *Beantwoording van het verlangen naar sociaal-existentiële betekenis.* De 'zoektocht naar betekenis' blijft ook online een belangrijke sociaal-existentieel motief voor de aantrekkingskracht van extremistische groepen.⁴⁴ Met name jongeren zonder uitgehard zelfbeeld kunnen worden gedreven naar zoektocht naar identiteit. Omgekeerd duwt het gebrek aan ervaren geborgenheid in de eigen psychosociale context richting online kringen.
- *De behoefte aan een vereenvoudigd verklarend wereldbeeld.* Met name bij onzekerheid, maatschappelijke, sociale frustratie en wantrouwen zoeken mensen naar houvast. Extremistische ideologieën bieden de 'ontologische veiligheid' van een overzichtelijke zwart-witwereld. De meest ongeloofwaardige complottheorieën hoeven niet eens te overtuigen om aantrekkelijk te zijn. Ze suggereren het gevoel van ingewijd-zijn, spelen in op gevoelens van geborgenheid en markeren een helder vijandbeeld. Simplificatie wordt door extremisten ook expliciet als tactiek voorgeschreven. Ze zijn psychologisch belonend⁴⁵ en markeren de in-group.⁴⁶
- *Vatbaarheid door psychische persoonskenmerken.* Regelmatiger wijzen onderzoekers op de opvallende rol van mentale kwetsbaarheden en stoornissen onder daders. Onderzoek van Corner e.a. wijst op de 'comorbiditeit' tussen gewelddadige radicalisering en stoornissen zoals depressie, autisme of PTSS.⁴⁷ Geradicaliseerde eenlingen blijken oververtegenwoordigd in dit profiel: De online ruimte lijkt te fungeren als een onwenselijke katalysator voor de verdieping van mentale problemen. Bijvoorbeeld door het constant voeden met complotgedachten, of gruwelijke content. Latente gevoelens raken uitvergroot in kanalen waarin geen tegengeluid te horen is maar juist aanmoediging bestaat voor het wegnemen van interne remming. Extremistische groepen spelen daar soms in hun tactieken bewust op in, zoals in de hieronder besproken 'COM-groepen'.
- *Getrapt binnenhengelen.* De inlijvende kracht van online ecosystemen heeft soms ook te maken met de getrapte blootstelling aan steeds extremere content. Extremistische boodschappen kunnen op mainstream platforms worden verpakt in aaibare beeldtaal die makkelijker te verteren maar ook een aanknopingspunt biedt om mensen te benaderen en dieper in de biotoop te trekken. Zeker bij meme-propaganda helpt de aantrekkelijk lichtzinnige presentatie om een eerste interesse op te wekken, iemand vervolgens uit te

⁴² RAND, Ines von Behr et al., *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, 2013.

⁴³ Global Network on Extremism and Technology (GNET), Guri Mølmen & Jacob Ravndal, *Mechanisms of online radicalisation: how the internet affects the radicalisation of extreme-right lone actor terrorists*, 2021.

⁴⁴ Arie Kruglanski e.a., *The Psychology of Radicalization and Deradicalization*, 2014.

⁴⁵ Berger, J. M., *Extremism*, 2018.

⁴⁶ Sunstein, C. R., & Vermeule, A. (2009). *Conspiracy Theories: Causes and Cures*. *Journal of Political Philosophy*, 17(2), 202–227.

⁴⁷ Corner, E. e.a., *Mental health disorders and the terrorist: A research note probing selection effects and disorder prevalence*, 2016.

nodigen voor radicalere Telegramkanalen en pas dan gradueel bloot te stellen aan steeds extremere ideeën.⁴⁸

Blootstelling aan IS-propaganda verloopt op een getrapte manier. In eerste instantie worden gebruikers geconfronteerd met relatief onschuldige of zelfs sympathiek ogende content op platforms als TikTok, waar influencers zich richten op politiek geladen thema's zoals islamofobie, Palestina of antikolonialisme. Deze shortform video's sluiten goed aan bij bestaande sentimenten en blijven binnen de grenzen van het toelaatbare, maar fungeren ook als toegangspoort. Gebruikers die deze content liken of delen kunnen vervolgens worden uitgenodigd voor besloten kanalen op Telegram, waar de toon explicieter jihadistisch wordt en de ideologische lading zwaarder. Een volgende stap in deze radicaliseringsketen is dat individuen zelf gaan bijdragen aan de distributie-infrastructuur van IS-propaganda, bijvoorbeeld door het hosten van digitale magazines zoals *Khorasan* via decentrale online repositories. Door het verspreiden van dit materiaal over talloze digitale nodes wordt de continuïteit van het propagandanetwerk verzekerd. Deze laag voor laag opgebouwde architectuur maakt de beweging veerkrachtig en moeilijk uit te roeien.

Als iemand eenmaal is toegetreden tot meer extremistische omgevingen is de kans groot om daar verder in gezogen te worden. Online kanalen hebben hun eigen verstrikkende sociale dynamiek waarbij niet zelden gebruik wordt gemaakt van doelgerichte tactieken van exploitatie en intimidatie.

- *De hang naar sociaal krediet.* Eenmaal opgenomen in de groepscontext, proberen individuen hun rol van betekenis te bestendigen. Sociaal krediet wordt verworven door actief te delen, content te genereren, anderen te *groomen* of door hand- en spandiensten te verrichten of geweld te plegen in de offline wereld. Bijvoorbeeld, in IS-gemeenschappen worden deelnemers beloond met symbolische statuskenmerken zoals het label van 'kenner'.⁴⁹ Zo ontstaat het vooruitzicht van erkenning. Door proof of loyalty kan iemand versneld opklimmen. Maar deze dynamiek werkt ook competitief en 'verslavend'. Leden willen elkaar overbieden en relevant blijven en zuigen zich hierdoor verder vast in een steeds radicalere sociale dynamiek en bewijsdrang.
- *Love bombing, groomingtactieken en chantage.* In sommige groepen worden ook regelrechte manipulatietechnieken ingezet om personen te binden of af te persen. *Love bombing*, het overdreven overladen van een nieuwkomer met aandacht en waardering, creëert een vals gevoel van geborgenheid dat initieel aanzet tot het delen van kwetsbare openbaringen. Daarop wordt doorgepakt met groomingtactieken met het doel iemands grenzen te verschuiven door chantage met iemands gedeelde naaktbeelden of ontboezemingen. Twijfelende leden worden zo onder druk gezet om te blijven, of zich te bewijzen door extreme daden of het leveren van (steeds heftiger) seksueel materiaal. Deze combinatie van verleiding, conditionering en dwang vormt een dwingende sociale dynamiek die elke autonomie afbreekt en mensen vastzet in een hermetisch gesloten systeem.
- *Algoritmische radicalisering.* Veronderstelde filterbubbels of echokamers helpen vermoedelijk om te worden meegezogen in extremistische denkwerelden. Ook worden ze in verband gebracht met processen van self-radicalisation in het geval van extremistische

⁴⁸ Anti-Defamation League. 2020. *The Alt Right Playbook: Understanding Far-Right Tactics in Online Spaces*. New York: ADL.

⁴⁹ Tamara Kharroub, *Understanding Violent Extremism: The Social Psychology of Identity and Group Dynamics*, 2015.

eenlingen.⁵⁰ Er wordt uitgebreid gespeculeerd over hoe zwaar hun rol in de praktijk is.⁵¹ Kritische studies wijzen erop dat gebruikers toch in grote mate hun eigen mediakeuzes blijven maken.⁵² Ander onderzoek onderstreept dat algoritmen met name de radicale smaken versterken die er al zijn.⁵³ Algoritmen dragen bij aan een consistente influx van vers materiaal waardoor telkens aanleiding is om verder weg te zinken in haat.⁵⁴

Suicide watching in 764. De zelfverbranding van Samuel Hervey in november 2021 vormde een bizar en schrijnend voorbeeld van hoe een perverse, op proof of loyalty gebaseerde groepsdynamiek ontstaat in zogenaamde 'nihilistisch gewelddadig extremistische groeperingen (zie hieronder voor de beschrijving van de bespreking van deze groepen, ook wel COM-groepen genoemd). Hervey, een 25-jarige man uit Minnesota, bevond zich in ernstige psychische nood en besloot zichzelf na aanmoediging van een deel van de 764 community live op een door hem aangemaakt chatroom in brand te steken tijdens zijn backpackreis. In de besloten chatroom keek een internationale groep toe. De leden lachten daarbij en moedigden hem aan terwijl hij in brand opging. Eén deelnemer was een 15-jarig meisje dat hem via berichten had bevestigd in zijn plannen om zelfmoord te plegen. Ze bevond zich daarbij naar eigen zeggen in de illusie dat dit haar 'grote doorbraak' zou worden binnen deze extremistische groep. (Bron: Der Spiegel, Sadisten-Netzwerk um White Tiger: Wie ein FBI-Agent an der Hamburger Polizei verzweifelte, 2025).

⁵⁰ Mølmen, G. N., & Ravndal, J. A. (2021). Mechanisms of online radicalisation: how the internet affects the radicalisation of extreme-right lone actor terrorists. *Behavioral Sciences of Terrorism and Political Aggression*, 15(4), 463–487.

⁵¹ Zuiderveen-Borgesius, Frederik J., e.a. "Should we worry about filter bubbles?". Internet Policy Review 5 (1); Whittaker, Joe. 2022. "Recommendation Systems and Extremism: What Do We Know?" Global Network on Extremism and Technology (GNET).

⁵² Commissariaat voor de Media, Geen indicatie voor bestaan van filterbubbels in Nederland, 2019; Hosseinmardi, H., Ghasemian, A., Clauset, A., Mobius, M., Rothschild, D. M., & Watts, D. J. (2021). Examining the consumption of radical content on YouTube. *Proceedings of the National Academy of Sciences*, 118(32).

⁵³ Chen, A. Y., Nyhan, B., Reifler, J., Robertson, R. E., & Wilson, C. (2021, februari). Exposure to Alternative & Extremist Content on YouTube. Anti-Defamation League, Center for Technology and Society.

⁵⁴ Brown, Ryan Andrew, Todd C. Helmus, Rajeev Ramchand, Alina I. Palamaru, Sarah Weiland, Ashley L. Rhoades, en Liisa Hiatt. Violent Extremism in America: Interviews with Former Extremists and Their Families on Radicalization and Deradicalization. Santa Monica, CA: RAND Corporation, 2021.

4. Trends en online extremistische ecosystemen

Online extremisme behelst niet enkele de communicatie en organisatie van extremisten via digitale middelen. Het is een eigenstandig fenomeen dat unieke vormen van radicalisering, strategieën en dynamieken met zich meebrengt. Zo staan internethumor en het gebruik van memes centraal in het discours van online extremistische ecosystemen, waarin traditionele ideologieën samenvloeien tot hybride overtuigingen en radicalisering soms de vorm aanneemt van een game, met digitale puntentellingen en prestatiebadges. In bepaalde online subculturen is geweld geen middel, maar een doel op zich. Deze nihilistische geweldsverheerlijking gebruiken extremisten om online individuen te rekruteren voor hun doeleinden. Ook manifesten en digitaal martelaarschap vormen een bron van rekrutering en inspiratie voor radicaliserende personen. Dit alles gebeurt zelden onder de leiding van een centrale bevelstructuur; online extremisme kenmerkt zich door losjes gebaseerde netwerken van symbolen, inside jokes en gedeelde frustraties. Het ecosysteem van online extremisme is daarmee een krachtig, quasi-zelforganiserend geheel dat zich ultrasnel en tegelijk moeilijk beheersbaar kan mobiliseren in de offline wereld. Dit hoofdstuk gaat dieper in op deze trends en kenmerken die karakteristiek zijn voor online extremisme.

4.1. Meme-propaganda

Memes als dominante beeldtaal in de online extremistische cultuur. Memes zijn anoniem gecreëerde (bewegende) internetbeelden die op humoristische – soms meer cynische wijze commentaar geven op leven en actualiteit. Daarmee zijn memes dé symbolen geworden van internetcultuur.⁵⁵ Extremisten vermengen deze referenties met eigen symboliek en iconografie waardoor extremistische memes moeilijk te herkennen zijn. Onder een laag van sarcasme en internethumor schuilen gecodeerde en verborgen extremistische boodschappen.⁵⁶ Memes vervullen daarmee ook een functie in de identiteits- en groepsvorming van extremisten; het gebruik ervan is onderdeel van de online identiteit en versterkt deze.⁵⁷ Memes worden in groepen ook wel gedeeld met het doel om de gevoelstemperatuur te meten: Wat kan wel en wat niet? Tot slot bemoeilijkt het fluide karakter van memes moderatie en opsporing doordat het lastig is om op het eerste gezicht met zekerheid vast te stellen dat aangetroffen content extremistische inhoud bevat. Het anonieme karakter van het internet vergroot deze opsporingsproblematiek, doordat oorspronkelijke makers en verspreiders van haatdragende of opruiende content moeilijk te achterhalen zijn.

⁵⁵ Asaf Nissenbaum & Limmor Shifman, *Internet memes as contested cultural capital: The case of 4chan's /b/ board*, *New Media & Society*, 19(4), 2017, pp. 484-485.

⁵⁶ Ursul Kristin Schmid, e.a., *Memes, humor, and the far right's strategic mainstreaming*, *Communication & Society*, 28(4), 2024, pp. 539-540.

⁵⁷ Julia R. DeCook, *Memes and symbolic violence: #proudboys and the use of memes for propaganda and the construction of collective identity*, *Learning, Media and Technology*, 43(4), 2018, pp. 486-489.

‘The Honkler’: onschuldige cartoon blijkt nazi-icoon. Een bekend voorbeeld uit rechts-extremistische meme-cultuur is de ‘Honkler’: een kwaadaardige clown-versie van Pepe the Frog met een regenboogprui. Waar Pepe ooit begon als onschuldige stripcartoon uit de online serie *Boy’s Club*, werd het ook een symbool voor rechts-extremistische stromingen en alt-right. De Honkler is een specifieke versie van Pepe waarin de kikker met regenboogprui symbool staat voor de ridiculisering van de woke wereld, die wordt voorgesteld als een idiote ‘clown world’. Deze meme wordt binnen extremistische subculturen gebruikt om de woke generatie te bespotten en in extreme zin geweld ertegen te rechtvaardigen. Het ‘honk-honk’ van de toeter van Pepe the Clown wordt ook wel gebruikt als dog whistle voor ‘Heil Hitler’. Overigens beperkt het clownmotief zich niet tot de online wereld. Bij verschillende betogingen tegen abortus verschenen bijvoorbeeld ook leden van de Proud Boys in clownskostuum, refererend aan deze meme.

Memes en rekrutering. Waar memes een voorname rol spelen in onderlinge communicatie en identiteitsvorming tussen extremisten, zijn zij ook onderdeel van een gerichte online strategie om veelal kwetsbare jongeren te rekruteren in extremistisch gedachtengoed.⁵⁸ Extremisten gebruiken het ambigue karakter van memes om virale verspreiding van hun ideeën mogelijk te maken en zo een breed publiek te bereiken. Content wordt bijvoorbeeld quasi-onschuldig gedeeld “voor de lulz – for the laughs” – waar in feite haatdragende boodschappen worden gecommuniceerd, of de geesten warm worden gemaakt voor steeds extremere denkbeelden. Deze tactieken dragen bij aan graduele normalisering.⁵⁹ Memes gaan dienen als ‘gateway content’ voor meer radicalere kanalen.

Virale verspreiding. Een succesvolle meme is niet statisch, maar behoudt relevantie door continu te kunnen evolueren afhankelijk van de sociale context en actualiteit. Deze flexibiliteit draagt tevens bij aan de transnationale verspreiding van extremistische memes, door de nadruk op beeldtaal en het gemak waarin zij aangepast kunnen worden aan een specifieke nationale context.⁶⁰ Extremisten gebruiken daarnaast nieuwe technologieën, zoals AI-gegenereerde content, om memes met extremistische content op grotere schaal te produceren en verspreiden.⁶¹ De virale verspreiding en constante evolutie van memes maakt het nog moeilijker deze te modereren, en maakt hen des te aantrekkelijker als propagandamiddel voor de verspreiding van extremistisch gedachtengoed.

Instrumenten van provocatie en disruptie. Shortform content kan ook worden gebruikt om tegenstanders te provoceren. De term ragebait zegt in feite al wat het doet: het posten van provocerende, vervreemdende content dient ertoe om woede uit te lokken en discussies te verstoren. Ook ‘shitposting’, het dumpen van onzinnige boodschappen, heeft soms tot doel om een betekenisvol digitaal debat te torpederen.⁶² Het posten van onzinnigheden kan

⁵⁸ WODC, *Radicale reclame: hoe werven extremistische groeperingen nieuwe leden?*, 2024. Lisa Bogerts & Maik Fielitz, *The Visual Culture of Far-Right Terrorism, Global Network on Extremism & Technology*, 2020.

⁵⁹ Tina Askanius, *On Frogs, Monkeys, and Execution Memes: Exploring the Huma-Hate Nexus at the Intersection of Neo-Nazi and Alt-Right Movements in Sweden*, *Television & New Media*, 22(2), 2021, pp. 160-161; Ursul Kristin Schmid, e.a., *Memes, humor, and the far right’s strategic mainstreaming*, *Communication & Society*, 28(4), 2024.

⁶⁰ Jordan McSwiney, e.a., *Sharing the Hate? Memes and transnationality in the far right’s digital visual culture*, *Communication & Society*, 24(16), 2021.

⁶¹ Achi ishra & Vignesh Karumbaya, *A Deadly Trifecta: Disinformation Networks, AI Memetic Warfare, and Deepfakes*, *Global network on Extremism & Terrorism*, 2024.

⁶² Benjamin Aspray, *On Trolling as Comedic Method*, *Journal of Cinema and Media Studies*, 58(3), 2019.

bovendien een manier zijn om de aandacht af te leiden of om op te vallen binnen de sociale dynamiek van de *in-group*.⁶³

Rol van memes in de mainstream politiek. Memes blijven niet beperkt tot extremistische subculturen maar worden ook een mainstream politiek signaal. Donald Trump en Thierry Baudet gebruikten Pepe the frog om zich te identificeren met de alt-right achterban. Memes kunnen impliciete verwijzingen dragen naar omvolkingstheorieën, clown world of white genocide.⁶⁴ Op grotere schaal wordt de mobiliserende werking van memes ook herkend als een belangrijk instrument van ideologische oorlogsvoering. Andrew Anglin, oprichter van de neonazistische blog The Daily Stormer, zei over de verkiezing van Trump: “Without the memes it wouldn't have happened.”⁶⁵ Er zijn ook voorbeelden dat Amerikaanse groepen bewuste memecampagnes opzetten online om Europese verkiezingen te beïnvloeden.

Omvolkingscontent. Afgelopen jaren gebruikten verschillende rechtse politici de term omvolking in relatie tot immigratiedruk op Nederland. Hoewel steeds vaker te horen in het reguliere politieke debat, vindt de term zijn oorsprong in internationale rechts-extremistische complottheorieën die speculeren over een doelgericht geheim (vaak door Joden aangejaagd) beleid om de witte bevolking in Westerse naties te vervangen door niet-Westerse groepen. Op vrijwel alle platformen is bijzonder veel van dit soort content in omloop. Soms wordt daarbij ingespeeld op angstbeelden van een door migratie of woke-beleid ingestorte samenleving. Soms zet men juist in op de extreme verheerlijking van (uit de context getrokken) symboliek van Westerse hegemonie zoals de VOC-tijd, het Romeinse rijk of de kruistochten.

4.2. Ideologische hybridisatie

Aan de ene kant zijn online duidelijke ecosystemen en biotopen te onderscheiden. Denk aan de incel-cultuur of niche Reddit-groepen rondom eco-fascisme. Deze omgevingen zijn relatief coherent, hebben eigen jargon en gedeelde vijandbeelden, en kunnen daardoor analytisch goed worden gemarkeerd. Aan de andere kant is juist de vloeibaarheid en hybriditeit een centraal kenmerk van veel hedendaagse extremistische subculturen. In veel gevallen mengen ideeën uit uiteenlopende richtingen zich tot ‘syncretische ideologieën’: bijvoorbeeld een combinatie van etnonationalisme met technologische dystopie, misogynie en samenzweringdenken.⁶⁶ De ideologische positionering wordt nog extra ambigu wanneer memes gelijktijdig naar meerdere, soms zelfs innerlijk tegenstrijdige ideologische kaders verwijzen.

‘Saladebar extremisme.’ In tegenstelling tot de vorige golven van terrorisme, waarbij bewegingen vaak een coherente ideologie volgden (zoals anarchisme, antikolonialisme, marxisme

⁶³ Sarah E. Daly & Annie Laurie Nichols, ‘Incels are shit-post kings’: incels’ perceptions of online forum content, *Journal of Crime and Justice*, 47(1), 2024.

⁶⁴ Jullietta Stoencheva & Biljana Mileva Boshkoska, *Extremist narratives in the digital mainstream*, *MediaKultur*, 77, 2024.

⁶⁵ Peter Allen Clark, *The alt-right’s worldwide weaponization of memes*, 2017.

⁶⁶ Etnonationalisme refereert aan een ideologische stroming die andere volken en culturen enkel repsecteert zolang ze in hun eigen territorium blijven. Etnonationalisten definiëren de natie op basis van etnische afstamming, gedeelde cultuur en gemeenschappelijke afkomst. In zijn meest extreme vormen kan etnonationalisme etnische zuivering legitimeren, bijvoorbeeld doormiddel van deportaties en verdrijving, om de etnische homogeniteit in de natiestaat te waarborgen.

of religieus fundamentalisme), kenmerkt de huidige tijd zich door een eclectische en gefragmenteerde vorm van extremisme.⁶⁷ Deze nieuwe dynamiek is zichtbaar in zowel jihadistisch terrorisme als extreemrechts geweld, waar individuen en groepen ideologieën, complottheorieën en religieuze of politieke overtuigingen naar eigen inzicht vermengen.⁶⁸ Zo kan iemand een radicale islamistische visie combineren met online samenzweringstheorieën over een 'deep state', of kan een extreemrechtse terrorist elementen van christelijk fundamentalisme, ecologisme en anti-globalisme in zijn wereldbeeld verwerken. De online wereld speelt hierin een cruciale rol, omdat het een ongefilterde stroom aan ideologische fragmenten biedt die individuen zonder vaste structuur kunnen combineren tot een eigen radicale overtuiging.

Trend in Nederland? Ook in Nederland zien we een voorzichtige trend van groeiende ideologische verwarring waarbij daders niet altijd passen binnen bestaande hokjes. Dit sluit aan bij het fenomeen van knip-en-plak-extremisme, waarin individuen fragmenten uit verschillende ideologieën halen en samenvoegen tot een eigen, vaak incoherent wereldbeeld. Bijvoorbeeld bij Fouad L., een 32-jarige student geneeskunde die zijn buurvrouw en moeder neerstak en een docent aan het Erasmus MC een docent doodschoot, speelde een mengeling anti-zwart racisme en incel-ideologie, persoonlijke grieven en stoornissen.⁶⁹

Muslimwaffen en ecofascisten – zijn voorbeelden van hybride extremistische entiteiten. Muslimwaffen ontstond op 'Terrorgram' als verwijzing naar de synthese tussen jihadistische strijd en neonazistische doelen. Er bestaan immers raakvlakken op het punt van antisemitisme en het belang om chaos in het liberale Westen te versnellen. En zo zijn er meer hybridisaties. Zoals 'eco-fascisten' die maatschappelijke ontwrichting zien als route naar een witte etnostaat in harmonie met de natuur. Zij identificeren zich bijvoorbeeld online met de Yggdrasil-rune, de Noorse levensboom die dan zowel verwijst naar ecologische mystiek als naar het herstel van de 'boreale wereld.'

4.3. Gamificatie van extremisme: 'fun' als vehikel voor geweldsideologie

Memecultuur, ironische esthetiek en spelelementen maken extremistische content aantrekkelijker en moeilijker te herkennen. Het delen van extremistische memes, scores voor *kills* in manifesten van aanslagplegers en het gebruik van gamificatie in gewelddadige online competities draagt bij aan normvervaging en geweldsverheerlijking.

Gewelddadig extremisme als spel. Binnen online extremistische netwerken is steeds vaker een versmelting te zien van spelprincipes met extremistisch gedachtengoed. Deze gamificatie integreert spelelementen zoals scores, beloningen en doelen in extremistische communicatie en propaganda, waardoor geweld wordt gepresenteerd als iets spannends of speels.⁷⁰ Gewelddaden krijgen daardoor een game-achtige glans die de morele afschuw

⁶⁷ Gartenstein-Ross, D., e.a., *Composite Violent Extremism: Conceptualizing Attackers Who Increasingly Challenge Traditional Categories of Terrorism*, *Studies in Conflict & Terrorism*, 2023.

⁶⁸ Abdul Basit, *Conspiracy Theories and Violent Extremism*, *Counter Terrorist Trends and Analyses*, 13(3), 2021.

⁶⁹ Or Goldenberg, *Het giftige web genereert een giftige zelf*, *De Groene Amsterdammer*, 2023.

⁷⁰ Olivier Cauberghs, *Hate the player, not the game: Exploring extremist and terrorist use of games, gaming platforms and gamification strategies for propaganda purposes*, *Radices*, 4(1), 2025.

weet te omzeilen en daarmee het gebruik van geweld door het individu mogelijk maakt. Een typerend voorbeeld is het gebruik van kill scores of puntentellingen in manifesten van terroristen, zoals bij de aanslag van Brenton Tarrant in Christchurch Nieuw-Zeeland.⁷¹ Geweld wordt zo geframed als onderdeel van een competitie waarin het loont om zo veel mogelijk schade toe te brengen aan vermeende vijanden. In online gemeenschappen ontstaan vervolgens topscores, uitdagingen en roem voor wie zich 'onderscheidt' in de strijd. Deze speelse benadering van geweldsdaden vervaagt morele grenzen, doordat extremistisch gedachtengoed wordt verpakt in een format dat lijkt op populaire online culturen. Gamificatie is dan ook onderdeel van een bewuste strategie van extremisten om een breed, jong publiek in aanraking te laten komen met hun gedachtengoed en rijp te maken voor het plegen van extremistisch geweld.⁷²

Gamificatie van het radicaliseringsproces. Niet alleen geweld, maar ook het deelnemen aan meme-creatie of het verspreiden van haatcontent is steeds vaker onderdeel van een spel dat wordt beloond met status. Door het volbrengen van dergelijke quests of doelstellingen ontvangen individuen punten, stijgen ze op ranglijsten, of ontvangen ze een custom label of nickname. Deze gamificatie geeft bij radicaliserende individuen een gevoel van tevredenheid, bevredigt psychologische behoeftes en houdt hen zo betrokken bij het radicaliseringsproces.⁷³ Een voorbeeld van extremistische bewegingen die gebruik willen maken van deze dynamiek is de – nog niet gepubliceerde – app Patriot Peer van de rechts-extremistische Identitaire Beweging die onder aanvoering staat van onder meer Martin Sellner. In deze app zouden gebruikers punten ontvangen voor het netwerken met andere gebruikers, het bezoeken van bepaalde locaties en deelname aan protesten.⁷⁴ Op deze manier vergroot gamificatie niet alleen de toegankelijkheid van geweld, maar verlaagt het ook de drempel tot radicalisering in een extremistische beweging en gedachtengoed.

Live gamificatie: Brenton Tarrant als *first-person shooter*. Christchurch-schutter Brenton Tarrant was een van de eerste rechts-extremisten die zijn aanslag – waarbij 51 mensen op het leven kwamen – live uitzond op sociale media. Met een GoPro-camera slaagde hij erin 17 minuten lang zijn geweldsdaad te streamen op Facebook Live. Voor online kijkers kreeg de aanslag zo het karakter van een *Let's Play*, een video format waarin gamers hun spelervaringen laten zien. Door de positie van de camera ontstond een parallel met *first-person shooters* zoals Call of Duty, waarin spelers door de ogen van hun avatar richten en schieten. Tarrants begeleidend commentaar en achtergrondmuziek maakte de parallel tussen online livestreams van games compleet. Het gevolg van deze live gamificatie is tweeledig. Ten eerste lijkt Tarrant zijn eigen morele drempel te hebben willen verlagen. Aan de andere kant behielden kijkers door de parallel met populaire gamecultuur een grotere afstand tot het reële menselijk leed. Zij spraken na de aanslag over welke topscore Tarrant gehaald zou hebben en vergelijken sindsdien prestaties van nieuwe aanslagplegers met de Christchurch schutter op online ranglijsten (Lakhani & Wiedlitzka, 2023).

⁷¹ Adam Lankford, *The Gamification of Mass Violence: Social Factors, Video Game Influence, and Attack Presentation in the Christchurch Mass Shooting and Its Copycats*, *Studies in Conflict & Terrorism*, 2024.

⁷² Linda Schlegel, *Working Paper: The Role of Gamification in Radicalization Processes*, *modus | zad*, 2021.

⁷³ Linda Schlegel, *Jumanji Extremism? How games and gamification could facilitate radicalization processes*, *Journal for Deradicalization*, 23, 2020.

⁷⁴ Linda Schlegel, *Working Paper: The Role of Gamification in Radicalization Processes*, *modus | zad*, 2021, p. 5.

4.4. Nihilistische en misantropische geweldsverheerlijking

Desensitisering door gewelddadige en gore content. Binnen sommige online extremistische gemeenschappen vloeien beelden van geweld, seksueel misbruik en mishandeling rijkelijk. Dit is op zich geen onbekend fenomeen: internetvoyeurisme ten aanzien van gruwelijke ongelukken of executies — zogenaamde *gore content* — bestaat al ongeveer zo lang als de virtuele wereld zelf. Toch zien we dat men binnen extremistische kanalen een belangrijke stap verder gaat dan voyeurisme. Men participeert aan geweldsverheerlijking bij wijze van uitdaging om zelf geweld te plegen. En/of het kan zo zijn dat geweldsverheerlijking een strategisch doel dient in het licht van een dystopisch vergezicht. Vroege desensitisering van betrokkenen biedt een strategisch voordeel dat ook wordt herkend en benut in manifesten en strategische documenten. Of dit soort strategieën wordt letterlijk besproken in kanalen. Het maken en delen van gewelddadige content is een beproefde morele afbraaktactiek om vervolgens loyaliteit te winnen.⁷⁵

Extreem geweld als accelerationistische strategie. Extreem geweld wordt binnen bepaalde online subculturen gezien als een bewuste accelerationistische strategie. In de verschillende edities van *The Hater's Handbook*, verspreid door de rechts-extremistische Maniac Murder Cult (MKY), wordt geweld bijvoorbeeld stelselmatig verheerlijkt als katalysator voor chaos en maatschappelijke implosie. De onderliggende gedachte is dat door het plegen van choquerende, willekeurige aanslagen of moordpartijen het vertrouwen in instituties wordt ondermijnd, etnische spanningen worden aangewakkerd en repressieve overheidsreacties worden uitgelokt. Dit versnellen ('accelereren') van maatschappelijke afbraak wordt gepresenteerd als voorwaarde voor de geboorte van een nieuwe orde, waarin bestaande liberale democratische structuren en morele grenzen zijn weggevaagd. Geweld en desensitisering hebben een revolutionaire functie.

Geweld omwille van geweld. Het delen en plegen van geweld is in sommige extremistische kringen juist niet duidelijk ideologisch gemotiveerd. Er is in sommige omgevingen sprake van een zorgwekkende verheerlijking van geweld waarbij het enkel draait om een nihilistisch genoegen in sadisme of het verkrijgen van de volledige macht over een ander persoon.⁷⁶ Nihilistische subculturen lijken extra vaak kwetsbare jongeren aan te trekken die kampen met sociale grieven en mentale problematiek. De nihilistische groepsdynamiek die ontstaat leidt ertoe dat leden worden uitgedaagd of gechanteerd om terroristische daden te verrichten, zelfmoord te plegen of andere aan te moedigen tot seksuele handelingen. Maatschappelijke ontwrichting is hier noch het hoofddoel, noch de kern van de ideologie.⁷⁷ Waar kwetsbare jongeren en kinderen zich in deze subculturen ophouden ontstaan er risico's van seksuele en sadistische predatie. Zo werden eerder sleutelfiguren geïdentificeerd die wat ouder zijn en leden proberen af te persen of tot seksuele handelingen te dwingen voor eigen vermaak. Het strategische karakter wordt ondersteund door het circuleren van tactische handleidingen voor sextortion.

⁷⁵ Barbara Krahé, e.a., Desensitising to Media Violence: Links With Habitual Media Violence Exposure, Aggressive Cognitions, and Aggressive Behavior, *Journal of Personality and Social Psychology*, 100(4), 2011; James Hardy & Christopher Stewart, Gore and violent extremism: How extremist groups exploit 'gore' sites to view and share terrorist material, *Institute for Strategic Dialogue*, 2023.

⁷⁶ Daniel Siegel, Generation Doomer: How Nihilism on Social Media is Creating a New Generation of Extremists, *Global Network on Extremism & Technology*, 2022.

⁷⁷ Simon Purdue, Ideological Nihilism and Aesthetic Violence: Mass Shooters and Online Antisocial Subcultures, *Global Network on Extremism & Technology*, 2022.

Nihilistisch gewelddadig extremisme (NGE) of COM. Recent nemen de zorgen toe over de verspreiding van zogenaamde nihilistisch gewelddadige extremistische groepen (NGE), binnen de eigen subcultuur ook wel 'COM' genoemd. Honderden Discordgroepen en Telegramkanalen onder obscure namen als No Lives Matter (NLM) of 764 verheerlijken geweld als een doel op zich. Daarnaast zijn er een paar kanalen waar COM-leden naar toe stromen en uitwisseling plaatsvindt tussen groepen, zoals (-bij het moment van schrijven-) Leak Society. Weliswaar zijn er telkens kleine verschillen in hoe en waarom geweld wordt verheerlijkt of aangemoedigd. Sommige kanalen lijken bijvoorbeeld wat sterker de nadruk te leggen op het delen van filmpjes van moord en mishandeling van dieren of willekeurige menselijke slachtoffers. Andere lijken wat sterker in het teken te staan van seksuele afpersing. Er zijn verschillende zaken bekend van leden die in deze groepen zijn gegroomd tot het produceren van (steeds extremere) seksuele content, of aangemoedigd tot zelfverminking of zelfs het plegen van zelfmoord. Hoewel dit soort sadistische geweldsgroepen gebruik kan maken van rechts-extremistische, nazistische of satanistische motieven en symboliek is hun destructieve karakter niet duidelijk ideologisch gefundeerd. Ook zijn het geen cultgroepen of sektes zoals soms wordt beweerd. Er is noch een centrale leider die vereerd wordt, noch is er sprake van een consistente aanbidding van het occulte (hoewel sommige leden wel aangetrokken worden door satanistisch-nazistische groepen zoals de Order of the Nine Angles (O9A)).

4.5. Manifesten en digitaal martelaarschap

Manifesten legitimeren, inspireren en sensationaliseren extremistisch geweld. De aanhoudende relevantie van lone-wolf terrorisme in de Digitale Golf gaat gepaard met een groei in de publicatie van online manifesten voorafgaand aan daden van extreem geweld of terrorisme.⁷⁸ Bekende voorbeelden zijn het 1518 pagina's tellende manifest van rechts-extremisten Anders Breivik 2083 – *A European Declaration of Independence* en *The Great Replacement* van Christchurch schutter Brenton Tarrant. Naast ideologie bevatten manifesten drie gedeelde karakteristieken: een extreme vorm van in-group/out-group denken, demonisering en dehumanisering van de uit-groep en het presenteren van geweld als enige overgebleven optie voor het teweegbrengen van verandering.⁷⁹ Daarmee vervullen dergelijke manifesten voor de auteur een belangrijke rol in de legitimatie en psychologische rechtvaardiging van extremistisch geweld. Extremisten gebruiken manifesten daarnaast als onderdeel van een bewuste strategie om copy cats te inspireren tot het uitvoeren van soortgelijke geweldsdaden. Manifesten bevatten vaak expliciete oproepen of geven instructies over hoe geweld uit te voeren. Andersom verwijzen nieuwe manifesten vaak terug naar eerdere teksten van extremisten.⁸⁰ Een manifest dient daarmee ook om sensatie te genereren rondom de geweldsdaad en de dader zelf. In die zin zijn manifesten performatieve documenten waarmee de auteur betekenis en erkenning zoekt binnen de online gemeenschap. Dit fenomeen wordt

⁷⁸ Jacob Ware, *Testament to Murder: The Violent Far-Right's Increasing Use of Terrorist Manifestos*, ICCT, 2020.

⁷⁹ Julia Ebner, e.a., *Measuring socio-psychological drivers of extreme violence in online terrorist manifestos: an alternative linguistic risk assessment model*, *Journal of Policing, Intelligence and Counter Terrorism*, 19(2), 2024.

⁸⁰ Primavera Fisogni, *Contagion of Evil: The New Wave of Terrorism on the Onlife World*, 2020, pp. 44-47.

versterkt door online subculturen waarin de aanslagpleger niet slechts een dader is, maar een 'digitale martelaar' die navolging verdient.

Digitaal martelaarschap. De zogenaamde Saints Culture duidt op hoe daders van extremistisch geweld met gebruik van symboliek worden verheven tot quasi-religieuze voorvechtersfiguren en hun manifesten tot heilige teksten.⁸¹ De heiligverklaring is ook van toepassing op aanslagplegers die hun aanslagen hebben overleefd en zijn veroordeeld, zoals Anders Breivik.⁸²

Elliot Rodger: van Incel tot Heilige. De zaak van Incel Elliot Rodger is illustratief voor de manier waarop online manifesten en martelaarschap als inspiratiebron dienen voor extremistisch geweld. In 2014 publiceerde Rodger zijn manifest *My Twisted World: The Story of Elliot Rodger* waarin hij zijn misogyne en racistische wereldbeeld uiteenzette. In wat wordt beschouwd als een van de eerste extreem gewelddadige uitingen van de Incelgemeenschap, bracht Rodger vervolgens zes mensen om het leven en verwondde 14 anderen. In de jaren na deze aanslag refereerden andere misogyne daders van extremistisch geweld aan Elliot als inspiratiebron. Binnen de Incel gemeenschap verkreeg Rodger de status van heilige: men refereert aan 'Saint Elliot', herdenkt de dag van de aanslag als Saint Elliot's Day en beelt Rodger af als christelijke heilige. Tegelijkertijd fungeert zijn manifest als een soort bijbel die Incels bediscussiëren, interpreteren en gebruiken om dichterbij Rodger te komen (Witt, 2020).

4.6. 'Hybrid net activism' en 'leaderless resistance'

Hybrid net activism: de decentrale organisatievorm van hedendaags activisme. Om de online organisatie van extremistische groeperingen en bewegingen te begrijpen, is het nuttig om te kijken naar de manier waarop legitieme activistische bewegingen zich online organiseren. Een combinatie van technologische mogelijkheden en maatschappelijke atomisering heeft geleid tot een vorm van collectieve actie waarin online en offline activisme in elkaar overvloeien. In dit hybride activisme zijn het niet centrale, hiërarchische organisaties waarop een sociale beweging leunt, maar losse netwerken met veel ruimte voor improvisatie en individualiteit.⁸³ Individuen functioneren in een netwerk als op zichzelf staande knooppunten. Het gebrek aan afhankelijkheden maakt snel opschalen mogelijk, waardoor men zich snel en flexibel kan aanpassen in bijvoorbeeld het organiseren van een protest.⁸⁴

⁸¹ Graham Macklin, *Terrorgram: Saints Culture*, Accelerationism Research Consortium, 2024.

⁸² Ari Ben Am & Gabriel Weimann, *Fabricated Martyrs: The Warrior-Saint Icons of Far-Right Terrorism*, *Perspectives on Terrorism*, 14(5), 2020.

⁸³ W. Lance Bennet & Alexandra Segerberg, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*, *Information, Communication & Society*, 15(5), 2012.

⁸⁴ Zozan Baran & Daniela Stoltenberg, *Dynamics of scale shift: Contentious places and hybrid activism on social media*, *New Media & Society*, 2024.

Self-organizing systems (SOS): De organisatiestructuur van Extinction Rebellion

is een voorbeeld van hybride activisme mogelijk gemaakt door de technologische ontwikkelingen van deze tijd. Verschillende 'cellen', met elk een eigen functie, opereren als zelfstandige knooppunten die in een digitaal netwerk gezamenlijke online en offline actie coördineren en teweegbrengen. Individuen kunnen zich vrij aansluiten bij knooppunten in dit netwerk afhankelijk van hun interesses en vaardigheden. Deze gedecentraliseerde organisatievorm kan zonder centrale aansturing in nieuwe lokale contexten worden toegepast en aangepast. Op deze manier kan Extinction Rebellion als sociale beweging groeien zonder afhankelijkheid van traditionele centrale organisatiestructuren, maar door de spontane mobilisatie van individuen op het internet die in dit hybride activisme erkenning en zingeving vinden.

'Leaderless resistance' in het online extremistisch ecosysteem. De hybride, fluide organisatiestructuur van hedendaags activisme vertaalt zich in de context van online extremisme naar het fenomeen leaderless resistance. Het online ecosysteem van extremisme bevordert de gepersonaliseerde radicalisering van individuen die vaak informeel onderdeel zijn van een digitaal netwerk of beweging, maar die zich niet expliciet aansluiten bij een traditionele hiërarchische organisatie. Het gevolg voor extremistisch geweld is de dominantie van lone-wolf aanslagen: geweldsdaden uitgevoerd door eenlingen die zijn geïnspireerd (eventueel aangemoedigd) door online extremistische groeperingen, maar door niemand zijn aangestuurd.⁸⁵ Extremistische bewegingen kiezen vaak bewust voor zo'n fluide, decentraal organisatie-model om betrokkenheid bij geweldsdaden te kunnen ontkennen en andere betrokken individuen te beschermen. Zo beschrijft het Siege manifest van rechts-extremist Jason Mason hoe het "White Liberation Front het best kan worden opgebouwd volgens het 'Drie-plus-één'-model: drie soldaten en één eenheidsleider, die als enige contact heeft met de groepsleider die leiding geeft aan drie eenheden."⁸⁶

Active Club network: een netwerk van online/offline groeperingen. Ook het Active Club network, geïntroduceerd door witte suprematist Robert Rundo, gevoed door zijn 'netwerkfilosofie' van 'white nationalism 3.0', volgt bewust een *leaderless resistance* organisatie-model. In lokale Active Clubs verzamelen kleine groepen aanhangers zich met een combinatie van vechtsport en politiek activisme voor te bereiden op een onvermijdelijke rassenoorlog. Hoewel de offline activiteiten en rekrutering van deze clubs een lokale focus hebben, zijn alle Active Clubs aangesloten bij het online Active Club network op met name Telegram, waar zij ideologische inspiratie en praktische tips opdoen. Zo is er een hybride en decentraal netwerk van witte suprematische cellen ontstaan dat zich makkelijk kan uitbreiden naar nieuwe steden en landen. Zo kende het netwerk in 2023 al meer dan 92 clubs in zowel de VS als Europa (Ritzman, 2023; ADL, 2023)

⁸⁵ Jacob Ware, *The Evolution of Far-Right Terrorist Tactics and Targeting*, *Studies in Conflict & Terrorism*, 2024, pp. 3-9.

⁸⁶ Siege manifest, p. 480.

‘Swarming’ en spontane collectieve actie. Decentrale digitale netwerken bieden een omgeving voor het ontstaan van spontane – soms bewust opgehitste – collectieve actie. Online neemt dit de vorm aan van *swarming*: online intimidatiecampagnes uitgevoerd door zwermen aan trollen. Zulke campagnes kunnen honderden tot duizenden gebruikers mobiliseren om een aangewezen doelwit te bombarderen met intimiderende berichten en bedreigingen.⁸⁷ Spontane collectieve actie vertaalt zich ook naar de offline wereld. In juli 2024 leidde een combinatie van desinformatie, rechts-extremistische beïnvloeding en maatschappelijk ongenoegen in reactie op een steekincident tot het uitbreken van massale rellen in Southport en 26 andere steden in het Verenigd Koninkrijk. Een analyse van het rechts-extremistisch online ecosysteem in de dagen rond het incident laat zien dat verscheidende Telegramgroepen en andere alternatieve media een bepalende rol hadden in het mobiliseren van een ideologisch diverse groep relschoppers. Daarbij ontstond een digitaal netwerk dat zich uitstapte over meer dan 400 Telegramgroepen, 100 Youtube livestreams en meer dan 3000 links naar andere platforms.⁸⁸ Dit laat zien hoe schaalbare en fluïde digitale netwerken in korte tijd kunnen groeien en aanzetten tot massale collectieve actie in de offline wereld.

Technologische decentralisatie van online extremistische ecosystemen. Ook de digitale infrastructuur gebruikt door online extremisten raakt in toenemende mate gedecentraliseerd onder druk van content moderatie en succesvolle opsporing. Om hun afhankelijkheid van mainstream kanalen te verminderen ontwikkelen online groeperingen een eigen digitale infrastructuur: van alternatieve sociale media tot financiële ecosystemen met gebruik van cryptocurrencies voor crowdfunding. *Peer-to-peer* technologieën zoals Odysee en PeerTube maken het mogelijk extremistische content decentraal op te slaan en te bereiken, wat moderatie en toezicht bemoeilijkt.⁸⁹ Deze ontwikkeling staat in de context van een bredere trend waarbij onlinegebruikers steeds vaker gebruikmaken van gedecentraliseerde sociale media zoals Mastodon en Bluesky, onderdeel van het zogenaamde Fediverse.⁹⁰

⁸⁷ Xinyi Zhang & Mark Davis, *E-extremism: A conceptual framework for studying the online far right*, *new media & society*, 26(5), 2024, p. 2964.

⁸⁸ Institute for Strategic Dialogue, *Quantifying extremism: A data-driven analysis of UK riot-related far-right Telegram networks*, 2024.

⁸⁹ Dominik Hammer, e.a., *Inside the Digital Labyrinth – Right-Wing Extremist Strategies of Decentralisation on the Internet and Possible Countermeasures*, *Institute for Strategic Dialogue*, 2023, pp 12-15.

⁹⁰ Paula Gürtler, *Unpacking the Fediverse*, *Centre for European Policy Studies*, 2025.

5. Implicaties voor de maatschappelijke stabiliteit in Nederland

De implicaties van online extremisme voor de maatschappelijke stabiliteit in Nederland zijn in essentie drievoudig. Ze verdienen serieuze aandacht binnen zowel het veiligheidsdomein als het bredere publieke debat.

Ten eerste lijkt de kans op gewelddadige aanslagen toe te nemen van met name jongens die in de digitale biotopen verstrikt raken. In de VS is het aantal gevallen van online geïnspireerde extremistische eenlingen goed zichtbaar. De vraag is of Europa dezelfde tendensen te wachten staat. In Nederland zien we voorzichtige trends die wijzen in de richting van een toenemend online geïnspireerd terrorisme.

De tweede implicatie betreft de ondermijning van de democratische rechtsorde. Deze vorm van destabilisatie is minder zichtbaar, maar niet minder ontwrichtend. Waar geweldsdreiging zich concentreert op incidenten, werkt ideologische ondermijning als een langzaam corroderend proces. Dit uit zich onder meer in de normalisering en popularisering van antidemocratische of anti-institutionele 'tropes': hardnekkige denkbbeelden en narratieven die de legitimiteit van democratische instituties, rechtsstatelijke procedures of journalistieke normen ter discussie stellen. De kracht van deze retoriek zit in de aansluiting bij bestaande gevoelens van onvrede, onmacht of vervreemding. In plaats van zich af te zetten tegen de mainstream, haken online extremistische boodschappen daar op in, waardoor ze op subtiele wijze het maatschappelijk discours verschuiven.

Een derde, steeds veel onduidelijker waarneembare implicatie betreft de vervloeiing van online extremisme met de invloedssfeer van statelijke actoren en vormen van hybride aanvallen. Er zijn sporen van Russische inmenging in extremistische online dynamiek maar het is lastig om harde bewijzen te overleggen. Ten minste vervullen extremistische netwerken een vehikel voor uitwisseling tussen extremistische scenes in autocratische landen en Westerse gebieden. In de volgende paragrafen gaan wij dieper op deze implicaties in.

5.1. Online geïnspireerd terrorisme en extremistisch geweld

De schijnbaar toenemende samenkomst van radicalisering op jonge leeftijd, de opkomst online subculturen, psychologische kwetsbaarheid en ideologische vermenging roept vragen op over de aard en dynamiek van hedendaagse radicaliseringstrajecten. Deze sectie richt

zich daarom op de vraag in hoeverre deze ontwikkelingen een opmerkelijke rol spelen in radicaliseringstrajecten van terrorismegevallen, en of er ook in Nederland sprake is van een dergelijke trend.

Buitenlandse casussen illustreren een trend van online geïnspireerd terrorisme en extremistisch geweld. Hoewel het op basis van gefragmenteerde terrorisme-incidenten niet mogelijk is om een duidelijke trendbeeld vast te stellen, zijn er inmiddels talloze buitenlandse casussen waarbij extremistisch of terroristisch geweld duidelijk in verband staat met de online activiteiten van de dader. Vaak kan dit worden afgeleid uit de manifesten die daders achterlaten of online publiceren, die bol kunnen staan van onsamenhangende internetretoriek. De online invloed lijkt vooral herkenbaar in het rechts-extremistische domein en de Incelosfeer. Toch speelt online geïnspireerd terrorisme vermoedelijk breder dan alleen op rechts, zoals binnen islamitisch- en links-extremistische milieus. Al zijn de voorbeelden in met name de links-extremistische hoek zeer schaars en ook minder evident, online geradicaliseerd omdat deze gemeenschappen zich ook sterk fysiek organiseren om maatschappelijke activisme te bedrijven. Een selectie van tamelijk recente zaken, zeker niet uitputtend, waarbij online ecosystemen en biotopen een nadrukkelijke rol speelden:

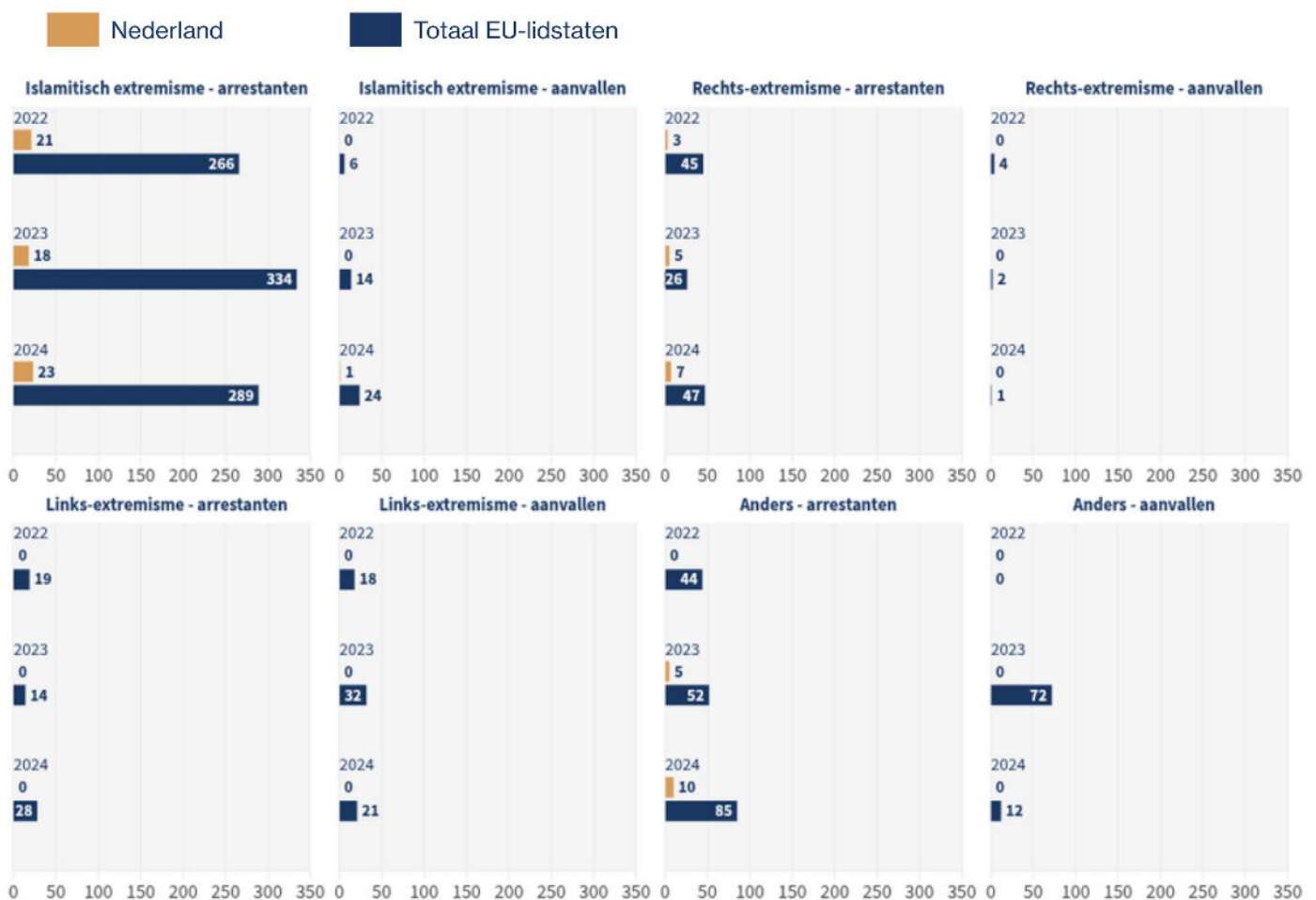
Tabel 1. Buitenlandse voorbeelden van online geïnspireerd terrorisme en extremistisch geweld.



Online extremistisch ecosysteem	Voorbeelden van online geïnspireerd terrorisme en extremistisch geweld (niet uitputtend)
Rechts-extremisme	• <i>Christchurch (2019)</i>. Brenton Tarrant vermoordt 51 mensen in twee moskeeën. Hij was actief op fora zoals 8chan en consumeerde jarenlang haatcontent. Zijn manifest, dat nog steeds breed circuleert, is doordrenkt met memes en dog whistles. Ook live-streamde hij de aanslag op Facebook in first-person shooter-stijl om de volledige online aandacht op te eisen. • <i>Oslo/Bærum (Noorwegen, 2019)</i>. Philip Manshaus (21) pleegt een mislukte aanslag op een moskee nadat hij zijn geadopteerde Aziatische stiefzus vermoordt. Hij radicaliseerde via Telegram. • <i>Hanau (Duitsland, 2020)</i>. Tobias Rathjen schiet negen mensen met een migratieachtergrond dood. Hij publiceerde online complottheorieën over "mind control" en demoniseerde migranten. • <i>Buffalo (VS, 2022)</i>. Payton Gendron (18) vermoordt tien zwarte Amerikanen in een supermarkt. Hij radicaliseerde op 4chan, Reddit en Discord en spiegelde zich aan Christchurch en El Paso. Zijn manifest bevatte memes, grafieken en verwijzingen naar digitale subculturen.
Manosfeer Incelosfeer	• <i>Isla Vista (VS, 2014)</i>. Elliot Rodger vermoordt 6 mensen en verwondt 14 personen in een misogynie aanslag op en rondom de Santa Barbara campus in Californië. • <i>Toronto (Canada, 2020)</i>. Een 17-jarige jongen vermoordt een medewerkster van een vrouwenopvang, geïnspireerd door het Incel-gedachtegoed.
Islamitisch extremisme	• <i>Wenen (Oostenrijk, 2020)</i>. Kujtim Fejzulaj pleegt een jihadistische aanslag waarbij vier mensen sterven. Hij bleek actief in IS-gekoppelde Telegramgroepen en radicaliseerde grotendeels online. • <i>Conflans-Sainte-Honorine (Frankrijk, 2020)</i>. Abdoullakh Anzorov onthoofd de Franse leraar Samuel Paty na het bekijken van virale berichten op sociale media waarin de docent werd beschuldigd van islamofobie. De dader raakte in enkele dagen geradicaliseerd, sterk aangewakkerd door Facebook- en TikTok-campagnes waarin het beeld van Paty werd opgevoerd als vijand. • <i>London (VK, 2020)</i>. Sudesh Amman (20) pleegt enkele dagen na zijn vrijlating een mesaanval in Londen. Tijdens zijn detentie bleef hij actief IS-propaganda downloaden en verspreiden via Telegram.
Links-extremisme	• <i>Portland (VS, 2020)</i>. Zelfverklaarde antifascist Michael Reinhoehl schiet een rechts-extremistisch lid van een knokploeg dood tijdens protesten in Portland. Hoewel de actie niet direct voortkwam uit een georganiseerde groep, weerspiegelde deze wel een bredere online militante sfeer.

Hoewel deze incidenten op zichzelf nog geen trend vormen, laat de opeenstapeling van casuïstiek zien dat online biotopen een factor zijn van inspiratie en radicalisering. De digitale omgeving fungeert daarbij niet louter als facilitator, maar ook als katalysator en inspirator. Hoewel veel van deze aanslagen uit verschillende ideologische hoeken komen en variëren in schaal en impact, delen ze een online gedeelde codes en narratieven. Deze aanslagen staan in de context van een aanhoudende terroristische geweldsdreiging binnen de EU en Nederland (zie onderstaande figuur).

Figuur 4. Aanslagen en arrestaties met een terroristisch oogmerk in de EU (Europol)



Bron: Europol, European Union Terrorism Situation and Trend Report 2025

Online geïnspireerd terrorisme in Nederland? Hoewel in het buitenland al meer aandacht is besteed aan de rol van online radicalisering in de aanloop naar terroristisch geweld, is hierover in de Nederlandse context nog relatief weinig systematische kennis beschikbaar. Toch zijn er ook in Nederland aanwijzingen dat het internet een significante rol speelt in het ontstaan van terroristische dreiging. Om voor deze studie inzicht te krijgen in de rol van online radicalisering bij Nederlandse terrorismeverdachten hebben we een analyse uitgevoerd van meer dan honderd terrorisme gerelateerde strafzaken in de periode 2014-2024. Een systematische, gerichte zoekopdracht via Rechtspraak.nl leverde 123 relevante casussen op

waarvan 90 voldoende informatie bevatten over het radicaliseringstraject van de verdachte om opgenomen te kunnen worden in onze database. Voor elke verdachte is vervolgens vastgesteld welke vormen van radicalisering zichtbaar waren, op basis van gangbare radicaliseringstrajecten in de wetenschappelijke literatuur (zie bijlage).⁹¹ De nadruk lag daarbij op de mate waarin online of sociale media expliciet werden genoemd als factor in het radicaliseringsproces, de aanwezigheid van psychische instabiliteit en tekenen van hybridisatie in de aangehangen ideologie. Door op deze manier te onderzoeken welke rol het internet speelde in radicaliseringstrajecten van terrorismeverdachten wordt het mogelijk om met meer zekerheid eventuele trends en structurele patronen te duiden. Een belangrijke kanttekening is dat rechtszaken soms meerdere jaren duren, waardoor belangrijke lopende casussen nog niet beschikbaar zijn voor analyse, en dat de dossiers van minderjarige verdachten niet openbaar zijn. Zo zijn er volgens Europol in 2024 40 mensen in Nederland gearresteerd voor terrorisme gerelateerde zaken, terwijl pas 10 mensen terecht hebben gestaan en in de dataset zijn opgenomen.⁹² Daarnaast is de analyse enkel gebaseerd op openbare gegevens van Rechtspraak.nl, waar politie- en inlichtingendiensten vermoedelijk over een gedetailleerder beeld beschikken. De hier gepresenteerde cijfers geven daarmee een indicatie van een trend, maar schetsen absoluut geen volledig beeld.

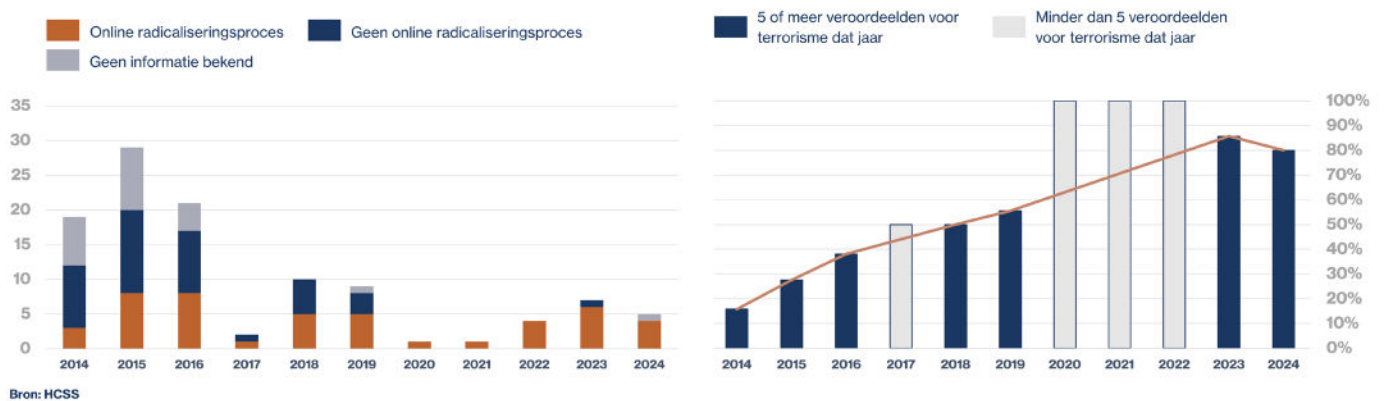
Online extremisme speelt een steeds nadrukkelijker rol bij Nederlandse terrorismeverdachten. Bij een meerderheid (56,6%) van de geanalyseerde verdachten blijkt het internet expliciet een rol te hebben gespeeld in hun radicalisering. Dit blijkt bijvoorbeeld uit de aanwezigheid van extremistische content op hun apparaten, uit communicatie via digitale netwerken, of uit verwijzingen naar online propaganda.⁹³ Figuur 6 hieronder laat een toenemende trend zien. Waar in de periode 2014-2016 het aantal verdachten met een duidelijke online component nog relatief beperkt was, is tussen 2019 en 2024 bij een overgrote meerderheid van de verdachten sprake van online radicalisering, met relatieve aandelen die schommelen tussen de 70% en 90%. Ook in de jaren met een beperkt aantal zaken – 2023, 2023 en 2024 – blijft de online component in de meeste gevallen aanwezig. Online beïnvloeding speelt een toenemende rol van betekenis.

⁹¹ Elke case die is opgenomen in de data base is beoordeeld en kreeg één of meer indicatoren toegewezen op basis van hun radicaliseringsproces (bv. Online social media (2), psychologische problemen (6), enz.). Sommige individuen hadden slechts één indicator, terwijl anderen er meerdere hadden. Belangrijk dus is dat de grafiek niet het aandeel laat zien hoeveel personen online zijn geradicaliseerd, maar eerder het aandeel van alle indicatoren in een bepaald jaar die als 'online/social media' zijn geclassificeerd.

⁹² Europol, European Union Terrorism Situation and Trend Report, 2025, p.16

⁹³ Toelichting: wanneer is de indicator 'online radicalisering' wel/niet toegewezen? De indicator is toegekend wanneer er in de verslaglegging voldoende aanwijzingen zijn dat digitale omgevingen een rol speelden in het radicaliseringstraject. De informatie is meestal terug te vinden in het onderdeel over 'de persoon van de verdachte', waar persoonsrapportages, psychologische beoordelingen en reclasseringsadviezen zijn opgenomen. Aangezien de radicaliseringsroute zelden expliciet wordt beschreven, is de toewijzing gebaseerd op interpretatie van indirecte signalen. Daarbij is steeds gezocht naar tekenen van betrokkenheid bij online netwerken of beïnvloeding via digitale kanalen. De indicator is wél toegewezen wanneer: In de rapportages expliciet wordt verwezen naar intensief en ideologisch gericht online gedrag, zoals langdurige tijdsbesteding aan extremistische content of actieve aanwezigheid op radicale kanalen; De verdachte aantoonbaar beeld- of tekstmateriaal met extremistische of terroristische strekking heeft vervaardigd of verspreid; De verdachte actief deelnam aan gesloten of semi-gesloten online extremistische fora of chatgroepen. De indicator is niet toegewezen wanneer het online gedrag beperkt bleef tot praktische informatievergaring, zoals het opzoeken van reisroutes; Er slechts incidenteel communicatie plaatsvond via online kanalen (zoals WhatsAppgesprekken met een buitenlandse contactpersoon); Het gebruik van social media beperkt bleef tot een eenmalige of oppervlakkige uiting zonder aantoonbare radicale betrokkenheid. Bij twijfelgevallen is ervoor gekozen de indicator niet toe te wijzen.

Figuur 5. Absolute en relatieve aandeel van Nederlandse veroordeelden voor terrorisme* waarbij wel of geen sprake is van online radicalisering in de gerechtelijke verslaglegging



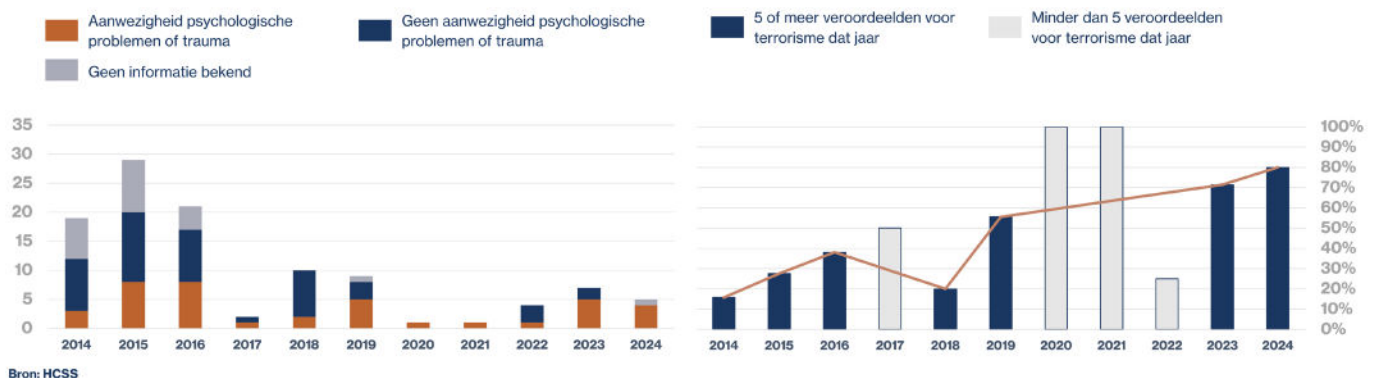
Bron: HCSS

*Met 'veroordeelden voor terrorisme' wordt bedoeld: verdachten die zijn veroordeeld op verdenking van 1) het plegen van een terroristische daad (Artikel 289a & 288a Sr); 2) voorbereiding terroristische misdrijven/aanslag (Artikel 176a,b Sr); 3) opruiing tot terroristische daden (Artikel 131 lid 1,2 & 83a Sr); 4) deelname aan een terroristische organisatie (Artikel 140a, 47, 48, 46a, 83c Sr); 5) andere aan terrorisme gelieerde misdrijven zoals het verzorgen van terroristische training, het verschaffen van inlichtingen aan terroristische organisatie(s) (B.v. Artikel 134a Sr). Verdachten van het financieren van terroristische organisaties zijn buiten beschouwing gelaten omdat deze daad minder duidelijk samenhangt met de mogelijkheid tot persoonlijke bereidheid tot geweldpleging op basis van (online) radicalisering. Van belang is om te melden dat de telling gebaseerd is op publieke gegevens van Rechtspraak.nl. Het beeld is daarom slechts indicatief en niet representatief. De criteria op grond waarvan zaken werden gemarkeerd als 'nadrukkelijk sprake van online radicalisering', o.q. 'nadrukkelijk sprake van psychologische ontoerekeningsvatbaarheid' zijn opgenomen in de bijlage van dit rapport.

De rol van psychologische kwetsbaarheid en ontoerekeningsvatbaarheid. Bij minder dan de helft van de geanalyseerde strafzaken concludeerden deskundigen dat de verdachte in verminderde mate, of volledig, ontoerekeningsvatbaar was wegens de aanwezigheid van psychologische problematiek.⁹⁴ Hoewel ontoerekeningsvatbaarheid geen sluitende maat is voor psychologische problematiek in bredere zin, vormt het wel een belangrijke indicator voor het feit dat mentale kwetsbaarheid een duidelijke rol heeft gespeeld in het radicaliseringsproces van de verdachte. Onderstaande Figuur 7 laat zien dat het relatieve aandeel verdachten met psychologische problemen of trauma geleidelijk toenam van 10-30% rond 2016 naar 70-80% in 2023 en 2024. Dit suggereert een opwaartse trend, al moet hierbij rekening worden gehouden met het kleine absolute aantal casussen in de database. Daarnaast worden forensisch-psychologische beoordelingen alleen opgenomen als deze in het kader van de strafmaat relevant zijn. De stijgende lijn in het relatieve aandeel kan deels samenhangen met veranderde verslagleggingspraktijken, of met een grotere bereidheid om psychologische kwetsbaarheden mee te wegen. Voorzichtigheid blijft dus geboden: het beeld is hooguit indicatief, niet representatief.

⁹⁴ Bij de toewijzing van de indicator 'psychologische ontoerekeningsvatbaarheid' is uitgegaan van expliciete passages in de rechterlijke verslaglegging, in het bijzonder uit de onderdelen waarin persoonsrapportages, forensisch-psychologische beoordelingen of reclasseringsadviezen zijn opgenomen. De indicator is uitsluitend toegekend wanneer deskundigen concludeerden dat de verdachte in verminderde mate, of volledig, ontoerekeningsvatbaar was wegens de aanwezigheid van psychologische problematiek. Dit kon op twee manieren voorkomen; (1) Omdat de verdachte ten tijde van het tenlastegelegde feit door psychologische problematiek beperkte of geen controle had over zijn/haar handelen of (2) dat uit rapportages bleek dat een psychische aandoening, verstandelijke beperking of trauma actief heeft bijgedragen aan de totstandkoming van het extremistische gedrag of het radicaliseringstraject. Een voorbeeld hiervan is het volgende: "Bij de verdachte is sprake van een licht verstandelijke beperking. Hij reageert vaak direct en op een impulsieve manier en hij is gemakkelijk beïnvloedbaar. [...] Hij was ten gevolge daarvan niet goed in staat om de impact van de racistische en rechts-extremistische uitspraken die hij zelf deed en welke hij deelde te overzien. Geadviseerd wordt om verdachte het tenlastegelegde vanwege zijn licht verstandelijke beperking in verminderde mate toe te rekenen." In gevallen waarin sprake was van psychologische problematiek, maar waarbij deze geen aantoonbare rol speelde in het handelen of de ideologische ontwikkeling van de verdachte, is de indicator niet toegekend. Dit gold ook voor situaties waarin psychische klachten pas ná het delict zijn ontstaan (zoals een posttraumatische stressstoornis ten gevolge van detentie of verblijf in een oorlogsgebied). In alle twijfelgevallen is ervoor gekozen de indicator niet toe te wijzen, teneinde de methodologische integriteit van de analyse te behouden.

Figuur 6. Absolute en relatieve aandeel van Nederlandse veroordeelden voor terrorisme waarbij nadrukkelijk wel of geen sprake is van psychologische ontoerekeningsvatbaarheid in de gerechtelijke verslaglegging



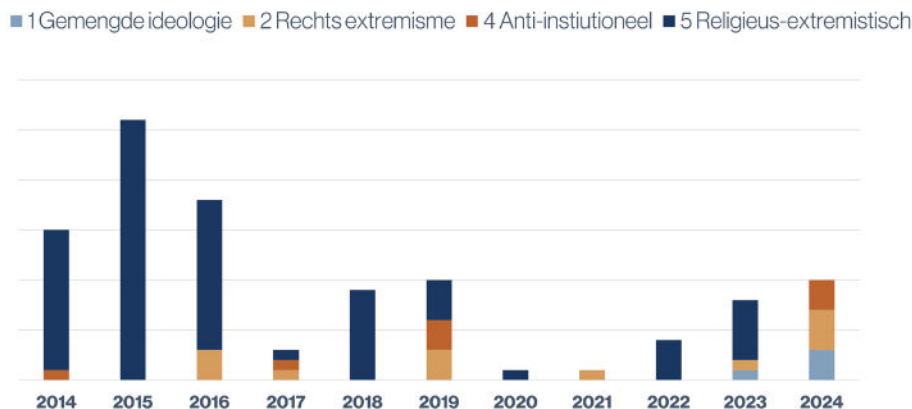
Bron: HCSS

*Met 'veroordeelden voor terrorisme' wordt bedoeld: verdachten die zijn voorgeleid op verdenking van 1) het plegen van een terroristische daad (Artikel 289a & 288a Sr); 2) voorbereiding terroristische misdrijven/aanslag (Artikel 176a,b Sr); 3) opruiing tot terroristische daden (Artikel 131 lid 1,2 & 83a Sr); 4) deelname aan een terroristische organisatie (Artikel 140a, 47, 48, 46a, 83c Sr); 5) andere aan terrorisme gelieerde misdrijven zoals het verzorgen van terroristische training, het verschaffen van inlichtingen aan terroristische organisatie(s) (Bv Artikel 134a Sr). Verdachten van het financieren van terroristische organisaties zijn buiten beschouwing gelaten omdat deze daad minder duidelijk samenhangt met de mogelijkheid tot persoonlijke bereidheid tot geweldpleging op basis van (online) radicalisering. Van belang is om te melden dat de telling gebaseerd is op publieke gegevens van Rechtspraak.nl. Het beeld is daarom slechts indicatief en niet representatief. De criteria op grond waarvan zaken werden gemarkeerd als 'nadrukkelijk sprake van online radicalisering', cq. 'nadrukkelijk sprake van psychologische ontoerekeningsvatbaarheid' zijn opgenomen in de bijlage van dit rapport.

Hybridisatie van ideologie? Bij verreweg de meeste verdachten was er sprake van één dominante ideologie, hoewel er in 2023 en 2024 vaker sprake was van daders die meer dan één ideologie hanteerden. In lijn met Rapoorts viergolventheorie en het Dreigingsbeeld Terrorisme Nederland is bekeken of verdachten een rechts-extremistische, links-extremistische, anti-institutionele of religieus fundamentalistische ideologie aanhielden. Als er sprake was van meer dan één dominante ideologie – ideologische hybridisatie – is dit aangegeven als 'gemengde ideologie'. Zoals te zien in Figuur 8 is religieus-extremisme het meest dominant onder daders in de periode 2014-2018, terwijl dit beeld in latere jaren iets diffuser wordt. Het figuur komt daarmee sterk overeen met het Dreigingsbeeld Terrorisme Nederland, en Rapoorts viergolventheorie die voorspelt dat we tussen 2020-2025 een nieuwe golf zouden zien vormkrijgen. De ideologische hybridisatie geobserveerd in 2023 en 2024 kunnen de eerste tekenen zijn van deze nieuwe Digitale Golf in Nederland. In 2023 ging het bijvoorbeeld om een verdachte die in zijn op Telegram verspreide manifest een verwarrende mix van islamitisch- en rechts-extremistische overtuigingen liet zien. In dit manifest stonden daarnaast verschillende memes over thema's zoals LHBTIQ+ en vrouwenrechten, en denkstromingen zoals het marxisme en communisme.⁹⁵ Hoewel het nog te vroeg is om een duidelijke trend vast te stellen, lijkt de data wel te wijzen op enige ideologische hybridisatie onder Nederlandse terrorismeverdachten.

⁹⁵ Rechtbank Midden-Nederland, [ECLI:NL:RBMNE:2024:5886](https://eclis.nl/RBMNE:2024:5886), 16.225800.23, 16 oktober 2024.

Figuur 7. Primair aangehangen ideologie door Nederlandse veroordeelden voor terrorisme*



Bron: HCSS

*Met 'veroordeelden voor terrorisme' wordt bedoeld: verdachten die zijn voorgeleid op verdenking van 1) het plegen van een terroristische daad (Artikel 289a & 288a Sr); 2) voorbereiding terroristische misdrijven/aanslag (Artikel 176a,b Sr); 3) opruiing tot terroristische daden (Artikel 131 lid 1,2 & 83a Sr); 4) deelname aan een terroristische organisatie (Artikel 140a, 47, 48, 46a, 83c Sr); 5) andere aan terrorisme gelieerde misdrijven zoals het verzorgen van terroristische training, het verschaffen van inlichtingen aan terroristische organisatie(s) (B.v Artikel 134a Sr). Verdachten van het financieren van terroristische organisaties zijn buiten beschouwing gelaten omdat deze daad minder duidelijk samenhangt met de mogelijkheid tot persoonlijke bereidheid tot geweldpleging op basis van (online) radicalisering. Van belang is om te melden dat de telling gebaseerd is op publieke gegevens van Rechtspraak.nl. Het beeld is daarom slechts indicatief en niet representatief. De criteria op grond waarvan zaken werden gemarkeerd als 'nadrukkelijk sprake van online radicalisering', cq. 'nadrukkelijk sprake van psychologische ontoerekeningsvatbaarheid' zijn opgenomen in de bijlage van dit rapport.

5.2. Druk op de democratische rechtsorde

Extremisten bedreigen de democratische rechtsorde. Veel extremistische bewegingen, zowel islamitisch als links- of rechts-extremistisch, lijken te worden gedreven door een fundamentele afkeer van de moderne samenleving. Zij beschouwen deze als corrupt, decadent of moreel failliet. Zij delen een afkeer van pluralisme en het idee van een open, tolerante samenleving, waardoor ze, ondanks hun tegengestelde ideologieën, bijdragen aan dezelfde dynamiek van maatschappelijke ontwrichting. Ook radicale anti-institutionele bewegingen, gedreven door complottheorieën of apocalyptisch denken, proberen de staat en haar instituties actief te delegitimeren door middel van desinformatie, sabotage en geweld.

Extremistische strategieën grijpen aan op autocratisch sentiment en complotdenken.

In het nastreven van deze antidemocratische en intolerante agenda's haken extremistische groeperingen aan op bestaande maatschappelijke onrust, autocratische tendensen en complotdenken in de samenleving. Door middel van de in Hoofdstuk 4 besproken digitale propagandatechnieken vermengen zij hun extremistische denkbeelden met actuele maatschappelijke thema's en gevoelens van ongenoegen. Daarmee bereiken extremisten op heimelijke wijze een breed digitaal publiek dat zo geleidelijk extremistische narratieven overneemt en normaliseert. Dit ondermijnt niet alleen de democratische rechtsorde, maar maakt ook een groter deel van de bevolking ontvankelijk voor rekrutering en radicalisering in een extremistisch gedachtengoed.

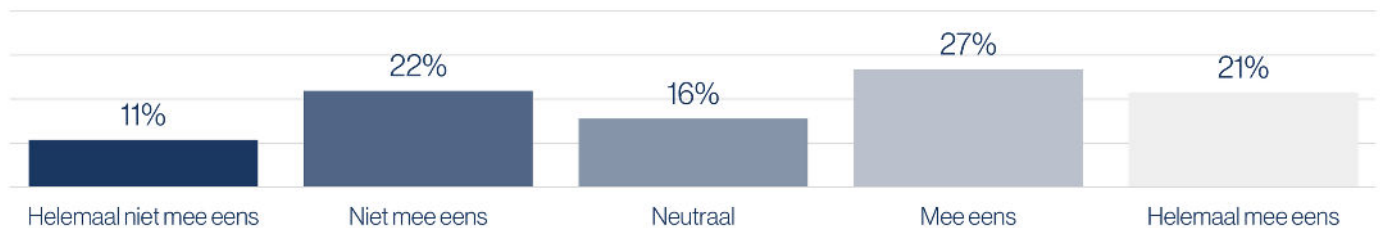
Een van de groeiende voedingsbodems voor extremisme in Nederland is het wantrouwen in de politiek en het functioneren van de democratie. Zo blijkt uit onderzoek van de HCSS Publieksmonitor dat 89% van de bevolking vindt dat de Nederlandse regering niet in staat

is met oplossingen te komen voor het land en beleid voornamelijk voor zich uitschuift.⁹⁶ Daarnaast heeft slechts een klein derde deel van de burgers het idee dat zij werkelijk invloed kunnen uitvoeren op het beleid van de overheid. Deze combinatie van teleurstelling in het handelen van de overheid en een gepercipieerd tekort aan democratische legitimiteit ondermijnt bij sommigen het vertrouwen in de democratie als bestuursmodel; de helft van de bevolking denkt dat de Nederlandse democratie minder goed zal functioneren. Het gevolg is dat 48% van de Nederlanders een grotere meerwaarde ziet in een daadkrachtige leider dan coalitievorming (zie Figuur 9), wat wijst op een significant autocratisch sentiment in de Nederlandse samenleving. Extremistische groeperingen haken in op dit sentiment door anti-democratische en anti-establishment narratieven te verspreiden onder een breder publiek en individuen te rekruteren op basis van deze grieven.

Figuur 8. Autocratisch sentiment in Nederland



In deze tijd hebben we meer aan een daadkrachtige leider dan aan een regering die altijd op zoek is naar compromissen



Bron: HCSS Publieksmonitor (zomer 2025)

De democratische rechtsorde komt verder onder druk te staan door de opkomst van complotdenken, dat het vertrouwen in democratische en maatschappelijke instituties doet afnemen. Tijdens de coronacrisis leidde een combinatie van een onbekende dreiging, sociale isolatie en economische instabiliteit tot een gevoel van existentiële onzekerheid, dat een deel van de bevolking vatbaar maakte voor samenzweringstheorieën. Sindsdien circuleren anti-institutionele en rechts-extremistische complottheorieën vrijelijk op sociale media en incidenteel binnen de politiek, terwijl het vertrouwen in traditionele informatiebronnen en de overheid afneemt. Uit cijfers van de HCSS Publieksmonitor (zie Figuur 10) blijkt dat dit aanhoudt: zo gelooft 37% procent van de bevolking in een achter de schermen opererende elite die macht uitoefent op politieke beslissingen. Extremistische groeperingen maken gebruik van deze ontvankelijkheid voor complotdenken om hun eigen theorieën en gedachtengoed te verspreiden. Zo vergroot de mate van complotdenken in de samenleving het risico op radicalisering in antidemocratische, extremistische gedachtengoeden die de democratische rechtsorde ondermijnen.

⁹⁶ HCSS, Publieksmonitor Maatschappelijke Stabiliteit, zomer 2025.

Figuur 9. Complotdenken in Nederland



Bron: HCSS Publieksmonitor (zomer 2025)

Verharding maatschappelijk debat en stochastisch terrorisme. Stochastisch terrorisme is de wetenschappelijke term voor hoe invloedrijke personen zoals politici of influencers bijdragen aan een klimaat waarin geweld tegen groepen statistisch waarschijnlijker wordt. Zo draagt een gepolariseerd en verhard maatschappelijk debat bij aan een verhoogde geweldsdreiging tegen bepaalde groepen. Dit gebeurt zonder directe oproep tot geweld maar door herhaalde demoniserende of dehumaniserende retoriek. De *broadcaster* verspreidt negatieve beeldvorming waarna dat via sociale media opgeblazen wordt. Er ontstaat zo een toenemende kans dat een extremistische eenling wordt getriggerd en handelt naar de opgeklopte vijandbeelden. In de praktijk is het onmogelijk om het precieze geweldsmotief van eenlingen te isoleren en de werkelijke invloed van toxische retoriek te identificeren. Ook de juridische grijze zone is problematisch: de oorspronkelijke uitingen zijn vaak beschermd door het recht op vrije meningsuiting. Stochastisch terrorisme duidt in die zin op een moeilijk oplosbaar probleem voor de democratische rechtsorde omdat de cascade-effecten van toxische retoriek moeilijk beteugeld kunnen worden. (Bron: Rand Europe, *Van woorden naar daden*, 2025).

Anocratieën en toenemende maatschappelijke instabiliteit. Het tanende vertrouwen in de democratie en maatschappelijke instituties in Nederland, en het autocratisch sentiment dat daarbij komt kijken, staan in de context van een wereldwijde democratische erosie. Waar in 2004 51% van de wereldbevolking in een vorm van democratie leefde, is dit in 2024 nog maar 27%. Slechts 12% van de wereldbevolking leeft in een liberale democratie zoals we die kennen in Nederland, blijkt uit data van het V-Dem Institute.⁹⁷ Wereldwijd is er volgens V-Dem bovendien sprake van toenemende druk op liberale democratieën en neemt de sympathie voor autocratisch bestuur toe. De transitie tussen democratie en autocratie wordt ook wel een staat van 'anocratie' genoemd; een situatie waarin een land kenmerken van beide vertoont, maar geen van beide volledig belichaamt. Volgens politicoloog Barbara Walter is het in deze transitieperiode dat het risico op politiek geweld – waaronder extremisme – het hoogst is (zie Figuur 11).⁹⁸ Als voorbeeld noemt Walter de VS die tegen het einde van Trump's eerste presidentschap de overgang maakte van een democratisch naar een anocratisch regime. Volgens haar verklaard deze transitie – en de democratische erosie die daaraan ten grondslag ligt – het uitbreken van massaal geweld tijdens de bestorming van het Capitool op 6 januari 2021.⁹⁹ Wanneer druk op de democratische rechtsorde leidt tot autocratische tendensen in

⁹⁷ V-Dem Institute, *Democracy Report 2025*, 2025.

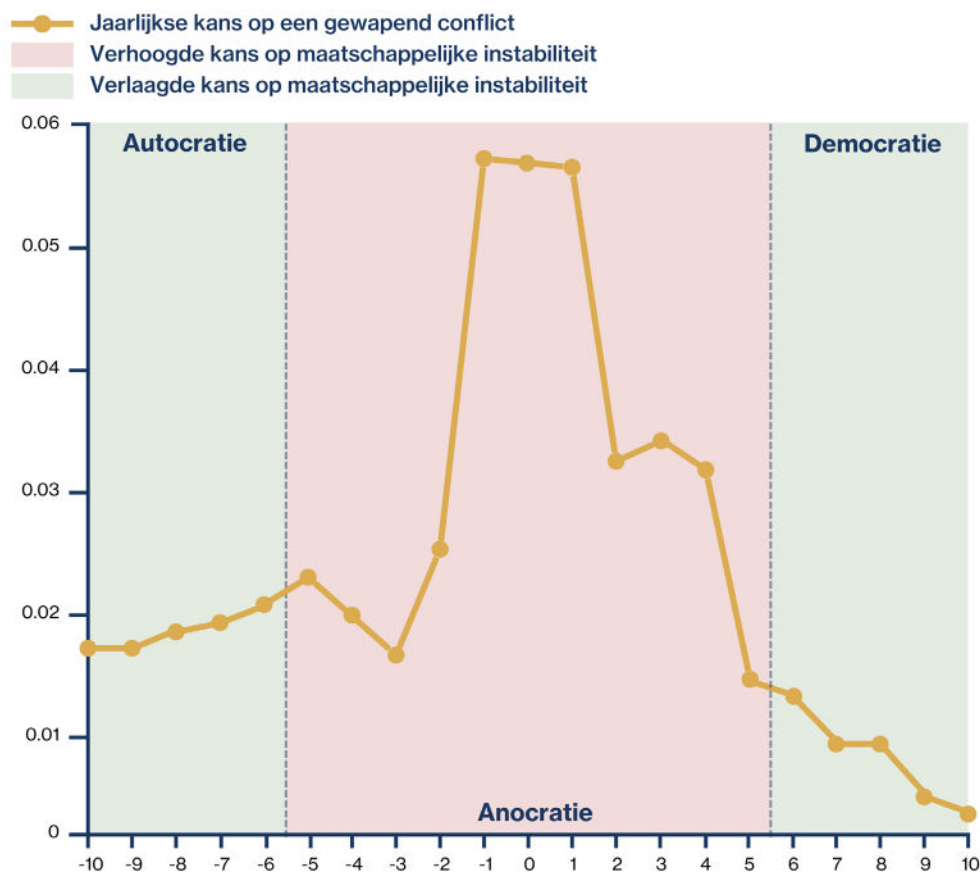
⁹⁸ Barbara F. Walter, *How Civil Wars Start: And How To Stop Them*, 2022.

⁹⁹ NPR, *All democracies are fragile – here are the early signs of civil war at home and abroad*, 2023.

het bestuur en politiek, ligt maatschappelijke instabiliteit dus op de loer. Extremistische groeperingen zullen gebruik maken van deze instabiliteit om hun ideologische agenda's te verspreiden en de democratische rechtsorde nog verder te ondermijnen.

‘Dark enlightenment’ (NRx): extremistische lijntjes naar mainstream politiek. Dark enlightenment (soms ook wel aangeduid als NRx, hoewel deze afkorting verwijst naar de bredere neoreactionaire beweging) is een antidemocratische ideologie die in de late jaren 2000 opkwam binnen online subculturen. Ideologische ‘kopstukken’ als Curtis Yarvin en filosoof Nick Land pleiten voor het faillissement van de liberale democratie ten gunste van autoritaire tech-oligarchieën. Daarmee verwerpen ze burgerlijke gelijkheid en beschouwen ze democratie als een obstakel voor vooruitgang. De ideeën zijn acceleratienistisch: door maatschappelijke implosie, ontstaat momentum voor een nieuw tijdperk. De invloed van NRx reikt verder dan de digitale wereld. In Silicon Valley hebben ‘brogarchs’ zoals Peter Thiel en Elon Musk belangstelling getoond voor deze ideeën. Politiek gezien hebben NRx-ideeën invloed gehad op de Amerikaanse politiek, met name binnen de entourage van voormalig president Donald Trump, waar bijvoorbeeld J.D. Vance elementen van deze ideologie zouden hebben omarmd. Daarmee is de anti-democratische NRx een voorbeeld van hoe online doctrines doorsijpelen in mainstream politiek.

Figuur 10. Anocratieën: staten in de gevarenzone van maatschappelijke instabiliteit



Bron: Barbara F. Walter, *How Civil Wars Start: And How to Stop Them*, 2022.

5.3. Sporen van vervloeiing met statelijke actoren

Landen zoals Rusland en Iran hebben via desinformatiecampagnes en online trollennetwerken bijgedragen aan het versterken van radicaal online sentimenten in westerse samenlevingen, door het uitvergroten van culturele tegenstellingen, het promoten van samenzweringstheorieën en het verspreiden van haatdragende content. Dit gebeurt niet alleen via open propaganda, maar ook door subtiele beïnvloeding van extremistische subculturen, waarbij bestaande radicale bewegingen worden versterkt en gestuurd zonder directe inmenging. Hierdoor vervaagt de grens tussen klassieke asymmetrische oorlogsvoering en de nieuwe realiteit van hybride oorlogsvoering, waarin staten extremistische groepen faciliteren en voeden als een manier om democratische samenlevingen van binnenuit te ondermijnen.

Desinformatie wakkert maatschappelijke onrust aan. Statelijke actoren zetten desinformatiecampagnes in om het maatschappelijk debat te polariseren en creëren zo een digitale omgeving die ontvankelijk is voor radicale en extremistische tendensen. Doel is hierbij het ondermijnen van maatschappelijke samenhang door het versterken van pessimistische en polariserende sentimenten.¹⁰⁰ Een concreet voorbeeld van deze werkwijze was zichtbaar tijdens de Europese Parlementsverkiezingen in 2024. Het Russische Social Design Agency zette een omvangrijk netwerk op van nieuwsites, Telegramkanalen en sociale media-accounts om maatschappelijke onrust aan te wakkeren en zo het electorale succes van radicaal-rechtse partijen te vergroten.¹⁰¹ Het gevolg van dergelijke campagnes is dat ook in Nederland pro-Russische narratieven en desinformatie weerklank vinden op mainstream sociale media en zelfs in de Nederlandstalige antwoorden van populaire AI modellen.¹⁰² En ook rechts-extremistische en anti-institutionele onlinemilieus nemen pro-Russische memes en standpunten over, vermoedelijk vanwege een ideologische overlap in misogyne, homofobe en fascistische thema's.¹⁰³ Op deze manier draagt desinformatie door statelijke actoren bij aan een gepolariseerde samenleving waarin radicaal gedachtengoed genormaliseerd raakt en maatschappelijke onrust een aangrijpingspunt vormt voor extremistische radicalisering.

Statale inmenging in extremistische milieus? In het Dreigingsbeeld Terrorisme Nederland (2024) waarschuwt de NCTV voor een groeiende interactie tussen de Russische staat en Westerse anti-institutionelen en rechts-extremisten.¹⁰⁴ Zo zochten zowel de Duitse Reichsbürgerbeweging als Franse soevereinen tijdens het voorbereiden van een staatsgreep ter ondersteuning contact met Russische liaisons. En ook Rusland zelf benadert en stimuleert actief anti-institutionele bewegingen om 'by proxy' bij te dragen aan de ondermijning van de rechtsorde. Steun aan rechts-extremistische groeperingen is nog directer: enkele leiders en groeperingen vinden in Rusland en op Russische sociale media een veilige haven. Ook rekruteert Rusland in rechts-extremistische chatgroepen individuen voor het uitvoeren van sabotageacties in Europese landen. Zo dient elke vorm van inmenging het Russische doel om maatschappelijke onrust en splijtzwammen aan te wakkeren. Hoewel directe interactie tussen Rusland en extremisten in Nederland volgens de NCTV minder vaak voorkomt dan in

¹⁰⁰ Christopher Paul & Miriam Matthews, *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Corporation, 2016.

¹⁰¹ James Pamment & Darejan Tsursumia, *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*, Psychological Defence Agency Sweden, 2025, pp. 79-89.

¹⁰² Pointer, *Een doodverklaarde NAVO-piloot en drugs van de Oekraïense overheid: zo worden AI-chatbots geïnfecteerd met Russische propaganda*, 19 Juni 2025.

¹⁰³ NCTV, *Dreigingsbeeld Terrorisme Nederland*, Juni 2025, pp. 40-42; Rijksuniversiteit Groningen, *Hoe een trollenleger de oorlogsretoriek van het Kremlin verspreidt*, 2023.

¹⁰⁴ NCTV, *Dreigingsbeeld Terrorisme Nederland*, Juni 2025, pp. 38-47.

andere landen, draagt de transnationale verspreiding van anti-institutionele en rechts-extremistische desinformatie en complottheorieën wel degelijk bij aan maatschappelijke onrust, ondermijning van democratische en maatschappelijke instituties, en bedreigingen richting zij die daar werken.

Van MKY wordt verondersteld dat deze werd opgericht door pro-Russische, Oekraïense ultranationalisten. Van de (inniddels ter ziele?) COM-groep 397 is bekend dat deze deels Russisch is, deels westers, omdat handleidingen over het maken van ontstekingsmechanismen bijvoorbeeld in beide talen in dit kanaal gedeeld werden.¹⁰⁵ Het hieronder besproken geval van de aanslag op Stürzenberger in Mannheim toont tenminste dat Duitse inlichtingendiensten Russen verdenken van actieve inmenging. Maar een daadwerkelijke (publiekelijk bekende) 'smoking gun' van actieve statelijke inmenging is er niet. Russische sporen kunnen bovendien ook worden uitgelegd als rechtse identificatie met de etnonationalistische politiek van Moskou, of simpelweg op internationale banden tussen gelijkgestemde extremisten in verschillende geopolitieke zones.

De aanslag in Mannheim met sporen van Russische inmenging. Op 31 mei 2024 vond in Mannheim een aanslag plaats tijdens een demonstratie van anti-islambeweging Pax Europa. Extreemrechtse influencer Michael Stürzenberger raakte ernstig gewond en een politieagent kwam om het leven. De gewezen Afghaanse asielzoeker Sulaiman Ataee stak hen neer voordat hij door de politie werd neergeschoten. Ataee verklaarde later dat hij handelde uit islamistische motieven. Over het werkelijke motief is echter twijfel ontstaan. Na de aanval bracht de Bundesnachrichtendienst (BND) naar buiten dat vanaf Russische ip-adressen — dagen vóór de aanslag — zoekopdrachten waren uitgevoerd met termen als “aanval op Michael Stürzenberger.” Daarnaast waren er vooraf pogingen gedaan om live camerabeelden van het marktplein te bekijken. Hoewel er geen direct bewijs is, beschouwt de Bundesnachrichtendienst (BND) deze digitale sporen als onderdeel van Russische inmenging. Dat zou duiden op Russische tactieken van stochastisch terrorisme (een tactiek van mediabeïnvloeding en demonisering die de kans op aanslagen verhoogt. Zie kader onder H. 5.2) of mogelijk zelfs de doelgerichte manipulatie van kwetsbare individuen. Zie kader onder H.) of mogelijk zelfs de doelgerichte manipulatie van kwetsbare individuen.

¹⁰⁵ The Red Pill Reversal, [From Shadows to Signal: The Extremist Emergence of Group “397”](#), 2025.

6. Strategische aandachtspunten

De voorgaande hoofdstukken hebben belicht hoe extremisme zich manifesteert in digitale ecosystemen, op basis van verschillende trends. Ook bespraken we dat de institutionele reactie hierop nog fragmentarisch is en dat er veel blinde vlekken zijn. In dit afsluitende hoofdstuk worden op basis van deze bevindingen enkele strategische aandachtspunten geformuleerd voor beleid, onderzoek en bestuurlijke praktijk. Deze aandachtspunten bieden geen blauwdruk en zijn niet uitputtend bedoeld. Ze vormen een weergave van punten opgemerkt in het onderzoeksproces als zodanig, of punten die deskundigen aandroegen ter versterking van de digitale weerbaarheid, opsporing en bewustwording over online extremisme.

6.1. Naar een betere kennispositie

Cijfers over de prevalentie en het bereik van online extremistische content in de Nederlandse context zijn zeer schaars. Er is tot op heden in Nederland geen structureel meetinstrument of centraal datapunt dat de omvang van extremistische uitingen op digitale platformen systematisch in kaart brengt, ook niet op basis van geanonimiseerde analyse van bulkdata. Nederland blijft grotendeels afhankelijk van thematische duidingen en fenomenanalyses van overheidsdiensten, zoals die van AIVD, NCTV of WODC, waarin trends, risicofactoren en voorbeelden worden geschetst. De uitspraken die worden gedaan in waarschuwende rapportages van overheidswege wijzen niet op systematische kwantitatieve monitoring. Deze rapporten bevatten in beginsel geen kwantitatieve metingen van het aantal extremistische accounts, het bereik van haatdragende posts of de verspreidingsdynamiek. Dit is in tegenstelling tot sommige landen waar gespecialiseerde organisaties via analyse van grootschalige steekproeven en datasets inzicht geven in het volume en bereik van online haat of extremisme, zoals ADL in de VS of Tech Against Terrorism internationaal. In de Nederlandse context registreert en verwijdert de Autoriteit Terroristisch en Kinderpornografisch Materiaal (ATKM) terroristisch materiaal, maar deze openbaart (tot op heden) geen (kwantitatieve) onderzoeksdata. Ook de NCTV waarschuwt regelmatig voor online radicalisering maar onderbouwt deze waarschuwingen zelden met meetbare gegevens. Hierdoor blijft het Nederlandse beeld van online extremisme fragmentarisch en methodologisch onderontwikkeld, zeker in vergelijking met landen als het VK. Ook commerciële transparantierapportages van grote techbedrijven leveren zelden uitsplitsingen op nationaal niveau. Wanneer deze bedrijven of andere internationale studies wel met tellingen komen, kan de Nederlandse situatie hooguit indirect worden geduid. Daardoor ontbreekt zicht op cruciale vragen: hoeveel extremistische content circuleert in de Nederlandse digitale ruimte, via welke kanalen, en welk bereik of invloed genereert deze content? Het gebrek aan data vormt daarmee een duidelijke blinde vlek in het beleidsterrein van digitale weerbaarheid, digitale deradicaliseringsstrategieën en cyber safety.

Blijvend obscuur: De rol van statelijke actoren in de verspreiding en het aanjagen van online extremisme. De rol van statelijke actoren in de verspreiding en aanwakkering van online extremisme blijft moeilijk te doorgronden. Dit komt ten dele doordat de werkelijke omvang van hybride aanvallen op het Westen (in de vorm van sabotage of beïnvloedingscampagnes) op zichzelf al ondoorgroendelijk is. Sommige deskundigen schatten in dat het gewone publiek slechts tien procent meekrijgt van wat er werkelijk gebeurt.¹⁰⁶ Zolang de digitale betrokkenheid van vijandige staten – met name Rusland – mistig blijft, kunnen groepen anders worden begrepen dan dat ze werkelijk zijn. Gelet op het soort interventies dat nodig is, maakt het wezenlijk uit of een groep opereert als proxy van een statelijke actor of niet. Zoals eerder toegelicht in hoofdstuk 5.3, zijn met name Russische sporen te vinden in recht-extremistische en NGE-netwerken. Zelfs wanneer de statelijke betrokkenheid sterk kan worden gerelativeerd, zijn banden tussen extremistische individuen of cellen 'in eigen huis' en Russische netwerken in het buitenland al zorgwekkend. De enorme waardering voor het totalitaire Rusland vloeit voort uit bredere gevoelens van vervreemding, complotgedachten en ultraconservatieve frustraties die we moeten begrijpen om ze te kunnen ontzenuwen. Aan de andere kant moeten we de Russische propagandamachines en ondergrondse netwerken structureel ontmaskeren en uitgraven om beïnvloedingsstrategieën te verstoren. De huidige ongrijpbaarheid van Russische routing, facilitering of beïnvloeding van extremistisch geweld frustreert effectieve bestrijding.

Onderzoek is overwegend gefocust op rechts-extremistische content. Dat onderzoek overwegend gericht is op rechts-extremistische content heeft meerdere redenen, die te maken hebben met empirische trends, maatschappelijke aandacht, en onderzoekstechnische obstakels. Zo resoneert rechts-extremistische content sterk met bredere zorgwekkende signalen over complotdenken, anti-migratieretoriek of anti-wokisme. Deze kruisverbanden verlenen studies naar online rechts-extremisme urgentie. Ook gebeurtenissen zoals de Capitool-bestorming (2021), de geplande Reichsbürgercoup in Duitsland en de rellen in en rondom Southport in het VK hebben de aandacht opgeëist. De focus is te begrijpen maar niet helemaal terecht met het oog op prevalentie. Uit de eerder gepresenteerde cijfers van Europol blijkt dat de groep jihadistische daders en arrestanten over 2024 een factor zes groter was dan die van rechts-extremisten. En ook het TCAP onderzoek door Tech Against Terrorism in het VK wijst uit dat de hoeveelheid en variëteit van terroristische online content vele malen groter is. Al met al lijkt er sprake te zijn van een zekere verslapping van de aandacht voor het (online) jihadisme, wat gezien de cijfers onterecht zou zijn.

Het online links-extremisme blijkt in de praktijk minder goed in beeld te krijgen. Naast de lage prevalentie in relatie tot jihadistische arrestaties en aanvallen, spelen hier mogelijk ook praktische en idealistische redenen. Links-extremistische netwerken leunen vermoedelijk minder zwaar op internetcultuur. Bovendien vallen social mediaplatforms onder de hoede van Big Techbedrijven die in het linkse denken juist veracht worden. Daarnaast speelt ook mee dat het imago van het links-extremisme 'aaihaarder' is. Waar rechts-extremisme wordt geassocieerd met de gewelddadige, racistische immoraliteit van het nazisme en suprematisme, identificeert het links-extremisme zich met activistische thema's die deels door het progressieve publiek gesteund worden. Ook de AIVD verklaart dat de risico's op links eerder (radicaal-)activistisch zijn dan extremistisch of terroristisch. De norm hierbij is dat de democratische rechtsorde niet bedreigd wordt, ook al is er sprake van maatschappelijke irritatie. Lage verwachtingen vertaalt zich misschien ook in een minder intensieve focus. Zo zijn er aanmerkelijk minder NGO's die links-extremistische netwerken onderzoeken.¹⁰⁷ Het zal van belang zijn om te blijven vaststellen of deze mindere aandacht in werkelijkheid niet tot een blinde vlek leidt.

¹⁰⁶ HCSS, *Chaos, Orde en Machtspolitiek: HCSS Strategische Monitor*, 2025.

¹⁰⁷ Onderzoeksinstituten zoals het Noorse Centre for Research on Extremism (C-REX), het Duitse Bundesamt für Verfassungsschutz (BfV) en het Britse International Centre for the Study of Radicalisation (ICSR) voeren wél actief onderzoek uit naar links-extremistische netwerken in Europa.

6.2. Naar meer politieke focus en wettelijke bewegingsruimte

Het politiek bewustzijn komt maar langzaam op gang. De politieke aandacht voor dit probleem is tot dusver fragmentarisch geweest en komt pas mondjesmaat op gang nu ook oudere generaties beginnen te beseffen dat de online en offline wereld onlosmakelijk met elkaar verbonden zijn. Waar men vroeger de digitale leefwereld zag als iets apart, toont bijvoorbeeld de recente hype rondom Netflix-serie *Adolescence* hoe de jongere generatie in één hybride realiteit leeft en onder grote online druk staat. Deze bewustwording onder beleidsmakers lijkt echter rijkelijk laat te komen en geschiedt schoksgewijs, terwijl de impact van online subculturen op het denken en handelen van jongeren al geruime tijd groeiende is. Ook de Amerikaanse politieke realiteit getuigt al jaren van een toenemende vervlechting van de online aangedreven alt-rightcultuur en de mainstream politiek. Dat deze dynamiek ten dele ook zou overslaan naar Europa was te voorzien geweest.

Pas recent klinken serieuzere waarschuwingen vanuit het veiligheidsdomein. Zo benadrukte de Nationaal Coördinator Terrorismebestrijding en Veiligheid dit jaar dat de razendsnelle online radicalisering van tieners grote zorgen baart en dat de aanpak van online radicalisering cruciaal is. Maar dit leidt nog niet tot systematische plannen. Terwijl op het gebied van kennis en wetgeving wel degelijk verandering nodig is. Zo dynamisch-adaptief als het online ecosysteem zich gedraagt, zo traag en ouderwets is het ambtelijk systeem en het wettelijk kader op basis waarvan geopereerd moet worden. Dit is niet alleen een kwestie van trage respons. Er zijn ook ingewikkelde dilemma's die zich aandienen tussen de morele plicht tot meer regulering en zicht op de digitale wereld enerzijds en het belang van rechts- en privacybescherming anderzijds. Brussel, maar ook Den Haag, lijken zich steeds vast te draaien op deze knelpunten.

Hostingbescherming op de schop? Een fundamenteel knelpunt in het zicht op online extremistische ecosystemen betreft de juridische bescherming van hostingdiensten, platformbeheerders en andere digitale infrastructuurleveranciers. Onder het huidige Europese kader, met name de E-Commerce Richtlijn (2000/31/EG), vallen deze partijen vaak onder de hostingvrijstelling. Dit houdt in dat zij niet aansprakelijk zijn voor door gebruikers geüploade content, tenzij zij expliciet op de hoogte zijn van de illegale aard ervan. Proactieve monitoring is niet verplicht, en veel partijen beroepen zich op hun rol als technische tussenpersoon. In de praktijk betekent dit dat extremistische fora, propagandasites en netwerken vaak langdurig gehost kunnen worden zonder interventie. De juridische verantwoordelijkheid wordt daarmee verschoven naar individuele gebruikers, terwijl de infrastructuur onaantastbaar blijft. Deze constructie belemmert opsporing en vroegsignalering. Terwijl bekend is dat er meerdere dubieuze hostingpartijen actief zijn die bijvoorbeeld ook worden gebruikt voor de verspreiding van desinformatie.¹⁰⁸ Zoals eerder beschreven zijn extremistische groepen, zoals die van IS-Khorasan, zich bovendien ook bewust van Nederland als een zeer privacyvriendelijk land dat het veiligst is om content te hosten. De wetgeving biedt dus niet alleen onvoldoende grip, maar wordt actief benut. Het is aan Brussel en Den Haag om op dit punt meer mogelijk te maken.

AVG-belemmeringen voor analyse van extremistische dreigingen. Naast het juridische vacuüm rondom hostingdiensten vormt ook de toepassing van de Algemene Verordening Gegevensbescherming (AVG, EU: GDPR) een belangrijke factor in de terughoudendheid bij het analyseren van online extremistische ecosystemen. De AVG beschermt (terecht) de verwerking van bijzondere persoonsgegevens en stelt hieraan strikte voorwaarden. Het is

¹⁰⁸ NRC, [Nederlands datacentrum is opnieuw de spil in een Russische beïnvloedingscampagne](#), 2024.

begrijpelijk dat instellingen als de Autoriteit Persoonsgegevens deze regels voorzichtig interpreteren: de bescherming vormt immers een fundamenteel uitgangspunt in de democratische rechtsstaat. Toch leidt deze voorzichtigheid ook tot structurele beperkingen in het zicht op online gedrag. Onderzoeksinstituten en maatschappelijke partners zijn terughoudend om instrumentatie te bouwen uit angst voor overtredingen bij het verwerken van bulkdata. Er lijkt veel juridische en praktische onzekerheid te bestaan over wat toelaatbaar is, zeker wanneer dergelijke analyses gericht zijn op automatisering.

De Europese Commissie waarschuwde in mei 2024 dat Nederland in de toepassing van de AVG mogelijk te rigide optreedt, waardoor legitieme maatschappelijke doelen, waaronder misdaadbestrijding en digitale veiligheid, in het gedrang kunnen komen.¹⁰⁹ Die waarschuwing onderstreept het spanningsveld waarin veiligheidsbeleid en fundamentele rechten zich bewegen: noodzakelijk, maar niet zonder frictie. Voor een effectievere aanpak van online extremisme is het daarom van belang dat er op Europees niveau helderheid komt over de ruimte die de AVG biedt voor proportionele analyse-initiatieven buiten de sfeer van inlichtingendiensten, mits gebonden aan zorgvuldige waarborgen.

Achterblijvende rol voor digitale signalering in de brede aanpak. De huidige 'brede aanpak' binnen de Nederlandse CTER-keten (Contra-Terrorisme, Extremisme en Radicalisering) kent belangrijke verdiensten, met name in de vorm van het casusoverleg waarbij actoren uit het brede domein van de veiligheidszorg samenwerken. Toch laat de praktijk zien dat signalen van online radicalisering weinig als primaire ingang fungeren voor het casusoverleg. Veel casussen komen pas in beeld doordat familie, docenten of wijkagenten gedragsverandering of zorgwekkende uitingen signaleren. In zulke gevallen komt de online component pas flankerend aan de orde. Dit is ook logisch: men moet eerst een gerechtelijk bevel verkrijgen voor infiltratie in persoonlijke kanalen en het verwerken van bijzondere persoonsgegevens.

Processen in de CTER-keten zijn bovendien nog vaak verzuild, dat wil zeggen ingedeeld naar ideologische kolommen van jihadisme, rechts- of links-extremisme. Dit is ook begrijpelijk vanuit de geschiedenis van terroristische zaken in Nederland die de CTER-aanpak sterk hebben geënt op ervaringen rondom de Hofstadgroep en IS-uitreizigers. Tegelijk sluit deze verzuiling mogelijk minder aan bij de hybride, eclectische realiteit van online radicaliseringsprocessen.

Hoewel gedragingen en motieven van geweldplegers niet eenvoudig toe te wijzen zijn aan online of offline paden, wijst het groeiende gewicht van de digitale omgeving op de noodzaak om strategieën te ontwikkelen die juist dáár beginnen met hun waarneming. In plaats van de online dimensie slechts als nadere toelichting te beschouwen zodra een casus al 'fysiek' zichtbaar is geworden, zouden casusoverleggen en signaleringskaders meer proactief moeten leren denken vanuit online indicatoren en de dynamiek van online ecosystemen. Dat vereist niet alleen betere OSINT-vaardigheden en digitale duiding binnen het casusoverleg, maar ook een fundamentele aanpassing in hoe extremisme in de keten wordt begrepen, gesignaleerd en geduid. Ook veronderstelt het zekere heroverwegingen in de bevoegdheidensystematiek binnen de CTER-keten.

Europese digitale soevereiniteit. De aanpak van online extremisme vergt structurele inspanningen om de verantwoordelijkheid van sociale mediaplatforms af te dwingen en Europese autonomie te versterken. Tot dusver blijft de medewerking van voornamelijk Amerikaanse platforms zoals X (voorheen Twitter), Meta, Telegram en Reddit wisselend. Er is sprake van

¹⁰⁹ NRC, [Brussel vindt Nederlandse privacywaakhond te strikt](#), 2020.

een in beginsel onwenselijk afhankelijkheid van de medewerking van bedrijven in het buitenland. Hoewel wetgeving als de Digital Services Act (DSA) en de Europese Richtlijn inzake het verwijderen van terroristische online-inhoud (TCO Regulation) een juridisch kader bieden worden de problemen van afhankelijkheid daar nog niet mee opgelost. De TCO-verordening verplicht aanbieders van hostingdiensten sinds juni 2022 om terroristische content binnen één uur na melding te verwijderen, maar wordt in praktijk nog beperkt toegepast. Meer Europees gecoördineerde druk op platformen kan wat effect sorteren. Maar de middelen om contentmoderatie af te dwingen in niet-Europese regimes is beperkt. Het speelt mee dat Europa al veel eerder zaken had moeten bereiken op het punt van digitale autonomie. Investeren in Europese, publieke of semi-publieke sociale platformen kan alsnog bijdragen aan digitale soevereiniteit en een betere inbedding van Europese rechtsnormen. Initiatieven daartoe bewegen zich echter zeer langzaam en zullen zeker niet waterdicht zijn, dan wel opgewassen tegen de hoge wendbaarheid van extremistische netwerken.

Leeftijdsverificatie? Binnen de EU wordt gewerkt aan een pan-Europese verificatie-app die leeftijdsgrenzen online op een privacyvriendelijke manier moet kunnen handhaven, zonder dat persoonsgegevens worden gedeeld met websites of overheden. In tegenstelling tot meer rigide vormen van online identiteitskaartcontrole, werkt dit systeem via een eenvoudige 'groen-rood'-signaalfunctie. Het is wellicht een bruikbare ontwikkeling voor het beschermen van mainstream gebruikers tegen ongepaste of schadelijke content, zonder grote inbreuk op privacy. Maar deze technologie is géén universele oplossing. Jongeren die al doelgericht op zoek zijn naar extremistische content weten zulke barrières eenvoudig te omzeilen via VPN's, alternatieve browsers of illegale platforms—zoals in het Verenigd Koninkrijk nu al zichtbaar is.¹¹⁰ Leeftijdsverificatie zal vooral de toegang beperken tot extremisme via reguliere kanalen, maar biedt nauwelijks bescherming tegen de ondergrondse, gesloten en reeds illegale infrastructuur waar veel extremistische ecosystemen zich vandaag al afspelen. Een toekomstgerichte aanpak van online extremisme vraagt uiteindelijk niet om een digitale muur, maar om het zorgvuldig inrichten van een sociaal en cultureel landschap waarin jongeren en hun omgeving de risico's leren zien. Weerbaarheid ontstaat niet primair door controle op content maar vooral met het bewustzijn over wat wel en niet verstandig is om je mee in te laten.

6.3. Naar een adaptieve preventie en aanpak

De aanpak van online extremisme moet aansluiten op de besproken trends en kenmerken: decentraal en hoog-adaptief, fluïde, post-organisatorisch en gericht op beïnvloeding van gevoel en identiteit van jongeren. Dit betekent dat klassieke repressieve modellen van opsporing en interventie tekort kunnen schieten. In plaats daarvan moet de respons adaptief zijn, gericht op vroege signalering en contextuele duiding. Dat vraagt om de vorming van interdisciplinaire interventieteams die kennis hebben van digitale subculturen, visuele propaganda en de psychologische mechanismen achter online radicalisering. Bovendien moet er sterk worden geïnvesteerd in preventie, met name onder jongeren. Mediawijsheid alleen volstaat niet: wat nodig is, is bewustzijn van de codes, rituelen en aantrekkingskracht van online haatmilieus—en handvatten om daar weerstand aan te bieden. Onderwijsinstellingen, jongerenwerk, jeugdzorg en hulpverlening dienen toegerust te worden om deze signalen vroegtijdig te herkennen en bespreekbaar te maken.

¹¹⁰ De Volkskrant, [Overheden zoeken naar nieuwe methoden voor leeftijdsverificatie online](#), 2025.

Digitale weerbaarheid begint aan de keukentafel. De sociale omgeving van jongeren, van vrienden en klasgenoten tot ouders en docenten, is vaak opmerkelijk slecht geïnformeerd over de digitale routes die kunnen leiden tot extremistische beïnvloeding. De extreme omgevingen waar zij in vertoeven, blijft dit voor hun directe omgeving meestal onzichtbaar. De gebruikte symboliek en codetaal zijn vaak zo contextspecifiek dat zij voor buitenstaanders nauwelijks te duiden zijn. Vooral ouders en opvoeders missen vaak het inzicht in deze digitale cultuur en weten daardoor niet waarop zij moeten letten. Hier ligt een belangrijke bewustwordingsopdracht, die niet alleen ligt bij de overheid maar ook bijvoorbeeld bij journalisten of andere ingewijden: het ontsluiten van deze fenomenen richting de 'offline omgeving'. Niet met alarmisme, maar met begrijpelijke duiding van hoe deze internetculturen werken, waarom ze jongeren aanspreken, en welke rol sociale onzekerheid of groepsdruk daarbij speelt. Cruciaal is ook dat het dagelijks internetgedrag dan thuis bespreekbaar wordt gemaakt, niet als controlemiddel, maar als ingang voor open gesprekken. Juist die dialoog aan de keukentafel kan een belangrijk verschil maken.

'Tegen-influencing' en het faciliteren van interne, ontzenuwende groepsdynamiek. Een effectieve, maar in beleidsland nog relatief onderbelichte strategie in het tegengaan van online radicalisering is het versterken van interne remmende dynamieken binnen extremistische subculturen.¹¹¹ Dit houdt in dat niet van buitenaf wordt gewaarschuwd of gecorrigeerd, maar dat kritiek, spot of twijfel ontstaat van binnenuit de bredere online biotoop. Een voorbeeld dat soms wordt aangedragen is het Reddit-forum IncelTears, waar gebruikers op satirische wijze uitingen uit de incelgemeenschap verzamelen, analyseren en bekritisieren. Omdat het gaat om een netwerk van ingevoerden ontstaat er een organisch contranarratief (tegen - in dit geval - incel-radicalisme). In kanalen kunnen bijvoorbeeld discussies ontstaan over hoe dom, grotesk of schadelijk opvattingen kunnen zijn, of over hoe moeilijk het kan zijn om verslavende, maar makkelijke geweldsnarratieven af te wijzen. De onderlinge digitale betrokkenheid zou kunnen helpen individuen te deradicaliseren of vermindert de algehele aantrekkingskracht van radicalere en gewelddadiger subculturen omdat deze minder statusverhogend werken. Spontane digitale contranarratieven kunnen daarnaast opgevat worden als een signaal van het zelfreinigende vermogen van de digitale cultuur (echter zonder dat daar nu volledig op vertrouwd kan worden als het gaat om deradicalisering).

Ten aanzien van diverse extremistische contexten zijn ook meer georganiseerde initiatieven ontstaan. Zo lanceerden jonge moslims wereldwijd de campagne #NotInMyName om zich openlijk af te zetten tegen jihadistische propaganda. Dit doorbrak het momentum van IS enigszins maar genereerde ook ruimte voor publieke distantie zonder loyaliteitsverlies. In de rechts-extremistische hoek zijn initiatieven zoals EXIT Deutschland¹¹² of het Zweeds Fryshuset voorbeelden van organisaties door spijtoptanten. Daarin treden voormalige neonaazi's naar voren om hun radicale verleden te verwerpen, wat vanwege het persoonlijk gedeelde ervaringsgezag kan doorwerken binnen de doelgroep. Structureel geldt dat contranarratieven het meest effectief lijken te zijn wanneer ze voortkomen uit stemmen met in-group-legitimititeit. Vanwege de noodzaak voor ervaringsgezag en authenticiteit is het lastig om deze culturen actief aan te jagen van overheidswege. Maar het belang ervan zou structureler kunnen worden opgenomen in beleid rond digitale weerbaarheid en extremismebestrijding. Beleid kan ook tot doel hebben om de voorwaarden te scheppen voor de groei en bloei van mildere digitale counter culture zonder daarin heel directief te zijn.

¹¹¹ Joel Busher e.a., *The internal brakes on violent escalation: a typology*, 2018.

¹¹² Zie website: [EXIT Deutschland](https://www.exitdeutschland.de/) - Ausstieg aus dem Rechtsextremismus.

Structureel investeren in OSINT-netwerken en -specialisten. De bestrijding van online extremisme vereist meer dan alleen technische monitoring: het vraagt om diep cultureel en digitaal begrip. Daarom is het noodzakelijk om structureel te investeren in OSINT-specialisten en daaraan verbonden netwerken, binnen én buiten de overheid. We herhalen dat Open Source Intelligence (OSINT) een sleutelrol speelt in het signaleren en analyseren van extremistische ecosystemen. Effectieve OSINT vraagt echter om meer dan alleen analytische capaciteit: het vereist aanpassing en begrip van de subcultuur. Succesvolle OSINT'ers zijn vaak vertrouwd met de codes, de taal en de inside jokes. Zonder deze contextkennis blijven veel signalen onder de radar of lopen het risico verkeerd te worden geïnterpreteerd. Dit punt vereist ook politieke urgentie en keuzes in personeelsbeleid. Veel diensten functioneren echter al met krappe bezettingen. Het risico is dat de noodzakelijke digitale voelsprietten structureel onderontwikkeld blijven. Overheden zouden daarom actiever OSINT-capaciteit moeten werven, ook extern (bijv. via academische instituten of gespecialiseerde NGO's), en gericht moeten investeren in opleiding, begeleiding en interdisciplinaire samenwerking.

Verstoren? In extremistische netwerken die opereren via online platformen is de klassieke opsporing – gericht op het identificeren en vervolgen van individuele daders – vaak ineffectief of traag, juist omdat deze netwerken geen hiërarchisch georganiseerde structuren kennen. De radicaliseringsdynamiek is organisch, versnipperd en decentraal. Het verzamelen van sluitend bewijs tegen één persoon is in dit diffuse krachtenveld moeizaam, temeer omdat veel communicatie plaatsvindt via tijdelijke accounts, anonieme fora of versleutelde berichten. Aansprakelijkheid is zo moeilijk te isoleren.

In plaats van zich uitsluitend te richten op individuele vervolging, kan daarom het strategisch verstoren van deze netwerken een effectievere aanpak vormen. Dit kan variëren van het onderbreken van de communicatie (zoals het offline halen van Discord-servers of Telegram-kanalen), het remmen van bereik, tot het ondermijnen van de groepscohesie door infiltratie, of het gericht onder druk zetten van sleutelfiguren. Door zo de samenhang en 'actiegerichtte bravoure' van het netwerk te ondermijnen, kunnen radicaliseringsprocessen worden onderbroken of vertraagd. Verstoring speelt zo in op een preventieve benadering van handhaving aangepast op de snelle dynamiek van online omgevingen. Dit onderstreept bovendien het eerste punt, dat systeemkennis minstens zo belangrijk is als opsporing.



The Hague Centre
for Strategic Studies

HCSS

Lange Voorhout 1
2514 EA The Hague

Follow us on social media:

@hcssnl

The Hague Centre for Strategic Studies

Email: info@hcss.nl
Website: www.hcss.nl