Radicale reclame op sociale media

Een onderzoek naar online rekrutering door en voor extremistische groepen

Charlie Stoeldraaijers, MSc
Dr. Elanie Rodermond
Dr. Fabienne Thijs
Prof. Dr. Rutger Leukfeldt
Prof. Dr. Frank Weerman

Juni 2024

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

Radicale reclame op sociale media

Een onderzoek naar online rekrutering door en voor extremistische groepen

Eindrapport

Projectnummer 3417
Juni 2024

Charlie Stoeldraaijers, MSc	Nederlands Studiecentrum Criminaliteit en Rechtshandhaving/Vrije Universiteit Amsterdam
Dr. Elanie Rodermond	Nederlands Studiecentrum Criminaliteit en Rechtshandhaving/Vrije Universiteit Amsterdam
Dr. Fabienne Thijs	Nederlands Studiecentrum Criminaliteit en Rechtshandhaving/Universiteit van Amsterdam
Prof. Dr. Rutger Leukfeldt	Nederlands Studiecentrum Criminaliteit en Rechtshandhaving/Universiteit Leiden/De Haagse Hogeschool
Prof. Dr. Frank Weerman	Nederlands Studiecentrum Criminaliteit en Rechtshandhaving/Erasmus Universiteit Rotterdam

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

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

Inhoud

Samenvatting

Achtergrond en onderzoeksvragen

In de afgelopen jaren is duidelijk geworden dat internet en sociale media een cruciale rol spelen in processen van radicalisering en rekrutering door en voor extremistische groepen. In de Nationale Contraterrorisme Strategie 2022-2026, het meest recente Dreigingsbeeld Terrorisme Nederland en het recente jaarverslag van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) wordt op verschillende manieren verwezen naar de rol van internet en sociale media. Zo wordt in het dreigingsbeeld benoemd dat de online wereld een belangrijke rol speelt in radicalisering, netwerkvorming en het aantrekken van jongeren met een al bestaande 'geweldslust en drang om te choqueren'. In de bespreking van een aantal verijdelde aanslagplots benoemt de AIVD daarnaast dat deze in sommige gevallen waren gepland door online gevormde groepen. Dergelijke ontwikkelingen onderstrepen het belang van op wetenschappelijke inzichten gestoelde preventie- en interventieprogramma's voor het tegengaan van online rekrutering (een 'evidence-based' aanpak). Hoewel er op basis van wetenschappelijk onderzoek al veel bekend is over mechanismen van online radicalisering, is het zicht op processen van online *rekrutering* nog beperkt.

Het huidige onderzoek beoogt in kaart te brengen hoe online rekrutering door en voor rechts-extremistische, jihadistische, anti-institutionele en links-extremistische groeperingen verloopt. Online rekrutering wordt hierbij gedefinieerd als "het proces waarbij een individu online wordt aangemoedigd om lid te worden van een groep, organisatie of beweging". We vertrekken vanuit theorieën die veronderstellen dat rekrutering bestaat uit verschillende fasen. Daarnaast gebruiken we theorieën die specifiek ingaan op hoe kenmerken van sociale media aansluiten bij de leefwereld van gebruikers en daarmee zowel gewenste als ongewenste ontwikkelingen kunnen faciliteren. Ter vergroting van de kennis over online rekrutering beantwoorden we de volgende overkoepelende onderzoeksvragen:

1) Wat is uit de literatuur en de praktijk bekend over de aard en mechanismen van online rekrutering door en voor extremistische groepen?

2) In hoeverre is er een wisselwerking tussen online rekrutering en offline gedrag?

3) Welke aanpakken en handelingsperspectieven zijn beschikbaar/geschikt voor instanties die zijn belast met de aanpak van extremisme?

Methode

Ter beantwoording van de onderzoeksvragen zijn verschillende onderzoeksmethoden gecombineerd. Allereerst is wetenschappelijke literatuur verzameld over online rekrutering door en voor extremistische groepen. Hiervoor zijn diverse databases geraadpleegd. Op basis van de literatuur is vervolgens een topiclijst opgesteld voor interviews met professionals die vanuit hun werkzaamheden (indirect) zicht hebben op deze thematiek en problematiek. In totaal is gesproken met veertien professionals, te weten drie medewerkers van de Nationale Politie, twee van de AIVD, twee van het

Landelijk Steunpunt Extremisme (LSE), twee van de Expertise-unit Sociale Stabiliteit (ESS), drie professionals werkzaam bij gemeenten en twee jongerenwerkers. Naderhand zijn de interviews systematisch gecodeerd en geanalyseerd met het programma ATLAS-ti.

Vervolgens is een kwalitatieve contentanalyse uitgevoerd van zeven openbare online groepen op Telegram en Facebook. Om een zo breed mogelijk beeld te krijgen hebben we ons hierbij op vier ideologische stromingen gericht, namelijk extreemrechts, extreemlinks, anti-institutioneel en jihadisme. De keuze voor specifieke online groepen is gebaseerd op recente Dreigingsbeelden Terrorisme Nederland (DTN's) van de NCTV, jaarverslagen van de AIVD en mediaberichtgeving over specifieke groepen. Voor de analyse zijn gedurende een bepaalde periode berichten verzameld die in de groepen werden geplaatst. Vervolgens zijn de berichten gecodeerd en geanalyseerd met het programma ATLAS.ti. Ook beeldmateriaal en videofragmenten zijn geanalyseerd. Tot slot is een expertmeeting met professionals en wetenschappers georganiseerd om de voorlopige onderzoeksresultaten te bespreken en de aanbevelingen aan te scherpen.

Resultaten

Het online domein als een unieke omgeving

Uit de resultaten blijkt allereerst dat het online domein verschillende kenmerken heeft die kunnen bijdragen aan het proces van online rekrutering. Professionals gaven aan dat het online domein 'easy in – easy out' is; de drempel om toe te treden tot een extremistische groep en ook weer uit een groep te stappen ligt online veel lager dan offline. Dit lijkt vooral voort te komen uit een beperktere (tijds)investering die gepaard gaat met online toetreding en de anonimiteit van internet. Dit laatste maakt dat iemand kan toetreden tot een extremistische groep zonder dat iemands offline sociale netwerk daarvan op de hoogte is en dat iemand zich in de online wereld vrijer voelt om gedrag te vertonen dat in de offline wereld minder geaccepteerd is. Daarnaast werd meermaals benadrukt dat het online domein letterlijk over grenzen gaat, waardoor fysieke nabijheid geen vereiste meer is om te rekruteren of gerekruteerd te worden. Tot slot werd benoemd dat het online domein een vertekend, positiever beeld kan geven van de groepscohesie, -grootte en reikwijdte van een groepering, waardoor potentiële rekruten zich eerder aangetrokken kunnen voelen tot een bepaalde groep.

Uit de analyse blijkt dat extremistische groepen gebruik maken van een grote diversiteit aan platforms, waaronder *mainstream* sociale mediaplatforms zoals Facebook en YouTube en *low profile* platforms zoals Telegram. Daarnaast worden ook gaming platforms zoals Roblox gebruikt, al is het zicht hierop tot op heden beperkt. Telegram is volgens de professionals op dit moment het meest gebruikte platform onder extremistische groepen. Als reden werd genoemd dat dit platform meer anonimiteit biedt en minder actief is op het gebied van content-moderatie. Mainstream platforms zijn echter ook nog steeds belangrijk; niet alleen worden ze veelvuldig gebruikt om de ideologie van de groep te verspreiden, ook fungeren ze regelmatig als doorgeefluik naar *low profile* platforms.

Online rekrutering: generiek en specifiek

Bij het in kaart brengen van daadwerkelijke processen van online rekrutering bleek al snel de noodzaak om te onderscheiden naar twee varianten van online rekrutering, namelijk 'generieke rekrutering' en 'specifieke rekrutering'. Bij generieke rekrutering is sprake van een op een breed publiek gericht

rekruteringsproces, waar groepsvorming (‘community building’) een belangrijk onderdeel van uitmaakt. Via deze groepsvorming wordt geprobeerd bezoekers in het algemeen aan de groep te verbinden. Bij specifieke rekrutering is daarentegen sprake van op specifieke subpopulaties gerichte rekrutering. Hoewel deze twee varianten in sommige gevallen in elkaar overgaan, worden ze ook afzonderlijk ingezet.

Voor wat betreft generieke rekrutering blijkt dat extremistische groepen aan online groepsvorming doen door het creëren van sociale cohesie en gedeelde ideologische narratieven. Gemeenschappelijke doelen worden aan de hand van extremistische memes (humoristische afbeeldingen, video’s of tekstfragmenten die online worden gedeeld) en ideologische berichten verspreid. Opvallend is dat de groepsvorming zich niet beperkt tot het online domein. Alle door ons onderzochte online groepen maken melding van offline groepsactiviteiten, variërend van het geven en bijwonen van lezingen tot gezamenlijk sporten en het organiseren en bijwonen van protesten. Gedurende de onderzoeksperiode werden diverse berichten geplaatst waarin bezoekers concreet werden uitgenodigd om lid te worden van de groep.

Specifieke rekrutering richt zich op bepaalde subpopulaties zoals vrouwen, minderjarigen of technisch geschoolde individuen. Uit de wetenschappelijke literatuur blijkt dat deze doelgerichte rekrutering, ook wel ‘narrowcasting’ genoemd, met name veelvuldig is ingezet door grote terroristische organisaties zoals Al Qaida en Islamitische Staat (IS). Voorbeelden zijn de grootschalige mobilisatie van uitreizigers door IS, alsmede de rekrutering van technische studenten en werknemers door Al Qaida. Uit de resultaten van het huidige onderzoek komt echter naar voren dat dergelijke specifieke rekrutering op dit moment binnen de Nederlandse context weinig voor lijkt te komen. Volgens de geïnterviewde professionals komen de meeste personen in aanraking met een extremistische groep doordat ze zelfstanding online op zoek gaan naar gelijkgestemden en lid worden van een openbare online groep. In een trapsgewijs proces dat daarop volgt, kunnen geïnteresseerden dieper in de groepering binnenkomen door uitgenodigd te worden voor besloten groepen en doorlichtingsprocedures te doorlopen. Dergelijke procedures bestaan uit onder meer de beantwoording van kennisvragen over de groep of ideologie en het uitvragen van de bereidheid om offline samen te komen of bij te dragen aan de groepsdoelen.

Een belangrijke constatering is dat er meer overeenkomsten dan verschillen lijken te bestaan tussen het gebruik van sociale media door de onderzochte groeperingen. Zo is in alle groeperingen sprake van online groepsvorming en worden de verschillende andere gebruiksmogelijkheden van het online domein actief gebruikt, onder meer via het delen van extremistische content, memes en het verspreiden van de ideologie. Daarnaast organiseren alle groepen offline activiteiten, al varieert de aard van deze activiteiten tussen de groepen. Lezingen en presentaties lijken de meest voorkomende activiteiten te zijn onder de anti-institutionele, jihadistische en extreemlinkse groepen. De extreemrechtse en jihadistische groepen berichten daarnaast ook, in tegenstelling tot de twee andere stromingen, over gezamenlijk trainen en vechtsporten. Oproepen tot lidmaatschap komen met name voor in extreemrechtse en anti-institutionele groepen. Doorlichtingsprocedures worden vooral ingezet door extreemrechtse, jihadistische en anti-institutionele groepen.

De wisselwerking tussen online en offline leefwerelden

De interactie tussen de online en offline wereld is onderwerp van interesse binnen zowel de wetenschap als overheidsinstanties. Uit het onderzoek komt naar voren dat er op minstens drie manieren naar de relatie tussen online rekrutering en de offline wereld kan worden gekeken. Ten eerste kan iemands offline situatie, bijvoorbeeld een moeilijke thuissituatie, zijn of haar vatbaarheid voor online rekrutering vergroten, waar vooral sprake van zou zijn onder jongeren. Hoewel dergelijke kwetsbaarheden niet direct leiden tot lidmaatschap, kunnen ze wel als een risicofactor worden beschouwd.

Ten tweede kan online rekrutering overgaan in 'onlife' rekrutering, waarbij sprake is van een continue wisselwerking tussen online en offline processen. Online worden bijvoorbeeld offline bijeenkomsten aangekondigd, waar vervolgens weer online verslag van wordt gedaan, vaak tezamen met oproepen aan lezers om zich aan te sluiten bij de groep. Ondanks de toenemende aandacht voor het online domein merken respondenten dat het offline domein recentelijk weer een prominentere rol krijgt, vooral in latere rekruteringsfasen. Dit zou te wijten zijn aan een toegenomen veiligheidsbewustzijn van extremistische groepen en de realisatie dat opsporingsinstanties kunnen meelezen, wat leidt tot een kritischer toelatingsbeleid en een herwaardering van fysiek contact.

De derde relatie tussen online rekrutering en de offline wereld betreft het overgaan tot daadwerkelijke offline (gewelddadige) extremistische acties. Uit zowel de literatuur als interviews blijkt dat deze relatie ingewikkeld vast te stellen is. Uitzonderingen zijn de rekruteringsstrategieën van Al Qaida en IS, waarbij online rekrutering een duidelijke opmaat was naar offline terroristische acties. Vaak is de relatie echter veel complexer.

Bestaande aanpakken en handelingsperspectieven

Met de toenemende aandacht voor processen van online rekrutering hebben ook maatregelen ter preventie daarvan zich in de laatste jaren snel ontwikkeld. Op basis van de wetenschappelijke literatuur is in het huidige onderzoek met name ingezoomd op maatregelen gericht op weerbaarheid, online tegengeluiden en regulering en moderatie.

Preventieve online weerbaarheidsprogramma's in binnen- en buitenland zijn vooral op jongeren gericht, waarbij wordt geprobeerd om hen te informeren over gewelddadig extremisme, hen bewust te maken van 'grooming' gedrag en hun mediageletterdheid te verhogen. Een belangrijk overkoepelend doel is de ontwikkeling van vaardigheden om berichtgeving kritisch te beoordelen, bronnen te evalueren en betrouwbare informatie van desinformatie te onderscheiden. Hoewel veel online weerbaarheidsprogramma's nog niet zijn geëvalueerd, onderschrijven verschillende respondenten het belang van aanpakken gericht op weerbaarheid en roepen zij op tot verdere doorontwikkeling en praktische handvatten. Daarbij werd meermaals de rol van ouders aangestipt, die een cruciale rol zouden spelen in de digitale opvoeding en het bevorderen van online weerbaarheid. Respondenten benoemden dat de huidige generatie ouders daarin ook ondersteund moet worden, gelet op de snelle ontwikkelingen in het online domein.

De inzet van de tweede aanpak, online tegengeluiden, wordt uitgevoerd door zowel overheden als het maatschappelijk middenveld. Deze initiatieven richten zich doorgaans niet specifiek op het voorkomen van online rekrutering, maar op diverse gerelateerde processen, waaronder online radicalisering en de

verspreiding van nepnieuws. Het literatuuronderzoek en de interviews tonen aan dat het onduidelijk is welk effect online tegengeluiden hebben. Ook is weinig bekend over onbedoelde neveneffecten of zelfs tegengestelde effecten, zoals versterking van extremistische standpunten. Hieruit volgt dat er ook nog maar weinig inzicht is in eventuele werkzame elementen van online tegengeluiden.

De derde aanpak, het modereren en reguleren van online materiaal, gebeurt op verschillende niveaus door internationale organen (EU, Europol), nationale overheden, private partijen (sociale mediabedrijven, internetproviders) en maatschappelijke organisaties en individuen die in staat zijn om illegale online content te identificeren en daarvan melding te maken (ook wel 'trusted flaggers' genoemd). Sinds de invoering van de Digital Services Act (DSA) worden private partijen binnen de EU gedwongen op te treden tegen illegale content, al zijn grote sociale mediabedrijven zoals Meta al een aantal jaren bezig met het modereren en reguleren van online materiaal. Dit heeft als gevolg dat expliciet beeld- en instructiemateriaal steeds meer lijkt te verplaatsen naar besloten groepen op *low profile* platforms als Telegram, zo blijkt uit de literatuur en interviewresultaten. Nieuwe technologische ontwikkelingen, zoals technieken voor beeldherkenning en kunstmatige intelligentie, kunnen bijdragen aan het steeds beter opsporen en modereren van extremistische uitingen in het online domein.

Op basis van de interviews zijn tot slot nog enkele andere obstakels en uitdagingen geïdentificeerd die de (optimale) implementatie van de verschillende aanpakken in de weg staan. Ten eerste werd benoemd dat online platforms eigendom zijn van particuliere bedrijven die vallen onder andere jurisdicties dan waar hun gebruikers zich bevinden. Ten tweede werd gewezen op de enorme hoeveelheid extremistisch en terroristisch materiaal en de onmogelijkheid om al dit materiaal te modereren dan wel te verwijderen. Extra complex wordt het als het gaat om zogeheten borderline content, ook wel 'legal yet harmful' content genoemd. Deze content laat zich niet gemakkelijk modereren maar speelt een cruciale rol in het radicaliseren en rekruteren van nieuwe leden. Hieraan gerelateerd werd ten derde gewezen op een capaciteitsgebrek binnen zowel de rechtshandhaving als bij andere organisaties die zich bezighouden met het voorkomen van radicalisering, extremisme en terrorisme. Ten vierde is er een behoefte aan meer inhoudelijke expertise en duidelijke richtlijnen over de bevoegdheden van verschillende professionals en organisaties, onder meer ten aanzien van het delen van informatie. Ten vijfde blijkt meer algemeen een gebrek aan inzicht over de algehele effectiviteit van bestaande aanpakken en de eventuele werkzame elementen daarbinnen.

Conclusie en aanbevelingen

Op basis van de onderzoeksresultaten en hierboven geïdentificeerde knelpunten zijn verschillende aanbevelingen voor vervolgonderzoek en voor beleid en de praktijk gedaan. Alvorens deze te benoemen is het belangrijk om de beperkingen van het huidige onderzoek is kaart te brengen. Ten eerste is per instantie slechts met een beperkt aantal medewerkers gesproken. Ten tweede is de contentanalyse van beperkte omvang, zowel wat betreft de tijdsperiode als het aantal geanalyseerde berichten. Ten derde hebben we niet gesproken met mensen die zelf zijn gerekruteerd dan wel anderen hebben gerekruteerd. Desalniettemin leveren de onderzoeksresultaten verschillende overkoepelende inzichten op die leiden tot de onderstaande aanbevelingen. We bespreken eerst de aanbevelingen voor vervolgonderzoek. Daarna volgen de aanbevelingen voor beleid en de praktijk.

Met betrekking tot vervolgonderzoek verdient het allereerst aanbeveling om de in dit onderzoek gebruikte methode van contentanalyse uit te breiden. De verwachting is dat onderzoek met een

langere analyseperiode en de inclusie van meer berichten leidt tot aanvullende inzichten, onder meer ten aanzien van de verschillende rollen die online gebruikers vervullen, interactiepatronen en netwerkvorming. Het is belangrijk dat in dit vervolgonderzoek nadrukkelijk wordt ingezoomd op gaming platforms, zeker gelet op de populariteit van interactieve games en het tot op heden gebrekkige zicht op rekruteringsprocessen via dergelijke platforms. Daarnaast dient vervolgonderzoek de ervaringen van mensen die zelf zijn of hebben gerekruteerd mee te nemen. Op basis van deze ervaringen kan meer zicht ontstaan op de volgordelijkheid van rekruteringsprocessen, de werkwijze van rekruteurs en waar de aantrekkingskracht van online groepen precies zit. Dergelijk onderzoek kan ook worden gebruikt om een beter beeld te krijgen van de relatie tussen online rekrutering, online mobilisatie en offline acties, iets waar tot op heden nog maar weinig over bekend is.

Ten aanzien van de aanpak van online rekrutering werd vastgesteld dat er zeer beperkt zicht is op de effectiviteit van bestaande programma's en de werkzame elementen daarvan. Evaluatieonderzoek is nodig om de effectiviteit van de programma's in kaart te brengen. Specifiek voor de aanpakken gericht op weerbaarheid geldt dat het belangrijk is om de werkzame elementen van die aanpakken te onderzoeken. Daarbij ligt het voor de hand om te vertrekken vanuit de inmiddels rijke wetenschappelijke literatuur over weerbaarheid in andere contexten. Tot slot zou vervolgonderzoek de mogelijkheden die overheidsinstanties en tech-bedrijven hebben om online content te modereren en platforms te reguleren in kaart moeten brengen, alsmede hoe dergelijke instanties en bedrijven in de praktijk gebruik maken van deze mogelijkheden, hoe ze de DSA implementeren en wat de effecten van deze aanpak zijn. Daarbij dient niet alleen te worden gekeken naar duidelijk illegale content maar ook naar de eerder besproken borderline content.

Met betrekking tot beleid en de praktijk komen wij tot de volgende aanbevelingen. Allereerst wordt aanbevolen om evidence-based programma's ter vergroting van de online weerbaarheid verder te ontwikkelen. Hier dienen professionals vanuit verschillende instanties buiten het strafrechtelijk domein, variërend van jongerenwerkers tot leerkrachten, nadrukkelijk(er) bij te worden betrokken. Het regelmatig betrekken van jongeren bij de (door)ontwikkeling van programma's wordt daarbij belangrijk geacht om een beter beeld te krijgen van waar jongeren online mee in aanraking komen. Belangrijk om te benoemen is dat de programma's niet alleen op de jongeren moeten worden gericht, maar ook op hun ouders en verzorgers. Zij hebben zoals blijkt uit het huidige en eerder onderzoek een cruciale rol als het gaat om 'digitale opvoeding'. Tegelijkertijd heeft de huidige generatie ouders ook niet altijd de juiste kennis en vaardigheden om die digitale opvoeding adequaat vorm te geven. De laatste jaren zijn diverse initiatieven ontwikkeld om ouders hierin te ondersteunen en tips te geven en dit is een goede ontwikkeling. Dergelijke initiatieven zouden wel nog actiever naar ouders kunnen worden gecommuniceerd. Het is belangrijk om dit soort initiatieven breed uit te rollen binnen verschillende gemeentelijke instanties, zodat de belasting niet bij één enkele instantie ligt (tot nu toe zijn dit vaak de scholen) en de initiatieven een groter bereik hebben. Gelet op de genoemde kwetsbaarheden verdient het ook aanbeveling om de focus op online weerbaarheid te combineren met al bestaande programma's ter vergroting van de weerbaarheid in de offline wereld. In het huidige onderzoek is geconstateerd dat processen van (online) rekrutering door en voor extremistische groepen op een aantal punten overeenkomen met processen van rekrutering voor de georganiseerde misdaad en cybercriminele netwerken. Het lijkt daarom zinvol om na te gaan welke op weerbaarheid gerichte elementen uit programma's ter voorkoming van onder meer rekrutering van jongeren voor de georganiseerde misdaad bruikbaar zijn voor het voorkomen van online rekrutering voor extremistische groepen.

Ten tweede is het belangrijk om in te zetten op verdere professionalisering rond het voorkomen van online rekrutering. Uit het onderzoek is gebleken dat onder professionals behoefte bestaat aan meer duidelijkheid over waar professionals in verschillende functies, variërend van voetbaltrainers tot leerkrachten, terecht kunnen in geval van zorgen over problematisch online gedrag. In trainingen, die volgens professionals een structureler karakter zouden moeten hebben, zou aandacht kunnen worden besteed aan de signalen van rekrutering en kennis over de eigen bevoegdheden. Het werken met de 'Richtlijn Radicalisering' zou hier onderdeel vanuit kunnen maken. Deze richtlijn wordt momenteel vanuit het Meerjarenplan Richtlijnen Jeugd ontwikkeld en beoogt jeugdprofessionals vanaf het najaar van 2024 handvatten te bieden voor het signaleren en aanpakken van radicalisering onder jeugdigen.

Hieraan gerelateerd verdient het aanbeveling dat de samenwerking tussen instanties wordt geïntensiveerd, waarbij met name expertise rond offline radicalisering en rekrutering wordt gecombineerd met expertise rond online processen. Kennis over online processen is cruciaal wanneer in de offline wereld individuele casussen worden gewogen. Dat vraagt om de toevoeging van professionals met deze kennis binnen de persoonsgerichte aanpak (PGA) in de verschillende gemeenten. Meer in algemene zin wordt aangeraden om de kennis over het online domein sterk te vergroten binnen de lokale overheid.

Naast aanbevelingen die zijn gericht op de aanpak ter voorkoming dat individuen online worden gerekruteerd, volgen uit de resultaten ook aanbevelingen met betrekking tot het online domein zelf. Met betrekking tot illegale extremistische content wordt geadviseerd om in samenwerking met tech-bedrijven verbeteringen te blijven doorvoeren met betrekking tot het detecteren van online extremistisch materiaal. Een concrete aanbeveling die ook uit de literatuur volgt is het bouwen van een database waarin 'rekruteringstaal' wordt bijgehouden. Om dit laatste mogelijk te maken, is het belangrijk dat opsporingsinstanties voortdurend samenwerken met professionals met inhoudelijke en vooral actuele expertise op het gebied van online communicatie door extremistische groepen. Gelet op het snel veranderende werkveld is deze samenwerking tussen beleid, de praktijk en de wetenschap ook in bredere zin belangrijk, zeker gelet op de hierboven besproken aanbevelingen voor vervolgonderzoek. Met name het onderzoek naar hoe de DSA wordt geïmplementeerd, welke knelpunten spelen en wat de effecten zijn heeft een sterk toegepast karakter met directe relevantie voor de praktijk.

Het huidige onderzoek en recente andere studies onderstrepen daarnaast het belang van een concretere aanpak van borderline content. Gelet op het spanningsveld tussen het modereren van legal yet harmful content enerzijds en het waarborgen van fundamentele rechten en vrijheden anderzijds wordt aanbevolen om een 'taskforce borderline content' op te richten. Binnen deze taskforce zouden professionals vanuit de praktijk en beleid en de tech-sector plaats moeten nemen, alsmede een breed pallet aan wetenschappers inclusief extremisme-experts, juristen en ethici. Gezamenlijk zouden de professionals zich moeten buigen over de vraag hoe de onwenselijke gevolgen van borderline content kunnen worden tegengaan met inachtneming van belangrijke rechten en vrijheden. Een antwoord op die vraag is broodnodig, zeker nu uit het huidige onderzoek blijkt dat het rekruteringsproces doorgaans aanvangt op openbare platforms waar niet zozeer illegale content maar veel vaker borderline content bijdraagt aan de aantrekkingskracht van, en daarop volgende toetreding tot, extremistische groepen.

1. Inleiding

1.1 Aanleiding en doelstelling

[naam verdachte] maakt deel uit van de rechts-extremistische groepering Assault Division. Via Telegram verspreidt Assault Division berichten waarin wordt aangezet tot rassenhaat en antisemitisme en berichten waarin geweldplegers worden verheerlijkt. Ook verspreidt Assault Division online informatie over vuurwapens, survival skills en guerrilla tactieken. [naam verdachte] heeft admin-rechten binnen de Telegram-groep Assault Division en binnen het openbare Telegram-kanaal Assault Division. [naam verdachte] maakt ook deel uit van The Base, een internationaal netwerk van rechts-extremisten. The Base ziet zichzelf als het fundament van een verzetsgroep tegen een door Joden gedomineerd politiek systeem. The Base verspreidt online informatie over survivaltechnieken en zelfverdediging en organiseert trainingen en ontmoetingen. The Base propageert op zijn openbare Telegram-kanaal het bezit van vuurwapens en dreigt met vuurwapengeweld. (Rechtbank Rotterdam, 10/960131-20, ECLI:NL:RBROT:2021:11857)

In de Nationale Contraterrorisme Strategie 2022-2026 wordt benoemd dat “de rol die internet en sociale media spelen bij radicalisering en terroristische voorbereiding niet genoeg kan worden benadrukt” (p. 15). De bovenstaande casus is één van de voorbeelden die dit lijkt te bevestigen. In deze casus werd de verdachte vervolgd voor voorbereidings- en/of bevorderingshandelingen voor het plegen van een (moord)aanslag op toenmalig premier Rutte, het geven van een terroristische training en deelname aan de extremistische organisatie The Base en opruiing. De casus illustreert de rol van internet bij het verspreiden van in dit geval rechtsextremistisch gedachtegoed en het samenbrengen van aanhangers van dat gedachtegoed. Deze belangrijk rol is de laatste jaren meermaals duidelijk geworden en niet alleen in Nederland. Uit onderzoek naar de door Brendon Tarrant gepleegde rechts-extremistische aanslag in Christchurch (Nieuw-Zeeland) blijkt dat internet belangrijk was in de aanloop naar de aanslag en met name cruciaal was voor het verstevigen van zijn ‘belief-system’ (Williamson, 2020). Voorafgaand aan de Capitoolbestorming in 2021 werd veelvuldig online gecommuniceerd over deze gebeurtenis. In Nederland leidde grootschalige online communicatie ertoe dat ‘corona-protesten’ middels een serie van gewelddadigheden uitgroeiden tot ‘corona-rellen’ (Van den Berg, 2021). Het tonen van antisemitische leuzen op de Erasmusbrug tijdens de jaarwisseling werd online voorbereid en naderhand door aanhangers van de rechtsextremistische White Lives Matters-Telegram groep online geprezen. Op datzelfde platform werd opgeroepen tot nieuwe acties (Groenendijk, 2023).

Dergelijke gebeurtenissen maken dat het online domein al langere tijd de aandacht heeft van organisaties die zich met orde en veiligheid bezighouden. In het laatste Dreigingsbeeld Terrorisme Nederland (DTN60; NCTV, 2024) wordt benoemd dat de online wereld een belangrijke rol speelt in onder meer radicaliseringsprocessen en netwerkvorming. Met betrekking tot het jihadisme wordt benoemd dat soms zeer jonge personen online radicaliseren ‘buiten de gekende jihadistische netwerken om’. Daarnaast wordt in het rapport melding gemaakt van jongeren die ‘vanuit geweldslust en de drang naar choqueren uitkomen bij rechts-terroristische chatgroepen en platforms’ en wordt gewezen op het soms grote online bereik van rechts-extremistische groepen. Een AIVD-rapport over anti-institutioneel extremisme wijst op de invloed van het online domein op de ‘vermenging van verschillende protesten’, en hoe mensen elkaar ‘snel en laagdrempelig online vinden’ (AIVD, 2023).

Deze inzichten passen in het bredere beeld van de toenemende invloed van het online domein op verschillende vormen van ongewenst gedrag en in de uiterste vorm op (ernstige) vormen van criminaliteit. In een tijd waarin in Nederland bijna elke inwoner tussen de 12 en 45 jaar gebruik maakt van sociale media (Centraal Bureau voor de Statistiek, 2023), wordt de online omgeving ook steeds vaker aangewend voor diverse criminele doeleinden (Bekkers, Moneva, & Leukfeldt, 2022; Weerman, 2019). Zo is al langer bekend dat internet, meer specifiek sociale media, een belangrijke rol spelen bij het rekruteren van (vaak jonge) individuen bij vormen van georganiseerde misdaad en drugscriminaliteit. Recent onderzoek toont bijvoorbeeld aan dat sociale media veelvuldig worden ingezet om 'geldezels' te rekruteren (Bekkers et al., 2022), of uithalers van ladingen cocaïne in de haven van Rotterdam (Staring et al., 2023). Daarbij worden diverse beloftes gedaan aan de gerekruteerde individuen en zijn de 'targets' veelal kwetsbare jongeren. 'Traditionele' criminele groepen maken niet alleen volop gebruik van de mogelijkheden van de online wereld om nieuwe leden te rekruteren, maar ook om facilitators in te schakelen of om delicten beter uit te kunnen voeren (zie bijvoorbeeld Leukfeldt et al., 2019; Leukfeldt & Roks, 2020; Roks et al., 2020).

Er zijn veel aanwijzingen dat soortgelijke processen ook een rol spelen binnen de context van extremistische organisaties en -bewegingen. Onderzoek toont aan dat online activiteiten van invloed kunnen zijn op radicaliseringsprocessen (Hassan et al., 2018; Herath & Whittaker, 2021; Mølmen & Ravndal, 2021), op het rekruteren voor en deelnemen aan extremistische organisaties (Johnston et al., 2020) en dat online processen de kans op offline activistische en/of extremistische acties kunnen vergroten (Hassan et al., 2018; Whittaker, 2022). Tegelijkertijd is de kennis hierover gefragmenteerd en ontbreekt een overzicht van de relevante wetenschappelijke en praktijkkennis. Dit geldt met name voor de kennis over online rekrutering. Dit heeft tot gevolg dat er tot op heden slechts een beperkte *evidence-base* is waarop maatregelen ter preventie van online rekrutering kunnen worden gebaseerd. Een complicerende factor in dit verband is dat de terminologie en operationalisatie in diverse onderzoeken door elkaar lopen. Waar sommige studies kijken naar de invloed van sociale media op radicalisering van ideeën, kijken andere studies heel specifiek naar manieren waarop terroristische organisaties leden rekruteren voor de organisatie, of waarop individuele extremisten andere internetgebruikers mobiliseren voor acties in de offline wereld. Het is belangrijk om oog te hebben voor deze verschillende activiteiten, de kenmerken van platforms waarop ze plaatsvinden en de uitwerking op daadwerkelijk gedrag in de offline wereld. Kennis rondom deze aspecten kan bijdragen aan de ontwikkeling van passende maatregelen om de verschillende gebeurtenissen te voorkomen.

1.2 Onderzoeksvragen

Uit bovenstaande blijkt dat de wetenschappelijke kennis over online processen die de kans op betrokkenheid bij extremisme dan wel extremistische groepen vergroten gefragmenteerd is. Daarnaast is veel relevant onderzoek uitgevoerd in de Verenigde Staten. Hoewel online extremisme niet aan landsgrenzen is gebonden, is aannemelijk dat bepaalde processen toch voor een deel contextafhankelijk zijn. Tevens verschilt de aanpak van online extremisme in verschillende landen. Het huidige onderzoek beoogt daarom om een breed overzicht te bieden van de bestaande kennis over rekrutering door en voor extremistische groepen en daarnaast specifiek in te zoomen op de situatie in Nederland.

Om dit te bewerkstelligen worden verschillende onderzoeksmethoden gebruikt, te weten een literatuuronderzoek, een kwalitatieve content-analyse van sociale media platforms, interviews en een expertmeeting. Hierbij zijn de volgende onderzoeksvragen geformuleerd, verdeeld over drie thema's:

Aard en mechanismen van online rekrutering

1) Wat is uit de literatuur en de praktijk bekend over de aard en mechanismen van online rekrutering?
   a. Welke rol speelt het online domein in de rekrutering en aansluiting bij extremistische organisaties en groeperingen?
   b. In hoeverre zijn er voor vraag a verschillen en overeenkomsten waarneembaar tussen verschillende extremistische groeperingen vanuit specifiek het rechts-extremisme, anti-institutioneel extremisme, jihadisme en links-extremisme?
   c. Welke kenmerken van de verschillende online platforms vergroten de kans dat ze succesvol kunnen worden aangewend voor online rekrutering?

Interactie tussen online en offline gedrag

2) In hoeverre is er een wisselwerking tussen online rekrutering en offline gedrag?
   a. Wat is er bekend over de aard en omvang van offline extremistische acties die hun oorsprong online vinden?
   b. Wat is bekend over de volgordelijkheid van online en offline extremisme en de verschillen tussen mensen die online gerekruteerd zijn dan wel zelf online aansluiting hebben gezocht bij een extremistisch netwerk?
   c. Wat is er bekend over de rekruterings-modus operandi van extremistische netwerken die zowel online als offline actief zijn?
   d. In hoeverre zijn er voor vraag a t/m c verschillen en overeenkomsten waarneembaar tussen verschillende extremistische groeperingen vanuit rechts-extremisme, anti-institutioneel extremisme, jihadisme en links-extremisme?

Handelingsperspectieven en mogelijke aanpakken

3) Welke aanpakken en handelingsperspectieven zijn beschikbaar/geschikt voor instanties die zijn belast met de aanpak van extremisme?
   a. Wat is bekend over de mogelijkheden en effecten van maatregelen om online rekrutering tegen te gaan, of het gebruik van bepaalde sites of online platforms te reguleren? Bijvoorbeeld door de internetsector of de overheid?
   b. Wat is bekend over mogelijkheden en effecten van aanpakken gericht op de weerbaarheid van personen tegen online rekrutering? Via voorlichting aan jongeren en ouders, of via preventie op scholen en via jongerenwerk?
   c. Wat is bekend over de mogelijkheden en effecten van aanpakken waarbij online tegengeluiden worden aangeboden, al dan niet gericht op bepaalde groepen? Bijvoorbeeld door de overheid of door maatschappelijke partijen?
   d. Welke verdere aanbevelingen voor handelingsperspectieven en mogelijke aanpakken zijn af te leiden uit de wetenschappelijk inzichten met betrekking tot de bovengenoemde vragen?

2. Wetenschappelijk kader

Dit hoofdstuk biedt een overzicht van wetenschappelijke literatuur over online rekrutering en gerelateerde concepten. Allereerst wordt in paragraaf 2.1 ingegaan op het concept radicalisering. Daarbij wordt literatuur over risico- en beschermende factoren besproken, evenals verschillende fasen van radicalisering en verschillen in radicaliseringsprocessen tussen extremistische stromingen. In paragraaf 2.2 worden online radicalisering, rekrutering en mobilisatie geconceptualiseerd, waarbij wordt stilgestaan bij de samenhang en verschillen tussen deze concepten. Vervolgens wordt in paragraaf 2.3 kort besproken wat bekend is over online rekrutering voor andere vormen van criminaliteit. Tot slot geeft paragraaf 2.4 een overzicht van het mediagebruik van extremistische groepen door de tijd heen, om zo de hedendaagse online activiteiten van extremistische groepen beter te begrijpen. Daarbij wordt in 2.4.3 ingezoomd op de functionaliteiten van sociale media aan de hand van het bouwstelen-model en het *affordances*-model.

2.1 Radicalisering

Radicalisering wordt door de NCTV gedefinieerd als 'een proces van toenemende bereidheid om de uiterste consequentie uit een denkwijze te aanvaarden en die in daden om te zetten. Deze toenemende bereidheid kan leiden tot gedrag dat andere mensen diep kwetst of in hun vrijheid raakt, kan aanleiding zijn voor individuen of groepen om zich af te keren van de samenleving en kan leiden tot het gebruik van geweld' (NCTV, 2024). Inmiddels is al veel bekend over factoren die de kans op individuele radicalisering vergroten. Zo hebben onderzoekers uit verschillende academische disciplines contextuele omstandigheden en individuele kenmerken geïdentificeerd die zouden kunnen verklaren waarom iemand radicaliseert en uiteindelijk een bedreiging voor de samenleving kan worden (bijvoorbeeld Doosje et al., 2016; Feddes, Mann, & Doosje, 2012; King & Taylor, 2011; McCauley & Moskalenko, 2008; Wolfowicz, Litmanovitz, Weisburd, & Hasisi, 2020). Uit een systematische review naar risico- en beschermende factoren komt naar voren dat vooral criminogene factoren zoals een gebrek aan zelfbeheersing, het zoeken naar sensatie/het nemen van risico's, een criminele achtergrond en radicale attitudes risicoverhogend werken als het gaat om radicale intenties en radicaal gedrag (Wolfowicz et al., 2020). De grootste effecten qua beschermende factoren komen van leeftijd, binding met school, het volgen van de wet en respect hebben voor de overheid en autoriteiten. Deze bevindingen over beschermende factoren komen overeen met een eerder uitgevoerde studie naar beschermende factoren, waarin daarnaast ook zelfbeheersing, positief ouderschapsgedrag, niet-gewelddadige dierbaren en niet-gewelddadige leeftijdsgenoten als beschermend werden genoemd (Lösel et al., 2018). Ander onderzoek toont ook het belang van familie-gerelateerde factoren aan. Zo blijkt dat een hoge mate van conflicten binnen het gezin een risicofactor is voor radicalisering, terwijl een hoge sociaaleconomische status van het gezin, het hebben van een groter gezin en grote verbondenheid binnen het gezin juist beschermend werken (Zych & Nasaescu, 2022).

In verschillende studies worden ook meerdere stappen in het radicaliseringsproces onderscheiden. Bekend is het gedetailleerde *staircase to terrorism* model van Moghaddam (2005). Uit onderzoek blijkt dat het radicaliseringsproces niet altijd precies deze stappen volgt en dat deze modellen ook wat te deterministisch zijn opgesteld. Desondanks lijkt het nuttig om bij radicalisering in ieder geval een aantal hoofdfasen of aspecten te onderscheiden. In het literatuuroverzicht van Nickolson et al. (2021)

worden drie globale fasen onderscheiden: de gevoeligheidsfase, de groepsfase en de actiefase (zie ook Doosje et al., 2016 voor een vergelijkbaar onderscheid). In de eerste hoofdfase gaat het om het verwerven van radicale kennis en attituden. De radicalisering zit hier vooral in het hoofd van de betrokkenen en vrijblijvende communicatie met anderen en niet per se in de aansluiting bij bepaalde groepen of bewegingen of het daadwerkelijk uitvoeren van extremistische acties. Bij de tweede fase gaat het om de verdergaande, consistente interactie met en/of aansluiting bij extremistische groeperingen. In de derde fase gaan sommigen individueel of in groepsverband daadwerkelijk over tot extremistische actie(s). Bij het merendeel van de geradicaliseerde individuen blijft het bij gedachten en overtuigingen, en eventueel aansluiting bij en interactie met gelijkgestemden. Hoewel momenteel een aantal studies wordt uitgevoerd naar de hamvraag welke factoren bijdragen aan het overgaan tot actie (zie bijvoorbeeld Thijs, Rodermond, Kleemans & Van de Weijer, 2022), is bekend dat deze overgang zich moeilijk laat voorspellen.

Hoewel bovengenoemde modellen een theoretische onderbouwing voor radicalisering in het algemeen beogen te bieden, bestaat de laatste jaren ook toenemende aandacht voor verschillen in radicaliseringsprocessen in verschillende extremistische stromingen. Voorheen lag de focus vaak op één specifieke ideologie of extremistische groepering, wat het risico op bias of een eenzijdig beeld over radicaliseringsprocessen vergroot (Gaikwad et al., 2022). Uit de vergelijkende studies blijkt dat echter dat radicaliseringsprocessen van verschillende ideologieën meer overeenkomsten dan verschillen vertonen (Van Wonderen et al., 2023). De volgende overeenkomsten worden genoemd in Doosje et al. (2016), Brzuszkiewicz (2020) en Marwick et al. (2022): grote ontevredenheid over hoe instituties omgaan met ‘serieuze’ problemen in de samenleving, superioriteit van eigen normen en waarden, legitimeren van geweld, spanning tussen revolutionaire en traditionele waarden, de cultus van het heldendom, zwart-wit denken, aanzet tot polarisatie en verspreiding van desinformatie.

Ondanks de vele overeenkomsten, zijn er ook enkele vergelijkingsstudies die verschillen in radicaliseringsprocessen opmerken (Van Wonderen et al., 2023). Een belangrijke studie op dit gebied is de studie van Chermak en Gruenewald (2015). Zij vonden een aantal verschillen in persoonskenmerken en sociaal-demografische kenmerken tussen groepen die verschillende ideologieën aanhangen, wat zou kunnen leiden tot diverse ontwikkelingspaden van radicalisering. Zo zouden rechtsextremistische en jihadistische daders significant vaker met psychische stoornissen kampen dan links-extremistische daders, en leefden rechtsextremistische verdachten minder vaak in stedelijke gebieden dan jihadistische en links-extremistische verdachten. Daarnaast is het volgens Van Wonderen en collega’s (2023) relevant om aandacht te besteden aan de wijze waarop de samenleving reageert op verschillende extremistische stromingen. De studie van Marwick en collega’s (2022) constateert dat jihadistische aanslagen vaak sterk worden uitvergroot door de hoeveelheid aandacht die eraan wordt besteed door de media en andere instituties. Rechtsextremistische acties lijken volgens de auteurs minder te worden uitvergroot, zowel in de hoeveelheid aandacht die eraan wordt besteed als in hoe de acties gelabeld worden. Islamitisch extremisme kan hierdoor worden ervaren als verder afstaand van de ‘gemiddelde’ normen en waarden in de samenleving. Dit kan er vervolgens weer voor zorgen dat individuen die geassocieerd worden met deze ideologie een sterker gevoel van deprivatie ervaren en mogelijk ontvankelijker worden voor extremistisch gedachtegoed (Van Wonderen et al., 2023).

2.2 Online radicalisering, rekrutering en mobilisatie

Voor het huidige onderzoek onderscheiden we drie concepten: 'online radicalisering', 'online rekrutering', en 'online mobilisatie'. Deze drie vormen van online invloeden in het kader van extremisme sluiten goed aan bij de drie eerder onderscheiden fasen van het radicaliseringsproces. Over de eerste term, 'online radicalisering', blijkt binnen de wetenschappelijke literatuur geen consensus te bestaan. Uit een literatuurreview van Macdonald en Whittaker (2019) bleek dat slechts 21 procent van de studies over dit onderwerp een toelichting gaven op de term 'online radicalisering', en dat de overige studies verschillende definities hanteerden. De impact van internet op radicaliseringsprocessen wordt met uiteenlopende termen beschreven, waaronder 'faciliterend', 'versterkend', 'versnellend' en 'de primaire drijfveer van radicalisering' (zie o.a. Von Behr et al., 2013). Daarnaast wordt een breed scala aan gedragingen ondergebracht onder 'online radicalisering'; van het bekijken van extremistische propaganda tot het delen van gedetailleerde plannen voor een aanslag op een sociale media platform (zie o.a. Gill et al., 2015; Mutton et al., 2023).

Voor het huidige onderzoek definiëren we 'online radicalisering' als het proces waarbinnen een individu, door middel van online interacties en blootstelling aan online content, geweld gaat zien als een legitieme methode om sociale en politieke conflicten op te lossen (Bastug et al., 2020; Bermingham et al., 2009). Dit sluit aan bij de eerste fase van radicalisering die door Nickolson et al. (2021) wordt onderscheiden, namelijk de gevoeligheidsfase. In deze fase gaat het om processen in het hoofd van de betrokkenen en vrijblijvende communicatie met anderen en niet om processen van het aansluiten bij bepaalde groeperingen of het daadwerkelijk uitvoeren van extremistische acties.

Online rekrutering (in enge zin) sluit aan bij de tweede fase, de groepsfase. Radicalisering kan weliswaar een onderdeel zijn van rekrutering, maar toch is het belangrijk om deze twee begrippen van elkaar te onderscheiden. Opgemerkt dient te worden dat 'rekrutering' net als '(online) radicalisering' een containerbegrip lijkt te zijn, en dit wordt versterkt door online dynamieken, waardoor 'rekrutering' een veel meer fluïde (en ook moeilijk meetbaar) begrip wordt. Desalniettemin is het belangrijk om voor het huidige onderzoek te vertrekken vanuit een bepaalde definitie. Jones (2017) definieert rekrutering als een dynamisch proces waarbij een individu wordt aangemoedigd om lid te worden van een groep. Belangrijk daarbij is dat zowel de rekruteurs als de rekruten een afweging maken; rekruteurs over welke potentieel nieuwe leden zij benaderen (of juist niet benaderen) en mogelijke rekruten over het wel of niet aansluiten bij een groep. In navolging van de definitie van Jones (2017) verstaan wij onder 'online rekrutering' *het proces waarbij een individu online wordt aangemoedigd om lid te worden van een groep, organisatie of beweging.* 'Online mobilisatie' sluit aan bij de laatste fase van radicalisering, de actiefase, waarin individuen online worden beïnvloed om extremistische handelingen te verrichten, geweld te plegen of betrokken te raken bij terrorisme (Nickolson et al., 2021). Rekrutering kan in veel gevallen niet los worden gezien van initiële radicalisering van ideeën en mobilisatie. Een belangrijk onderscheid is echter dat radicalisering van ideeën niet per definitie om interactie vraagt, terwijl dat bij online rekrutering, in elk geval volgens bovenstaande definitie, wel het geval is. In het huidige onderzoek wordt daarom ook specifiek ingezoomd op de wijze van en betrokkenen bij de interactie.

2.3 (Online) rekrutering voor andere vormen van misdaad

Het onderzoek naar rekrutering voor extremistische groepen heeft veel raakvlakken met een bredere onderzoekstraditie naar mechanismen van toetreding tot andersoortige groepen. We bespreken hier kort wat bekend is over online rekrutering voor andere vormen van misdaad. Uit criminologisch onderzoek met betrekking tot de rol van peers en jeugdgroepen en met betrekking tot 'jonge aanwas' in de georganiseerde misdaad wordt duidelijk dat jongeren en jongvolwassenen op verschillende manieren betrokken kunnen raken bij criminele activiteiten en groeperingen. Zo wordt uit onderzoek naar het aansluiten bij problematische jeugdgroepen en gangs duidelijk dat hierbij verschillende processen moeten worden onderscheiden (Decker, Melde & Pyrooz, 2013; Densley, 2015; Weerman, Lovegrove & Thornberry, 2015). Er kan bijvoorbeeld sprake zijn van *invloed* van leeftijdsgenoten en vrienden die al deelnemen aan zo'n groep waardoor de kans wordt vergroot dat iemand zich ook gaat aansluiten. Anderzijds kunnen jongeren met een bepaalde achtergrond of levensloopontwikkeling er ook zelf voor kiezen om zich aan te sluiten (of dat te proberen) en is er dus sprake van *zelfselectie* zonder dat daar contacten of vriendschappen met andere jongeren in zulke groepen aan vooraf gaan. Kwalitatief onderzoek naar rekrutering door leden van gangs in Engeland laat zien dat het opbouwen van onderling vertrouwen van belang is bij het rekruteren van nieuwe leden voor gangs. Jongeren die in aanmerking komen om lid te worden van zo'n groep worden door al aanwezige gang-leden gemonsterd en getest op betrouwbaarheid en 'echtheid' (Densley, 2012).

Een andere vorm van criminaliteit waar regelmatig gebruik wordt gemaakt van de parapluterm rekrutering is georganiseerde misdaad. In een recente systematische meta-analyse (Adamse et al., 2023) worden vier typen processen onderscheiden waarbinnen jonge aanwas wordt gerekruteerd (zie ook De Boer, Ferwerda & Kuppens, 2022). Ten eerste kunnen jongeren en jongvolwassen actief worden gerekruteerd door personen uit georganiseerde criminaliteitsgroepen, voor incidentele en structurele activiteiten. Ook hier kan het opbouwen van onderling vertrouwen en het testen van 'echtheid' en in dit geval criminele vaardigheden weer een rol spelen (zie ook Smith, 2014 en De Boer et al., 2022). Ten tweede kunnen jongeren ook langzamerhand ingroeien in een georganiseerde criminaliteitsgroep via bestaande sociale structuren, zoals vriendschappen, familie en werk. Er kan ten derde sprake zijn van zelfselectie, waarbij jongeren en jongvolwassenen zelf contact leggen met georganiseerde misdaadgroepen, voor het uitvoeren van klussen of voor langduriger betrokkenheid. Ten vierde kunnen personen ook zelf het initiatief nemen voor het opzetten van een eigen georganiseerde criminaliteitsgroep, en daarbij weer anderen betrekken of rekruteren.

Waar het gaat om *online* rekrutering voor traditionele en cybercriminaliteit blijkt dat sociale media mogelijkheden bieden voor cybercriminele netwerken op het gebied van nieuwe leden vinden en op een snelle manier kunnen communiceren met mededaders (De Boer, Ferwerda & Kuppens, 2022; Roks, Leukfeldt & Densley, 2020). Criminelen rekruteren nog steeds via traditionele methoden, maar maken ook gebruik van nieuwe online mogelijkheden op dat vlak (Roks et al., 2020). Een recente studie naar zogeheten 'geldezels' (*money mules*) middels de bestudering van 43 Instagram accounts, toont bijvoorbeeld aan dat er verschillende online mechanismen een rol spelen (Bekkers & Leukfeldt, 2023). Met snel geld verdienen als doel bleek dat binnen de specifieke subcultuur rond geldezels drie mechanismen van belang zijn voor rekrutering: de belofte van een luxe levensstijl (via het tonen van emoticons en plaatjes van geld en luxe goederen), het normaliseren van de geldezel activiteiten (bijvoorbeeld door te verwijzen naar eerdere succesverhalen), en, in mindere mate, het neutraliseren

van de illegaliteit en risico's van deze praktijken (onder andere door te benoemen dat het meedoen zonder risico is). Daarnaast beschrijven de auteurs dat de accounts meer als een soort reclameboodschap kunnen worden beschouwd, dan dat de rekruteurs actief (dus aan de hand van veel berichten/plaatjes posten) mensen binnenhalen. Dit is ook in lijn met eerder onderzoek van Leukfeldt en Kleemans (2019) en wat hierboven beschreven is als 'zelfrekrutering', waarbij nieuwe aanwas op eigen initiatief contact zoekt met rekruteurs.

2.4 Mediagebruik van extremistische groepen door de tijd heen

2.4.1 Voorafgaand aan de komst van internet en sociale media

Om de hedendaagse online activiteiten van extremistische groepen te begrijpen, is het belangrijk om eerst een beeld te schetsen van hoe extremisten in de loop der jaren gebruik hebben gemaakt van verschillende vormen van media. Kenmerkend voor extremistische groeperingen is dat ze elke gelegenheid benutten om hun ideologie onder de aandacht te brengen bij een groot publiek en nieuwe leden te rekruteren, dergelijke groepen hebben dan ook altijd snel ingespeeld op nieuwe ontwikkelingen in de media (Scrivens & Conway, 2019).

Voor het ontstaan van moderne massamedia waren extremisten beperkt in hun mogelijkheden om de massa's te bereiken. Dit weerhield hen er echter niet van om hun boodschap over te brengen en invloed uit te oefenen op een groter publiek, bijvoorbeeld door middel van openbare executies (Rapoport, 1984) en muurschilderingen (Matusitz, 2014). Rekruteringsprocessen speelden zich top-down en grotendeels face-to-face af, en radicalisering vond veelal plaats als resultaat van actieve rekrutering (Smith & Alarid, 2019). Met de komst van de eerste vormen van media zoals kranten en magazines (door Scrivens & Conway (2019) ook wel 'low-tech media tools' genoemd) werd het eenvoudiger om extremistische denkbeelden te verspreiden, nieuwe leden te rekruteren en steun te krijgen van een breder publiek. Ook de high-tech kanalen van destijds zoals radio en televisie, hadden directe invloed op terrorisme en extremisme (Carruthers, 2000; Chaliand, 1985; Hoffman, 2006; Schmid & De Graaf, 1982). Extremistische stromingen en groeperingen zoals het nationaalsocialisme in Duitsland en de Ku Klux Klan in de Verenigde Staten speelden in op deze nieuwe vormen van media door onder meer propaganda te verspreiden en aan te zetten tot actie in radiotoespraken en films. Radiopropaganda droeg bijvoorbeeld bij aan het rekruteren van nieuwe leden voor de NSDAP, en zette aan tot antisemitische acties (Adena et al., 2015).

2.4.2 Internet en sociale media

Met de komst van internet rees de vraag hoe extremistische groepen en individuen hierop zouden inspelen. In eerste instantie werd vooral gedacht aan cyberterrorisme, waarbij het online domein het doel is van of het middel voor een terroristische aanval (zie bv. Collin, 1997; Devost et al., 1997; National Research Council, 1991). Hierbij kan bijvoorbeeld gedacht worden aan een grootschalige verstoring van een computernetwerk (het online domein als doel), of het online domein dat wordt gebruikt als communicatiemiddel om een terroristische actie te beramen in de offline wereld. Al snel werd geconcludeerd dat de relatie tussen extremisme en internet complexer lag. Er werden vijf doelen onderscheiden waarvoor extremisten internet gebruiken, te weten: informatieverstrekking, financiering, netwerken, rekrutering en informatieverzameling (Conway, 2006). Deze doelen overlappen vaak en kunnen dan ook niet los van elkaar worden gezien. Daarnaast verschilt internet,

en met name sociale media, wezenlijk van traditionele media (zoals kranten en televisie) wat betreft hun bereik, interactiviteit, bruikbaarheid en hun alomtegenwoordigheid (Baccarella et al., 2018).

Een belangrijke vraag die sinds de komst van internet wordt gesteld is in hoeverre online processen offline processen kunnen vervangen (Schils & Verhage, 2017). Lang werd gedacht dat fysiek contact noodzakelijk was voor het begaan van 'hoog-risico activiteiten' zoals het rekruteren voor extremistische groeperingen of het plannen van gewelddadige acties. Sommige onderzoekers zagen de komst van internet echter slechts als een veranderende context waarbinnen extremisten opereren. Extremistische groepen hebben zich altijd al ingespannen om nieuwe leden te rekruteren en daarbij steeds gebruik gemaakt van bepaalde vormen van media. Door zich simpelweg aan te passen aan een nieuwe context gebruiken extremistische groepen telkens nieuwe vormen van media om hun doelen na te streven (Klein, 2009; Schils & Verhage, 2017; Trend, 2007).

Andere onderzoekers wijzen erop dat internet en sociale media een aantal kenmerken hebben die hen onderscheiden van traditionele media en dat die kenmerken radicaliserings- en rekruteringsprocessen bevorderen. Zo zijn sociale media interactiever dan andere vormen van media. De constante mogelijkheid tot real-time interactie zorgt ervoor dat rekruteurs gemakkelijk banden kunnen opbouwen en onderhouden met (potentiële) rekruten. Daarnaast zorgt internet ervoor dat individuen ten alle tijden eenvoudig toegang kunnen krijgen tot extremistische narratieven, waardoor niet alleen interesse kan worden gewekt voor deze narratieven, maar deze interesse ook in stand gehouden kan worden (Thompson, 2011; Schils & Verhage, 2017). Dit sluit aan bij de vijf hypothesen die Von Behr en collega's (2013) opstelden op basis van een uitgebreide literatuurstudie over de rol van internet in radicaliseringsprocessen: 1) internet creëert meer kansen om te radicaliseren, 2) internet fungeert als 'echokamer' van ideeën die worden ondersteund door gelijkgestemden, 3) internet versnelt het radicaliseringsproces, 4) internet maakt radicalisering mogelijk zonder fysiek contact en, 5) internet vergroot de kans op 'zelfradicalisering'. In lijn met de laatste twee hypothesen, wordt door een aantal auteurs gesuggereerd dat sommige *lone wolves* wellicht radicaliseerden en tot actie overgingen enkel door het opdoen van een gewelddadig extremistisch gedachtegoed via internet en dus zonder direct contact met anderen (Jones, 2017; Sageman, 2008; Weimann, 2012).

Door de jaren hebben extremistische groepen veelvuldig gebruik gemaakt van internet en hebben zich daarbij continue aangepast aan veranderende en uitbreidende mogelijkheden (Conway, Scrivens, & Macnair, 2019). Voorafgaand aan het ontstaan van het World Wide Web (WWW) maakten groepen al gebruik van de voorloper, het Bulletin Board System (BBS). Conway en collega's beschrijven hoe in de Verenigde Staten rond 1984 het 'Aryan Nation Liberty Net' werd opgericht en gerund door de rechts-extremistische Louis Beam. Iedereen met een computer en een modem kon via bepaalde telefoonnummers 'inbellen' en vervolgens op het Liberty Net allerhande haat-propaganda vinden. Daarnaast werd het kanaal gebruikt om informatie te delen over bijeenkomsten van de Aryan Nation en over andere rechts-extremistische groepen (Conway et al., 2019). Met de ontwikkeling en snelle groei van het WWW halverwege de jaren '90 breidden de online mogelijkheden zich verder uit. In deze periode maakten extremistische groepen vooral gebruik van de meer statische websites en fora om hun gedachtegoed te verspreiden, hun netwerk uit te breiden en contacten te onderhouden. Met de komst van web 2.0 verlegden extremistische groepen hun focus van websites en fora naar 'mainstream sociale media' zoals Facebook, Twitter (nu X), en YouTube (Hegghammer, 2014). Inmiddels heeft er een verschuiving plaatsgevonden naar meer versleutelde, low profile platforms zoals Telegram, omdat

mainstream platforms zich steeds meer zijn gaan richten op het detecteren en verwijderen van extremistische content (Jensen et al., 2018). Om te kunnen begrijpen hoe dergelijke platforms kunnen worden aangewend voor rekrutering, is het van belang om de voornaamste functionaliteiten van sociale media in kaart te brengen. Op deze functionaliteiten gaan wij nu in.

2.4.3 Functionaliteiten van sociale media

Om te begrijpen hoe extremistische groepen sociale media kunnen gebruiken moet niet alleen worden gekeken naar kenmerken van de sociale media zelf, maar ook naar hoe die kenmerken aansluiten bij de leefwereld van de gebruikers. In dit kader beschrijven we twee modellen, het bouwstenen-model van Kietzmann et al. (2011) en het gerelateerde 'affordances-model' (Boyd, 2010; Todorović, Sieckelick, Manders, Timmerman, & Van der Linden, 2023).

Het bouwstenen-model

Kietzmann en collega's beschrijven de verschillende kenmerken en functionaliteiten van sociale media aan de hand van zeven bouwstenen. De eerste bouwsteen van sociale media die door Kietzmann en collega's (2011) wordt beschreven, is de mate waarin gebruikers met anderen **communiceren**. Veel sociale media platforms bieden de mogelijkheid om te communiceren met andere gebruikers met behulp van functies zoals "vind-ik-leuk", "beantwoorden/reageren" en het versturen van directe berichten. Deze functionaliteit maakt het voor extremisten eenvoudiger om in contact te komen met (potentiële) rekruten door een-op-een gesprekken te voeren met kwetsbare individuen, om ze vervolgens te isoleren en geleidelijk kennis te laten maken met de extremistische groep en het bijbehorende gedachtegoed (Apau, 2018).

Naast communiceren met andere gebruikers, wordt op sociale media **content uitgewisseld**, zoals foto's, video's en andere bestanden. Het gemak waarmee content gedeeld kan worden op sociale media, maakt het aantrekkelijk om extremistische content te delen die wellicht offline minder goed zou worden ontvangen. Daarnaast creëren sociale media de mogelijkheid voor extremistische groepen om valse informatie (ook wel 'fake news' of desinformatie genoemd) te verspreiden. Aangezien alle soorten informatie op sociale media op gelijke voet wordt weergegeven, kan dit de geloofwaardigheid en legitimiteit van extremistische narratieven versterken (Apau, 2018).

Ten derde geven sociale media informatie over de **beschikbaarheid en bereikbaarheid** van anderen, zowel online als offline. Veel sociale media platforms maken gebruik van locaties van gebruikers, en gebruikers kunnen deze informatie ook zelf delen met anderen. Informatie over de beschikbaarheid en bereikbaarheid van een persoon stelt anderen in staat om in real time direct te communiceren (Elaluf-Calderwood et al., 2005), waardoor meer invloedrijke interacties kunnen ontstaan (Apau, 2018; Kaplan & Haenlein, 2010).

Ten vierde communiceren gebruikers met andere gebruikers op basis van een **gedeelde connectie**, bijvoorbeeld een bepaalde interesse of gemeenschappelijke vrienden, waardoor ze zich associëren met elkaar. Extremisten gebruiken bijvoorbeeld bepaalde gaming platforms om in contact te komen met sympathisanten of potentiële rekruten, om ze vervolgens te indoctrineren met radicale ideeën en uiteindelijk te mobiliseren voor actie (Rosenblat & Barrett, 2023).

Daarnaast speelt de **reputatie** van gebruikers een belangrijke rol op sociale media platforms. Hiermee wordt gedoeld op de mate waarin gebruikers de positie van anderen en zichzelf kunnen bepalen en beïnvloeden in het online domein. De reputatie van gebruikers kan bijvoorbeeld aangegeven worden door het aantal volgers, weergaven en 'likes', maar ook door hoe lang iemand al actief is op het platform. Zoals eerder werd benoemd, kan elke gebruiker content delen op sociale media, al dan niet anoniem. Wanneer echter een gebruiker met een invloedrijke reputatie bepaalde schadelijke of onjuiste content deelt, bereikt dit een groter publiek en kan het daardoor meer schade aanrichten.

Op de zesde plaats maken veel sociale media platforms het voor gebruikers mogelijk om lid te worden van **groepen** of er zelf een te creëren, gecentreerd rond gedeelde interesses, opvattingen of doelen. Door deze functie kunnen gebruikers een online gemeenschap vormen waarin verschillende individuen samenkomen om informatie of steun te bieden of te ontvangen (Lea et al., 2006). Onderdeel uitmaken van een dergelijke (online) gemeenschap, creëert een gevoel van emotionele verbondenheid en saamhorigheid waardoor leden zich gesteund voelen binnen de gemeenschap. In de internationale literatuur wordt vaak het belang aangestipt van 'the need to belong', en sociale media kunnen voorzien in deze behoefte (McMillan & Chavis, 1986). Een keerzijde van deze groepsfunctie op sociale media is dat er een "ingroup-outgroup bias" kan ontstaan of worden versterkt, waarbij individuen zich met de ingroup identificeren en zich tegen de outgroup afzetten (Brewer, 1999; Tajfel & Turner, 2004). De sociale media groep fungeert dan als een soort echokamer waarin eigen opvattingen en overtuigingen worden versterkt en die van de outgroup gebagatelliseerd, wat kan bijdragen aan verdere polarisatie. Daarnaast kunnen de gedeelde visies van leden ervoor zorgen dat online gemeenschappen een primaire rol spelen in mobilisatie en collectieve actie, zowel online als offline. Dergelijke online groepen waar in beginsel iedereen aan kan deelnemen kunnen lang onder de radar blijven (Weimann, 2010), wat de aanpak ervan lastig maakt.

Het laatste en centrale kenmerk van sociale media is het presenteren van een eigen **identiteit**. Naast het verstrekken van objectieve persoonsgegevens, zoals naam of leeftijd, kunnen gebruikers ook hun interesses delen door deel te nemen aan specifieke groepen rondom dat thema, of door te reageren op bepaalde content. Het instellen van een gebruikersnaam, profielfoto en eventueel aanvullende informatie is een voorwaarde van de meeste sociale media-applicaties. Op deze manier positioneren gebruikers zichzelf ten opzichte van anderen in het online domein, wat vervolgens kan bijdragen aan processen van rekrutering en mobilisatie.

Het affordances-model

Kennis over de bovengenoemde bouwstenen is belangrijk om de invloed van de online leefwereld te begrijpen. De laatste jaren gaat met name veel aandacht uit naar de invloed van de online leefwereld op de ontwikkeling van adolescenten (Todorović et al., 2023), en hierbij wordt veelvuldig gewezen op de term 'online affordances' (Boyd, 2010). In hun onderzoek naar het concept online affordances en het belang daarvan beschrijven Todorović en collega's wat dient te worden verstaan onder het concept affordances. Het gaat hier om de bedoelde en onbedoelde gebruiksmogelijkheden zoals geboden door bepaalde objecten. Als voorbeeld wordt een mok genoemd, die niet alleen kan dienen om uit te drinken, maar ook als maatbeker, of als pennenhouder. Met betrekking tot online affordances wordt geciteerd dat online affordances 'emerge(s) from the relation between the technology and other actors and is thereby not solely related to the features of the technology' (Aasback, 2022 p. 352; Todorović et al., 2023, p. 167). In de literatuur worden zeven van deze gebruiksmogelijkheden van de

online wereld genoemd die een belangrijke rol spelen in de leefwereld van adolescenten, en die dus ook belangrijk zijn om de invloed van de online wereld op adolescenten te begrijpen. In de handreiking 'Echt zijn in de online leefwereld' (Todorović et al., 2023) worden deze gebruiksmogelijkheden uiteengezet (zie ook Tabel 1). De eerste gebruiksmogelijkheid is asynchroniteit, ofwel 'de mogelijkheid om te communiceren wanneer het uitkomt, in realtime (synchroon) of uitgesteld (a-synchroon)'. De tweede mogelijkheid is anonimiteit, en dan met name 'de mogelijkheid om te bepalen in welke mate de communicatie anoniem is'. De derde mogelijkheid is bereikbaarheid, 'de mogelijkheid om wel of niet online te zijn en alert aan of uit te zetten'. De vierde mogelijkheid betreft de toegankelijkheid, en meer specifiek de mogelijkheid 'om makkelijk informatie op te zoeken, contact te leggen en te onderhouden'. Zichtbaarheid is de vijfde mogelijkheid, en dan met name om 'de omvang en aard van het publiek te bepalen'. De zesde mogelijkheid is de verspreidbaarheid, waarbij inhoud kan worden gekopieerd of gedeeld. Tot slot is de zevende mogelijkheid permanentie, ofwel de mogelijkheid 'van het bewaren en later ophalen van gepubliceerde inhoud'.

Het belang van het affordances-model zit met name in de koppeling van de genoemde gebruiksmogelijkheden aan de ontwikkelingsbehoeften van jongeren in de online leefwereld (en overigens ook van ouderen, zie bijvoorbeeld Jung & Sundar, 2018)., behoeften als het vormen van een zelfbeeld, online relaties, en talentontwikkeling (Todorović et al., 2023). Het is juist deze aansluiting die cruciaal is voor het begrijpen van de invloed van de online wereld op een veelheid aan uitkomsten, waaronder online rekrutering.

Tabel 1. Gebruiksmogelijkheden van het online domein (Todorović et al., 2023; Valkenburg, 2014).

Gebruiksmogelijkheden	Beschrijving
Asynchroniciteit	De mogelijk om te communiceren wanneer het uitkomt, in real time (synchroon) of uitgesteld (asynchroon).
Anonimiteit	De mogelijkheid om te bepalen in welke mate de communicatie anoniem is.
Bereikbaarheid	De mogelijkheid om wel of niet online te zijn en notificaties aan of uit te zetten.
Toegankelijkheid	De mogelijkheid om makkelijk informatie op te zoeken, contact te leggen en te onderhouden.
Zichtbaarheid	De mogelijkheid om de omvang en aard van het publiek te bepalen.
Verspreidbaarheid	De mogelijkheid om inhoud te kopiëren of te delen.
Permanentie	De mogelijkheid van het bewaren en later ophalen van gepubliceerde inhoudt.

2.5 Tot slot

De laatste jaren is steeds duidelijker geworden dat internet, meer specifiek sociale media, een enorme invloed kan hebben op processen van radicalisering en rekrutering. In dit hoofdstuk is allereerst ingezoomd op het concept radicalisering en een aantal theoretische modellen die radicalisering trachten te verklaren. Een belangrijke gemene deler van de verschillende modellen is dat radicalisering als een proces wordt gepresenteerd, bestaande uit verschillende fasen. Een veelgebruikte indeling is die naar een 'gevoeligheidsfase', een 'groepsfase' en een 'actiefase', waarbij wordt gewezen op het

feit dat maar weinig mensen de laatste fase bereiken. In dit hoofdstuk werd het theoretische model vertaald naar de online omgeving en de verschillende processen die daar kunnen spelen, te weten online radicalisering, online rekrutering en online mobilisatie. Online radicalisering is gedefinieerd als 'het proces waarbinnen een individu, door middel van online interacties en blootstelling aan online content, geweld gaat zien als een legitieme methode om sociale en politieke conflicten op te lossen'. Online rekrutering definieerden wij als 'het proces waarbij een individu online wordt aangemoedigd om lid te worden van een groep, organisatie of beweging'. Online mobilisatie werd tot slot gedefinieerd als 'de fase waarin individuen online worden beïnvloed om extremistische handelingen te verrichten, geweld te plegen of betrokken te raken bij terrorisme'. Wij achtten het belangrijk om deze definities te geven, ook van processen die niet op de voorgrond staan in het huidige onderzoek, omdat eruit volgt dat de processen sterk met elkaar verweven (kunnen) zijn. Hoewel nog veel onbekend is over de volgordelijkheid van processen wordt algemeen aangenomen dat online rekrutering doorgaans niet helemaal los kan worden gezien van radicalisering van ideeën. Een belangrijk onderscheid is echter dat radicalisering van ideeën niet per definitie om interactie vraagt, terwijl dat bij online rekrutering, in elk geval volgens bovenstaande definitie, wel het geval is.

Met de toename aan kennis over het online domein is ook vast komen te staan dat inzichten in offline processen niet a priori vertaalbaar zijn naar online processen. Sociale media hebben verschillende functionaliteiten die maken dat de online context sterk afwijkt van de offline context. In dit hoofdstuk zijn daarom ook twee theoretische modellen behandeld die deze functionaliteiten centraal stellen en daarbij specifiek ingaan op hoe de functionaliteiten aansluiten bij de leefwereld van gebruikers, met name jongeren. Dergelijke functionaliteiten zoals anonimiteit, beschikbaarheid en bereikbaarheid en het uitwisselen van content maken van het online domein een omgeving waar mensen potentieel makkelijker kunnen worden gerekruteerd en anderen kunnen rekruteren. Uit eerder onderzoek naar online rekrutering voor traditionele en cybercriminaliteit blijkt inderdaad dat sociale media talloze mogelijkheden bieden aan (cyber)criminele netwerken om nieuwe leden te vinden en op een snelle manier te communiceren met mededaders.

De vraag is hierbij in hoeverre extremistische groepen de functionaliteiten van internet aanwenden om online nieuwe leden te rekruteren. Daarom zijn we in dit hoofdstuk tot slot ingegaan op het mediagebruik van extremistische groepen door de jaren heen. Lang werd gedacht dat fysiek contact noodzakelijk was voor het begaan van 'hoog-risico activiteiten' zoals rekrutering of aanvalsplanning. Daarnaast is gebleken dat extremistische organisaties door de jaren heen veelvuldig gebruik hebben gemaakt van internet en zich daarbij continue hebben aangepast aan veranderende en uitbreidende mogelijkheden. De unieke functionaliteiten van internet lijken vervolgens een belangrijke bijdrage te hebben geleverd aan grootschalige online radicalisering, netwerkvorming en rekrutering. Hoewel over online radicalisering inmiddels al veel bekend is, is nog veel minder zicht op hoe extremistische groepen de functionaliteiten van internet en sociale media inzetten om nieuwe aanwas voor de groep te vinden. Dit is problematisch gelet op de in hoofdstuk 1 en 2 geschetste ontwikkelingen. In de huidige studie trachten we daarom te achterhalen hoe processen van online rekrutering door en voor extremistische organisaties verlopen. In het volgende hoofdstuk beschrijven we de diverse methoden die we gebruiken om antwoord te geven op de eerder uiteengezette onderzoeksvragen.

3. Methode

Ter beantwoording van de onderzoeksvragen is gebruik gemaakt van (1) een verkenning van de wetenschappelijke literatuur, (2) interviews met professionals, (3) een kwalitatieve contentanalyse van een selectie van openbare online platforms en (4) een expertmeeting met professionals uit de praktijk en wetenschappers. Het literatuuronderzoek vormde de start van het huidige onderzoek. Vervolgens is een eerste reeks interviews uitgevoerd die mede richting hebben gegeven aan de contentanalyse van een selectie online platforms. Gedurende deze contentanalyse is de interviewreeks voortgezet. Richting het eind van het onderzoek is een expertmeeting georganiseerd waarin de resultaten zijn gepresenteerd en bediscussieerd. In wat nu volgt, bespreken we de verschillende onderzoeksmethoden. Tot slot wordt in paragraaf 3.5 ingegaan op een aantal ethische overwegingen en privacyaspecten.

3.1 Scan van de literatuur

Gedurende de eerste fase is een uitgebreide verkenning verricht van de literatuur over rekrutering door extremistische groepen en -individuen en online mobilisatie voor extremistische acties. Hiervoor zijn verschillende databases geraadpleegd, namelijk Google Scholar, Criminal Justice Abstracts, Web of Science, WODC Kennisbank, PsycInfo en Scopus. Bij de zoekstrategie is rekening gehouden met de gevarieerde terminologie die wordt gebruikt in literatuur over rekrutering en mobilisatie in relatie tot extremisme (rekruter*, mobili*, ronsel*, werv*, select*, recruit*, call* for). Na vaststelling van de zoekstrategie is deze in de hierboven genoemde zoekmachines ingevoerd. Op basis van de titels en abstracts van de publicaties is vervolgens bezien welke studies geschikt zijn voor inclusie in de review. Hierbij is onder meer gekeken naar de relevantie en kwaliteit van de studies, het tijdsbestek waarin de studies zijn uitgevoerd, en de taal waarin de studies zijn gepubliceerd. Wat betreft de relevantie en kwaliteit van de studies is voornamelijk gekeken naar de mate waarin de studies specifiek aandacht besteden aan rekrutering en/of mobilisatie. Aangezien we slechts een beperkte hoeveelheid studies (20) hebben gevonden die specifiek gaan over rekrutering en/of mobilisatie voor extremistische groepen, en deze sterk verschillen qua methodiek en sample size, is ervoor gekozen om niet verder te excluderen op kwaliteitscriteria. Daarnaast lag de focus op Nederlandstalige en Engelstalige wetenschappelijke studies en rapporten en beleidsstukken.

3.2 Interviews

Voorts zijn semigestructureerde interviews met twee groepen professionals uitgevoerd, namelijk (1) medewerkers die in het kader van de handhaving, opsporing en vervolging in hun primaire werkzaamheden met de hier besproken thematiek en problematiek te maken hebben en (2) medewerkers die vanuit andersoortige dagelijkse werkzaamheden zicht krijgen op deze thematiek en problematiek. Met betrekking tot de tweede groep kan bijvoorbeeld gedacht worden aan medewerkers van het Landelijk Steunpunt Extremisme (LSE) die werken met de doelgroep of medewerkers van gemeenten die informatie krijgen van de politie en andere partijen tijdens multidisciplinaire casusoverleggen. In totaal is gesproken met 14 professionals, bestaande uit medewerkers van de Nationale Politie (3), Algemene Inlichtingen- en Veiligheidsdienst (2), Landelijk

Steunpunt Extremisme (2), Expertise-unit Sociale Stabiliteit (2), gemeenten (3) en jongerenwerkers (2). Een overzicht van de respondenten is weergegeven in Tabel 2.

Tabel 2. Overzicht respondenten

Interview	Respondent	Instantie
1	Respondent_politie_1	Nationale Politie
2	Respondent_politie_2	
3	Respondent_politie_3	
4	Respondent_AIVD_1	Algemene Inlichtingen- en Veiligheidsdienst
5	Respondent_AIVD_2	
6	Respondent_LSE_1 Respondent_LSE_2	Landelijk Steunpunt Extremisme
7	Respondent_ESS_1 Respondent_ESS_2	Expertise-unit Sociale Stabiliteit
8	Respondent_gemeente_1 Respondent_gemeente_2	Gemeenten uit Randstad en regio
9	Respondent_gemeente_3	
10	Respondent_jongerenwerk_1	[niet nader gespecificeerd i.v.m. privacy]
11	Respondent_jongerenwerk_2	

Op basis van de literatuurstudie is door de onderzoekers een topiclijst ontwikkeld. De topiclijst is ingedeeld in drie thema's die zijn gebaseerd op de hoofdvragen van het onderzoek: 1) aard en mechanismen van online rekrutering en mobilisatie, 2) interactie tussen online en offline gedrag, en 3) handelingsperspectieven en mogelijke aanpakken (zie Bijlage 2 voor de volledige topiclijst). De interviews zijn afgenomen tussen oktober 2023 en maart 2024. Een meerderheid van de gesprekken vond plaats op locatie en drie interviews zijn digitaal afgenomen. De gemiddelde duur van de interviews was een uur, waarbij het kortste interview 55 minuten bedroeg en het langste interview anderhalf uur. De interviews zijn na afloop van het gesprek verbatim getranscribeerd of samengevat, gepseudonimiseerd en op een beveiligde server opgeslagen.

Vervolgens zijn de interviews systematisch gecodeerd en geanalyseerd middels het programma ATLAS-ti. De onderzoekers hebben tijdens verschillende fasen van het analyseproces overlegd om overeenstemming te vinden over de codes en de toekenning ervan aan specifieke data. Hierbij is in beginsel een inductieve benadering gebruikt. Daarnaast zijn we ook op zoek gegaan naar nieuwbenoemde (gedeelde) ervaringen van de respondenten, die op hun beurt mogelijk kunnen bijdragen aan theorievorming. Gezamenlijk hebben de gesprekken bijgedragen aan kennis over mechanismen van online rekrutering en gaven tevens weer tegen welke beperkingen deze professionals aanlopen bij de preventie van rekrutering en mobilisatie. Hierbij valt bijvoorbeeld te denken aan de grenzen van de wettelijke bevoegdheden, waardoor de informatiepositie niet optimaal is. Tevens gaven de eerste interviews richting aan de contentanalyse, vooral wat betreft het aanscherpen van het codeerschema en het verkrijgen van beter inzicht in de platforms die momenteel worden gebruikt door extremistische groepen.

3.3 Contentanalyse

Om een beeld te krijgen van de mechanismen rondom online rekrutering en mobilisatie voor extremistische groepen, is een kwalitatieve contentanalyse uitgevoerd van openbare online platforms. Openbare platforms geven over het algemeen minder zicht op latere fasen van rekrutering, maar geven wel een goed beeld van (mogelijke) beginfasen van dergelijke processen. Om een zo breed mogelijk beeld te krijgen van rekruteringsprocessen hebben wij ons gericht op verschillende ideologieën, namelijk extreemrechts, extreemlinks, anti-institutioneel en jihadisme. De keuze voor specifieke groepen is gebaseerd op verschillende bronnen, waaronder recente Dreigingsbeelden Terrorisme Nederland (DTN's) van de NCTV en jaarverslagen van de AIVD. Hierbij dient te worden opgemerkt dat het concept 'extremistische groep' niet helder is gedefinieerd. Aangezien we ons met de contentanalyse daarnaast richten op openbare platforms die enkel een beeld geven van (mogelijke) beginfasen van rekrutering kan niet in alle gevallen worden gesproken van duidelijk afgebakende groepen die in het algemeen als 'extremistische groep' worden beschouwd. Wel worden in alle geanalyseerde groepen berichten geplaatst die geïnterpreteerd kunnen worden als uitingen van een extreem gedachtegoed. Om deze reden duiden we de geanalyseerde groepen niet aan als 'rechtsextremistisch' of 'jihadistisch extremistisch' maar als een 'extreemrechtse' of 'jihadistische' groep. Qua platforms hebben we ons beperkt tot Telegram en Facebook omdat deze platforms worden genoemd in DTN58 (het meest recente dreigingsbeeld ten tijde van de contentanalyse).

Het zoekproces verschilde per groepering. Een aantal groepen was onder hun exacte naam te vinden op Telegram of Facebook. Andere groepen waren niet direct vindbaar. Voor deze groepen is een zoekstrategie uitgevoerd op Google, door op de naam van de groepering te zoeken in combinatie met 'Nederland' en het specifieke platform waar de groepering actief zou zijn. De overige online groepen zijn gevonden via de website van de groepering. Indien een groepering meerdere online groepen had, is een selectie gemaakt op basis van de frequentie van berichten (minimaal meerdere berichten per maand) en het grootste aantal deelnemers.

Met de contentanalyse richten we ons op vier ideologische stromingen, namelijk extreemrechts, anti-institutioneel, jihadistisme en extreemlinks. Er zijn zeven online groepen, kanalen of pagina's[1] geselecteerd (zie tabel 3), afhankelijk van op welk platform de groepering openbaar actief was. De uiteindelijke selectie bestaat uit drie Telegramkanalen, één Telegramgroep en drie Facebookpagina's waarop hoofdzakelijk in het Nederlands wordt gecommuniceerd. Ten behoeve van het leesgemak duiden we deze aan als 'groepen'. Vanuit extreemrechts, anti-institutioneel en jihadisme zijn elk twee groepen geanalyseerd. Aanvullend is een extreemlinkse groep geïncludeerd, zodat er een betere vergelijking getrokken kan worden tussen groepen met verschillende ideologische overtuigingen en de analyse daarmee evenwichtiger is.

De groepen hebben gemiddeld rond de 1900 deelnemers, waarbij de kleinste groep rond de 80 deelnemers heeft en de grootste groep rond de 6600 deelnemers. De online groepen zijn allen relatief

[1] Van een online groep kunnen individuele gebruikers lid worden. Elk lid kan berichten plaatsen in de groep en op elkaars berichten reageren. Op een kanaal of pagina kan alleen de beheerder berichten plaatsen. Individuele gebruikers kunnen zich abonneren op een kanaal of een pagina volgen, en reacties plaatsen met tekstberichten en/of emoji's.

jong en opgericht tussen 2020 en 2023. Voor elke groepering is gekeken naar de laatste 15 dagen waarop berichten werden geplaatst tot aan de start van het dataverzamelingsproces op 1 november 2023. Dagen waarop geen berichten werden geplaatst, zijn niet geïncludeerd in de analyseperiode. Ter illustratie: van een groep die dagelijks berichten plaatst, loopt de analyseperiode van 17 oktober tot 31 oktober 2023. Wanneer een groep echter niet dagelijks berichten plaatst, is de analyseperiode langer en gaat deze verder terug in de tijd. Van de geanalyseerde groepen liep de langste analyseperiode van april 2023 tot aan november 2023, en de kortste periode bedroeg de laatste twee weken van oktober 2023. Ook waren niet alle geanalyseerde groepen even actief. In de analyseperioden werden er gemiddeld 26 berichten geplaatst. De minst actieve groep plaatste 15 berichten in de betreffende periode en de meest actieve groep plaatste 57 berichten.

Tabel 3. Overzicht geanalyseerde groepen contentanalyse

Naam groep	Gedachtegoed
Groep 1	Extreemrechts
Groep 2	Extreemrechts
Groep 3	Anti-institutioneel
Groep 4	Anti-institutioneel
Groep 5	Jihadistisch
Groep 6	Jihadistisch
Groep 7	Extreemlinks

Van deze berichten zijn schermafbeeldingen gemaakt, die vervolgens met behulp van een vooraf opgesteld codeerschema (zie Bijlage 3) middels het programma ATLAS.ti zijn geanalyseerd. Ook beeldmateriaal en videofragmenten zijn geanalyseerd. Het codeerschema is gebaseerd op de wetenschappelijke literatuur, alsmede op de eerste interviews met professionals. Net als voor de interviewtopiclijst, hebben de onderzoekers in verschillende fasen van het analyseproces overlegd om overeenstemming te vinden over de codes en de toekenning ervan aan specifieke data. In de analyse is primair gekeken naar mechanismen van rekrutering en mobilisatie, waaronder het detecteren van wervende teksten en oproepen tot actie (codes: ‘expliciete rekrutering’, ‘directe oproep tot actie’), het posten van links naar andere websites/apps (‘verwijzing openbaar platform’) en uitnodigingen voor privégroepen/chats (‘verwijzing besloten platform’). De codes zijn gebruikt om in kaart te brengen welke mechanismen worden gebruikt bij online rekrutering en om die mechanismen te ordenen en te classificeren. We hebben dus hoofdzakelijk een deductieve benadering (d.w.z. "theoriegestuurd") gebruikt om onze kwalitatieve gegevens te analyseren (zie ook Braun en Clarke 2006). Niet alle gegevens vielen echter te scharen onder deductieve codes. Daarom zijn een aantal inductieve codes toegevoegd aan het codeerschema, zoals ‘doorlichtingsprocedure’ (blijkt uit berichtgeving dat er bepaalde eisen worden gesteld aan lidmaatschap?), ‘rekruterings-/mobiliseringsnarratief’ (worden er bepaalde narratieven ingezet ten behoeve van rekrutering of mobilisering?) en ‘aanhaken op actualiteit’ (wordt er ingespeeld op actuele gebeurtenissen om het gedachtegoed te verspreiden onder potentiele nieuwe rekruten?).

3.4 Interactieve expertmeeting

Het doel van de expertmeeting was tweeledig. Allereerst is de bijeenkomst gebruikt om de onderzoeksresultaten terug te koppelen naar beleid en praktijk. Daarnaast had de bijeenkomst als doel om suggesties en input te ontvangen over mogelijke consequenties voor algemene handelingsperspectieven en concrete aanpakken. Daarmee heeft de bijeenkomst ons in staat gesteld om het rapport voor de praktijk werkbare aanbevelingen op te nemen. Tijdens de expertmeeting was een breed samengestelde groep professionals aanwezig, bestaande uit wetenschappers met expertise over relevante thema's en *practitioners* vanuit de gemeente en Reclassering Nederland (zie Tabel 4 voor een overzicht). Door het uitnodigen van deze experts zorgen wij ervoor dat de aanbevelingen van het onderzoek aansluiten bij de dagelijkse praktijk en dilemma's van de medewerkers in de keten, alsmede bij wettelijke regelgeving en internationale verdragen en snelle ontwikkelingen in de tech-sector.

De expertmeeting was als volgt opgebouwd. Eerst gaven de onderzoekers toelichting op de achtergrond van het onderzoek en de eerste voorlopige resultaten. Daarna zijn de deelnemers opgedeeld in twee groepen om in gezamenlijkheid en vanuit de eigen functie te reflecteren op de beschreven voorlopige resultaten. Vervolgens is gediscussieerd over welke kennis over online rekrutering aanvullend noodzakelijk is en wat (ervaren) obstakels zijn in het voorkomen van online rekrutering. Tot slot vond er een terugkoppeling plaats naar de hele groep en werd plenair verder gediscussieerd.

Tabel 4. Overzicht deelnemers expertmeeting

Deelnemers	Beschrijving functie
Deelnemer 1	Expert op het gebied van ethiek en filosofie van technologie
Deelnemer 2	Onderzoeker op het gebied van maatschappelijke spanningen, polarisatiedynamieken en het samenleven van bevolkingsgroepen
Deelnemer 3	Onderzoeker op het gebied van online extremisme en het gebruik van computational linguistics
Deelnemer 4	Onderzoeker op het gebied van cybercriminaliteit en rekrutering
Deelnemer 5	Gemeente medewerker digitale weerbaarheid
Deelnemer 6	Gemeente medewerker digitale weerbaarheid
Deelnemer 7	Medewerker TER-team Reclassering Nederland

3.5 Privacy en ethiek

Voorafgaand aan de dataverzameling is in samenwerking met de datamanager van het NSCR een Data Protection Impact Assessment (DPIA) uitgevoerd. Tevens is een gegevensbeschermingseffectbeoordeling (Privacy Impact Assessment, PIA) opgesteld en door de Privacy Officer van het WODC goedgekeurd. Het onderzoeksvoorstel met het bijbehorende datamanagementplan is daarnaast voorgelegd aan de Commissie Ethiek van de Faculteit der Rechtsgeleerdheid van de Vrije Universiteit Amsterdam. De commissie heeft een positief advies over het onderzoek uitgebracht.

Interviews

De geïnterviewde respondenten worden in het rapport niet bij naam genoemd. Om hun anonimiteit zoveel mogelijk te waarborgen, worden alleen de organisaties vermeld waar de respondenten werkzaam zijn. Aanvullende informatie zoals de specifieke functies van respondenten of de regio's waarin zij werkzaam zijn, wordt om deze reden niet vermeld. De interviews zijn na toestemming van de respondenten (op basis van een informatieformulier en een *informed consent* formulier) opgenomen middels een beveiligde digitale recorder. In drie gevallen zijn de interviews niet opgenomen vanwege de functie van de respondent. Deze interviews zijn vastgelegd middels schriftelijke aantekeningen. De interviews zijn na afloop van het gesprek verbatim getranscribeerd of samengevat, gepseudonimiseerd en op een beveiligde server opgeslagen. Na afloop van de interviewperiode zijn de gepseudonimiseerde interviewtranscripten ter controle beveiligd toegestuurd aan de respondenten.

Contentanalyse

Sociale media bieden een unieke mogelijkheid om op een onopvallende en niet-invasieve manier menselijk gedrag te bestuderen, mits de onderzoeker zichzelf niet als zodanig onthult. Dit houdt ook in dat data wordt verzameld zonder informed consent van de respondenten. Gezien de grootte van sommige online gemeenschappen is het verkrijgen van informed consent vrijwel onmogelijk (Van Es & Schäfer, 2017). Aangezien op veel online platforms sprake is van onbeperkt lidmaatschap en gegevens openbaar worden gearchiveerd, kunnen daarnaast vraagtekens worden gesteld bij het hebben van privacy op deze platforms (Golder et al., 2017; Hudson & Bruckman, 2005). Gebruikers van online platforms kunnen hun privacy wel in bepaalde mate vergroten door bijvoorbeeld hun profiel of bepaalde (persoons)gegevens af te schermen. Het huidige onderzoek houdt zo veel mogelijk rekening met de privacy van gebruikers van de geanalyseerde platforms en daarom zijn de volgende voorzorgsmaatregelen genomen. Allereerst is alleen data uit openbare groepen of kanalen verzameld. Deze data zijn op een beveiligde server opgeslagen en na afloop van de onderzoeksperiode gewist. Privacygevoelige informatie zoals gebruikersnamen, bijnamen of groepsnamen zijn niet gebruikt in de rapportage. Deze informatie is gepseudonimiseerd en vervangen door een code. De informatie uit de contentanalyse wordt hoofdzakelijk op een geaggregeerd niveau gepresenteerd. Wanneer gegevens op individueel niveau worden gepresenteerd, is alle informatie die te herleiden is naar individuele personen verwijderd.

In de volgende twee hoofdstukken presenteren we de resultaten die voortkomen uit de verschillende onderzoeksmethoden. In hoofdstuk 4 gaan we in op de aard, mechanismen en doorwerking van online rekrutering. In hoofdstuk 5 beschrijven we bestaande maatregelen ter preventie van online rekrutering en gaan we in op handelingsperspectieven. Na de bespreking van de resultaten sluiten we het rapport af met hoofdstuk 6, waarin we de belangrijkste resultaten samenvatten en aanbevelingen doen voor vervolgonderzoek, beleid en de praktijk.

4. De aard, mechanismen en doorwerking van online rekrutering

Uit het literatuuronderzoek blijkt dat het empirisch onderzoek naar online rekrutering en aanverwante processen zich in de laatste jaren snel heeft uitgebreid. De meeste gepubliceerde studies hebben gebruik gemaakt van contentanalyses van overwegend openbare online platforms als onderzoeksmethode. Daarnaast zijn studies uitgevoerd op basis van interviews. Daarbij valt op dat de conceptuele onduidelijkheden die we eerder beschreven ook terug te zien zijn in de studies. Vaak lopen concepten door elkaar heen en wordt er bijvoorbeeld zowel naar radicaliseringsprocessen als naar rekrutering gekeken. Desalniettemin ontstaat op basis van de studies een beeld van de verschillende facetten van online rekrutering. De voor het huidige onderzoek afgenomen interviews en de uitgevoerde contentanalyse bieden vervolgens zicht op een aantal onderliggende mechanismen en op processen die doorgaans niet zichtbaar worden tijdens onderzoek op open platforms. In wat nu volgt bespreken we de gecombineerde bevindingen op basis van de literatuur, de interviews en de contentanalyse. Allereerst wordt in paragraaf 4.1 ingegaan op een aantal belangrijke verschillen tussen het online en offline domein als het gaat om rekrutering, en wordt uiteengezet *welke platforms* worden gebruikt door extremistische groepen en waarom. Vervolgens beschrijven we hoe online rekrutering verloopt. Daarbij onderscheiden we op basis van de verschillende methoden twee varianten; eerst bespreken we in paragraaf 4.2 generieke rekrutering voor extremistische groepen middels het vergroten van de aantrekkingskracht van een groep. In deze categorie vallen ook studies die inzoomen op het belang van netwerk- en gemeenschapsvorming en de creatie van narratieven. Daarna bespreken we in paragraaf 4.3 specifieke, op individuen en subpopulaties gerichte rekruteringsprocessen, waarbij mensen niet alleen worden gerekruteerd voor de groep zelf, maar ook voor bepaalde acties (bijvoorbeeld uitreizen). We bespreken hiervoor eerst een aantal internationale terroristische organisaties. Vervolgens zoomen we in op de Nederlandse context en beschrijven we hoe rekrutering via een trapsgewijs proces verloopt (paragraaf 4.3.2) en hoe doorlichtingsprocedures hier onderdeel van zijn (paragraaf 4.3.3). In paragraaf 4.4 beschrijven we de doelen van online rekrutering. We sluiten het hoofdstuk af met een analyse van de interactie tussen online en offline leefwerelden, waarbij we een onderscheid maken tussen situaties in de offline wereld die van belang kunnen zijn in de aanloop naar online rekrutering (4.5.1), de overgang van online rekrutering en groepsvorming naar 'onlife' rekrutering en online rekrutering en groepsvorming als voorfase van offline gewelddadigheden (4.5.3).

4.1 Verschillen tussen het online en offline domein en de faciliterende werking van verschillende soorten platforms

In deze paragraaf bespreken we eerst een aantal belangrijke verschillen tussen de online en offline wereld die van invloed zijn op rekruteringsprocessen. Vervolgens zoomen we in op verschillende soorten online platforms in relatie tot extremistische groepen.

4.1.1 Verschillen tussen het online en offline domein

In de afgelopen decennia is veelvuldig onderzoek gedaan naar radicalisering en rekrutering in de offline wereld, zoals ook beschreven in hoofdstuk 2. In datzelfde hoofdstuk werd ook geschreven over de functionaliteiten van sociale media, en waar die functionaliteiten aansluiten bij de leefwereld van internetgebruikers. Gedurende de interviews werd meermaals impliciet dan wel expliciet verwezen

naar het belang van deze functionaliteiten voor generieke en op individuen gerichte rekruteringsprocessen. Een aantal professionals gaf daarnaast meer in het algemeen aan hoe de online context verschilt van de offline context in relatie tot rekrutering voor extremistische groepen.

Online is 'easy in – easy out'

Allereerst werd door verschillende geïnterviewde professionals benoemd dat de drempel om online toe te treden tot een extremistische groep veel lager ligt dan offline (o.a. AIVD_1, LSE_1, politie_1). Tegelijkertijd is het ook eenvoudiger om je terug te trekken uit een groepering zonder dat daar grote consequenties aan vast zitten. Een respondent van de AIVD gaf als voorbeeld dat iemand voor een lange periode lid kan zijn van een extremistische Telegramgroep en er zelfs actief aan kan bijdragen door video's te monteren. Vervolgens kan diegene ook weer eenvoudig uit de Telegramgroep stappen door bijvoorbeeld te zeggen dat de politie aan de deur stond en dat hij/zij zich voorlopig gedeisd moet houden. Het online domein zorgt er met andere woorden voor dat deelname aan een extremistische groepering 'easy in and easy out' kan zijn. Hieraan gerelateerd stellen professionals vast dat aan online lidmaatschap in beginsel minder eisen worden gesteld. Online hoeven leden van groeperingen, in tegenstelling tot offline, niet gelijk 'vuile handen' te maken, en meer in het algemeen is een lager niveau van commitment vereist.

Gefragmenteerde identiteiten

Ten tweede werd het belang van de anonimiteit van het online domein door professionals meermaals benadrukt. Deze anonimiteit werkt twee kanten op; enerzijds draagt de mogelijkheid tot (in beginsel) anonieme aanwezigheid bij aan de laagdrempeligheid van posten in een groep (aansluitend bij het idee van 'easy in – easy out'). Anderzijds zorgt anonimiteit, of het aannemen van een andere identiteit, er ook voor dat iemand kan deelnemen aan een online extremistische groep zonder dat iemands offline sociale netwerk daar iets van hoeft te merken. Een respondent van LSE zegt hierover het volgende:

"Waar ik me elke keer over verbaas, is dat je een dossier hebt waarin je een bepaald beeld krijgt van iemand, terwijl in werkelijkheid als je hem dan ziet een totaal ander persoon voor je hebt, wat dus lijkt alsof er een gefragmenteerde identiteit ontstaat. Het ene moment is hij zo, het andere moment is hij zo. De omgeving herkent die persoon ook helemaal niet in wat in een dossier staat, qua beschuldigingen, uitspraken die iemand doet, omdat daar gewoon geen zicht op is en iemand echt de kans krijgt om online een heel ander persoon te zijn." (Respondent_LSE_1)

In het online domein zouden daarnaast minder richtlijnen bestaan over wat wel en niet aanvaardbaar is dan in de fysieke wereld. Het ontbreken van bepaalde gedragsregels in het online domein draagt bij aan het ontstaan van dergelijke gefragmenteerde identiteiten.

Internationale invloeden

Zoals in hoofdstuk 2 al naar voren kwam, maakt internet het mogelijk dat mensen elkaar eenvoudiger vinden en contact kunnen onderhouden. Dit heeft onder andere tot gevolg dat Nederlandse online groepen of Nederlandse leden van online groepen aangestuurd of gefinancierd kunnen worden vanuit het buitenland (respondent AIVD_1, ESS_2, gemeente_3, LSE_1, politie_1, politie_3). Ook komt het bijvoorbeeld voor dat extremistische groepen een buitenlandse spreker uitnodigen voor een lezing (interview ESS). Met name in de rekruteringsfase is het niet noodzakelijk dat leden van eenzelfde groepering of netwerk zich op fysieke nabijheid van elkaar begeven.

Online als vertekende weergave van de werkelijkheid

Tot slot kan het online domein een vertekend beeld geven van de cohesie, grootte en reikwijdte van een groepering. Meerdere respondenten geven aan dat het regelmatig voorkomt dat iemand lid is van een extremistische online groep, zonder ooit andere leden offline te hebben ontmoet of zelfs maar te weten wie de andere leden zijn. Ook kunnen likes en volgers online gemanipuleerd worden, waardoor het aantal aanhangers van een gedachtegoed groter lijkt dan het in werkelijkheid is.

4.1.2 De faciliterende werking van verschillende soorten platforms

Volgens de in Hoofdstuk 2 besproken theoretische modellen (het 'bouwstenen-model en het 'online affordances-model') biedt internet diverse functionaliteiten die online rekrutering kunnen faciliteren. Er zijn echter veel verschillende platforms, met verschillende functionaliteiten. Het is daarom belangrijk om ook te beschouwen welke platforms doorgaans door extremistische groepen worden gebruikt, en waarom. Uit de literatuur blijkt dat extremistische groepen gebruik maken van een scala aan online platforms, waaronder *mainstream* sociale mediaplatforms zoals Facebook, X (voorheen Twitter), TikTok, Instagram en YouTube (Frischlich et al., 2022; McSwiney, 2021; Pohl & Riesmeyer, 2023; Scrivens & Conway, 2019; Vacca, 2019). Deze platforms hebben precies de eerder besproken kenmerken die het voor extremistische groepen aantrekkelijk maken om ze in te zetten voor rekrutering en mobilisering, waaronder de mogelijkheid om eenvoudig content uit te wisselen en samen te komen met gelijkgestemden via online groepen, kanalen of pagina's. Op het merendeel van bovengenoemde platforms (behalve YouTube) bestaat daarnaast de mogelijkheid om andere gebruikers één-op-één privéberichten te sturen via *direct messaging* (DM). Deze functionaliteit vergemakkelijkt direct contact tussen rekruteurs en potentiële rekruten, waardoor extremistische groepen kunnen overgaan tot *micro-targeting*, ongeacht de geografische afstand tussen beiden (Vacca, 2019).

Elk platform zit echter weer net iets anders in elkaar, waardoor platforms op verschillende manieren worden ingezet. Op X (voorheen Twitter) wordt bijvoorbeeld meer dan op andere platforms gebruik gemaakt van hashtags, waardoor berichten over hetzelfde onderwerp gebundeld worden en snel te vinden zijn. Deze functionaliteit heeft extremistische groepen niet alleen in staat gesteld om eenvoudig met gelijkgestemden in contact te komen, maar ook om hun gedachtegoed te verspreiden onder gebruikers die er niet naar op zoek waren (Vacca, 2019). Zo werden hashtags als #MeToo en #BlackLivesMatter in het verleden 'gekaapt' door extreemrechtse en rechtsextremistische groepen (Kim & Lee, 2021; Maricourt & Burrell, 2022). Waar X de nadruk legt op tekstuele berichten, is de content op Instagram visueler van aard. Extremistische groepen spelen hierop in door aan te haken op de 'Instagram aesthetic' en hun berichten op een visueel aantrekkelijke manier te presenteren (Pohl & Riesmeyer, 2023), iets wat bijvoorbeeld is terug te zien bij een groepering als Proud Boys (zie 4.2). Verder maken vrijwel alle sociale mediaplatforms gebruik van bepaalde algoritmes. Platforms als YouTube en TikTok staan het meest bekend om hun algoritmes. De manier waarop deze platforms zijn ontworpen, zorgt ervoor dat gebruikers steeds extremere content krijgen aangeboden gerelateerd aan een onderwerp waar ze op enig moment interesse in hebben getoond door bijvoorbeeld een video te liken maar ook als ze er langer dan gemiddeld naar hebben gekeken (Vacca, 2019).

De toenemende aanwezigheid van extremistische groepen en -individuen op online platforms in combinatie met de steeds grotere druk vanuit overheden en instanties om op te treden, zorgde ervoor dat sociale mediabedrijven als X, Instagram en Facebook zich vanaf ongeveer 2016 steeds meer gingen

richten op content moderatie. Zo meldde Twitter (nu X) in februari 2016 dat zij 125.000 accounts had geschorst wegens het dreigen met of promoten van terroristische acties. In de daaropvolgende jaren werd de content moderatie van *mainstream* platforms verder opgevoerd. Dit was een traag proces dat pas plaatsvond nadat enorme hoeveelheden extremistisch materiaal al was verspreid in het online domein (Vacca, 2019). Bovendien is Twitter's beleid rondom het tegengaan van dergelijke content flink teruggeschroefd sinds de overname door Elon Musk in 2022 (Arun et al., 2024).

Vanwege de inzet op content moderatie door diverse platforms hebben veel extremistische groepen zich verplaatst naar 'low profile' platforms zoals Telegram (Scrivens & Conway, 2019). In tegenstelling tot platforms als Facebook en Instagram, doet Telegram in veel mindere mate aan content moderatie. De oprichters van Telegram schermen met de veelvuldigheid aan privacy maatregelen die het platform heeft, waaronder encryptiesoftware en de mogelijkheid om geheime berichten te versturen die na een bepaalde tijdsperiode automatisch worden vernietigd (Bloom et al., 2019; Walther & McCoy, 2021).

Uit de door ons gehouden interviews komt naar voren dat Telegram momenteel het meest gebruikte platform door extremistische groeperingen is. Het overgrote deel van de respondenten wees Telegram aan als het belangrijkste platform in relatie tot online radicalisering-, rekruterings- en mobiliseringsprocessen. De populariteit van Telegram onder extremistische groeperingen zou inderdaad voornamelijk te wijten zijn aan de verscheidenheid van beveiligingsmaatregelen, privacyrichtlijnen en het feit dat het Telegram in tegenstelling tot andere sociale media platforms nauwelijks aan content moderatie lijkt te doen. Naast Telegram worden Facebook, TikTok, Instagram, X (voorheen Twitter) en Discord het vaakst genoemd door respondenten. Tussen deze platforms zouden verschillen bestaan in de doelgroep die er gebruik van maakt, de content die erop wordt geplaatst en de functie die de platforms innemen binnen extremistische groeperingen. Zo merken meerdere respondenten op dat op Facebook doorgaans een oudere leeftijdsgroep actief is dan op Telegram en TikTok. Daarnaast verschilt de aard van de content vaak per platform. Een medewerker van de politie zegt hierover het volgende als het gaat om jihadistische content:

> *"Op Facebook zie je wel preken, de oproepen tot doneren, de oproepen tot bidden voor, tot je steun uitspreken voor, en verwijzingen dus naar Telegram. Het feit dat men op Facebook verschillende profielen in stand kan houden, heeft ook te maken met dat ze met heel veel omhaal van woorden [berichten plaatsen] en de theologische onderbouwing. Terwijl je op Telegram meer direct instructiemateriaal hebt en oproepen tot. Daar heb je ook wel theologische onderbouwing, maar zeker ook in combinatie met korte instructies tot bommen maken, messen pakken, auto's en aan de slag. Dat zie je natuurlijk op Facebook niet want dan verdwijn je heel snel ervan."*
> (Respondent_politie_3)

Uit bovenstaand citaat blijkt dat Facebook kan fungeren als een soort doorgeefluik naar Telegram. Dit is iets dat andere professionals ook terugzien. Platforms als Facebook, Twitter en Instagram worden steeds vaker gebruikt om potentiële nieuwe leden door te verwijzen naar bepaalde (besloten) Telegramgroepen of -kanalen, servers of websites. Uit de contentanalyse blijkt overigens dat dit andersom ook het geval is. Geregeld worden verwijzingen gedaan naar andere openbare platforms, met name naar Facebook, Telegram en websites. Verder wordt verwezen naar platforms als TikTok, YouTube, Instagram, Twitter en LinkedIn.

Het verwijzen naar andere platforms gebeurt voor het grootste gedeelte in een van de anti-institutionele groepen (groep 4), waarin vaak onder een gedeelde video links staan naar andere platforms waarop de groep actief is.

Hoewel er vanuit de literatuur en op basis van de interviews consensus lijkt te bestaan over de belangrijke faciliterende rol van bepaalde platforms, met name Telegram, is meer onduidelijkheid over een ander veelgenoemd domein, namelijk gamingplatforms. De laatste jaren bestaan er toenemende zorgen over de mogelijke rol die gamingplatforms spelen in de aanloop naar extremisme en terrorisme. Extremistische groepen zouden deze platforms niet alleen kunnen inzetten voor het verspreiden van propaganda (Lakomy, 2019) maar ook voor rekrutering (EU, 2020; Europol, 2021). Hierbij wordt gewezen op extremistische groepen die hun eigen games ontwikkelen en groepen die bestaande games aanpassen ('modding') om het publiek te radicaliseren, maar ook op groepen die leden rekruteren via in-game chatfuncties en gamification (Rosenblat & Barrett, 2023; RAN, 2020). Diverse veiligheidsdiensten hebben in de afgelopen tijd melding gemaakt van specifieke radicaliserende activiteiten op gamingplatforms. Zo maakte de Australische federale politie in december 2023 melding van een snelle toename van het aantal kinderen dat via gaming platforms werd geradicaliseerd of gerekruteerd. De organisatie ontdekte dat op één van de onderzochte platforms, Roblox, veelvuldig games werden geprogrammeerd waarin extremistische narratieven worden verspreid, spelers gewelddadig extremistische gebeurtenissen of aanslagen kunnen naspelen (zoals de aanslag in Christchurch), propaganda wordt gedeeld, jongeren worden gerekruteerd en soms zelfs fondsen worden geworven (AFP, 2023). Ook de NCTV waarschuwde recent voor de faciliterende werking van gamingplatforms, en ook hier werd specifiek naar Roblox verwezen (DTN58). De NCTV schrijft hierover: "… ISIS benut het gebrekkige toezicht in de online gamesector om hun desinformatie en propaganda te verspreiden. Op het gameplatform Roblox konden nazistische gebruikers bijvoorbeeld lhbtiq+-symbolen aanvallen en specifiek voor Nederland is aldaar een spel ontdekt, waarin men als ISIS-terrorist politieagenten kon aanvallen" (p. 35). Hoewel deze berichten met name lijken te wijzen op mogelijke radicaliserende invloeden via de verspreiding van extremistische narratieven en propaganda, wordt dus ook genoemd dat via de platforms mogelijk mensen worden gerekruteerd voor extremistische groepen. Uit de interviews blijkt echter dat de organisaties hier nog onvoldoende zicht op hebben. Het beeld dat ontstaat is dat veel professionals weten dat het gebeurt, maar waar precies, en hoe, dat is onduidelijk. Een respondent van de politie zegt hier het volgende over:

"Ik weet dat het gebeurt maar hoe exact durf ik niet te zeggen. We weten dat de propaganda circuleert en dat het ook een manier is om mensen weer op andere platforms verder te krijgen, maar ik heb er zelf niet een heel goed beeld van. […] Er waren altijd wel ideeën dat men het kon gebruiken om onderling te communiceren met wie men al kende. Nu blijkt dat het inderdaad ook gebruikt wordt om onbekenden wellicht te beïnvloeden." (Respondent_politie_3)

4.2 Generieke rekrutering: gericht op breed publiek en groepsvorming

Uit het bovenstaande blijkt dat verschillende platforms worden gebruikt door extremistische groepen voor verschillende activiteiten, waaronder rekrutering. De vraag is vervolgens hoe die rekrutering verloopt. Zoals gezegd is 'generieke rekrutering', waarbij extremistische groepen zich richten op het aantrekken van een brede waaier aan potentiële rekruten, één van de varianten. Uit diverse studies blijkt dat extremistische groepen sociale media met name gebruiken om aan 'community building' te

doen en om internetgebruikers in het algemeen aan de groep te verbinden. Belangrijke aspecten van groepsvorming zijn het bevorderen van sociale cohesie binnen de groep, de vorming van een gedeeld narratief en het hebben van een gezamenlijk doel (Gaudette et al., 2022; Kutner, 2020; DeCook, 2018). Binnen rechtsextremistische groeperingen wordt de "us vs. them" dynamiek binnen de groep bevorderd door het gebruik van memes met een vaak haatdragende boodschap over gemarginaliseerde groepen (Kutner, 2020). Memes zijn humoristische afbeeldingen, video's of teksten die in het online domein worden verspreid en hergebruikt worden door individuen en groepen (Shifman, 2013). Memes worden gezien als een vorm van politieke participatie en een belangrijk onderdeel van online gemeenschapsvorming (Mina, 2018; Nagle, 2017; Shifman, 2013).

Een voorbeeld van een extremistische groep die inzet op generieke rekrutering via groepsvorming is Proud Boys. Deze groepering onderscheidt zich van andere neo-conservatieve bewegingen door hun veelvuldige en strategische gebruik van sociale media (DeCook, 2018) en derhalve bespreken we de strategie van deze specifieke groep, die overigens geen onderdeel uitmaakt van de content-analyse van het huidige onderzoek, wat uitgebreider. Provocatie is een centraal onderdeel van de online rekruteringsstrategie van Proud Boys. Leden van Proud Boys mengen zich in gesprekken op sociale media om anderen doelbewust te provoceren en vervolgens in hun eigen online groepen te vieren dat ze de desbetreffende persoon hebben 'getriggerd'. Wanneer hun tactiek of ideologie wordt bekritiseerd door anderen, spelen ze in op hun eerdergenoemde slachtofferstatus, om vervolgens gezamenlijk de betreffende perso(o)n(en) online te rapporteren, bedreigen of intimideren (Kutner, 2020). DeCook (2018) analyseerde het online gedrag van Proud Boys op Instagram en bracht in kaart hoe de groepering memes en andere content inzet om hun identiteit en ideologie te verspreiden en zo nieuwe leden te rekruteren. De data werden verzameld in een periode van drie maanden door te zoeken naar hashtags en accounts die relevant zijn voor Proud Boys en de grotere, aanverwante Alt-Right beweging. De bevindingen laten zien dat er diverse performatieve en taalkundige symbolen zijn die bijdragen aan de identiteit en acculturatie van Proud Boys, waaronder het gebruik van de Pepe the Frog cartoon, uitdrukkingen als 'Deus Vult' om het christelijke element van de groep te benadrukken, en foto's van Proud Boys tatoeages, die niet alleen hun rang in de groepering symboliseren maar die samen met de andere symbolen ook een esthetische functie hebben. Leden van Proud Boys creëren ook memes die hun ideaalbeeld van de sociale wereld weergeven, om vervolgens deze memes op te leggen aan anderen die openstaan voor hun boodschap. DeCook (2018) kwam bij Proud Boys op Instagram memes tegen waarbij de tekst 'West is the Best' veelvuldig werd gebruikt, een tekst die wordt gezien als het mantra van Proud Boys. Daarnaast worden symbolen van Amerikaanse masculiniteit gebruikt in hun rekruteringsmemes, zoals afbeeldingen van Uncle Sam en Jack Daniels whisky.

Vergelijkbare bevindingen komen naar voren in het onderzoek van Roks en Van der Schoot (2019) op basis van een exploratieve analyse van de wijze waarop drie rechts-extremistische groeperingen gebruik maken van sociale media. Uit hun onderzoek blijkt dat deze platforms worden gebruikt 'om hun ideologie uit te dragen, een groepsidentiteit te construeren en op te roepen tot (democratische) vormen van verzet' (p. 225). De creatie van een dergelijke groepsidentiteit lijkt met name belangrijk en aantrekkelijk voor individuen die zelf zoekende zijn naar hun identiteit. Peeters, Van Wonderen, Burggraaff en De Wit (2023) wijzen in dit opzicht op de belangrijke bijdrage die sociale media platforms leveren aan de ontwikkeling van een individuele identiteit. In hun onderzoek naar online extreemrechtse radicalisering benoemen de auteurs dat extreemrechtse groepen jongeren voor zich

proberen te winnen ‘door de vorm aan te nemen van ‘counterculture movements’ die focussen op lifestyle, jeugdcultuur en kunst’ (p.12).

De interviews die voor dit onderzoek zijn uitgevoerd, bieden nog meer inzichten in generieke rekruteringsprocessen en het belang van sociale media voor de groepsvorming van extremistische groepen. Zo gaven professionals uit het veiligheids- en maatschappelijke domein (o.a. politie_1, gemeente_3, LSE_1) aan dat mensen die lid worden van online groepen een behoefte hebben om ergens bij te horen en dat ze daarnaast worden aangetrokken door het duidelijke wereldbeeld en vaak samenhangend handelingsperspectief dat een extremistische groep te bieden heeft. Dit zou voor verschillende ideologische stromingen gelden:

“Het is menselijk om toch ergens bij te willen horen. Dat hebben we ook binnen jihadisme gezien. De psychologische processen zijn niet heel anders.” (Respondent_gemeente_3)

Een aantal respondenten noemde voorbeelden waaruit bleek dat extremistische groepen in het online domein aan groepsvorming doen. Zo wezen medewerkers van de politie en AIVD op het feit dat de ‘us vs. them’ dynamiek in sommige online groepen duidelijk naar voren komt als er bepaalde termen worden gebruikt voor buitenstaanders, waaruit kan worden afgeleid welke mensen wel en niet als onderdeel van de groepering of ‘passend’ bij het gedachtegoed worden gezien.

Eerder werd benoemd dat het gebruik van humor en memes centraal staat in de groepsvorming van de Proud Boys. Recentelijk publiceerde de NCTV een fenomeenanalyse waarin wordt beschreven welke rol memes hebben voor extreemrechts (NCTV, 2024). Het gebruik van humor was een terugkerend onderwerp tijdens de interviews. Daarbij ging het ook om de vraag of er verschillen op te merken zijn tussen verschillende ideologische groepen. Een aantal respondenten beschreef de ervaring dat in jihadistische groepen, in tegenstelling tot andere ideologische groepen, humor weinig werd ingezet, terwijl andere respondenten het idee hadden dat linkse groepen juist weinig gebruikmaken van humoristische content zoals memes. Een meerderheid van de respondenten was van mening dat het gebruik van humor en memes met name binnen rechts-extremistische groepen een belangrijke rol vervult, waarmee ze aansluiten bij het beschreven onderzoek naar de Proud Boys. Opvallend is echter dat op basis van de contentanalyse wel degelijk duidelijk wordt dat in alle bestudeerde online groepen humoristische content wordt geplaatst. Zo wordt er in een van de jihadistische groepen (groep 5) een reactie gedeeld van een X/Twitter-account dat reageert op een Tweet van Joe Biden (“The United States stands with the people of Israel”) met “habibi learn to stand first” en vier verschillende foto’s van Joe Biden die struikelt. In de extreemlinkse groep (groep 7) wordt de ‘Anime Girl Hiding from Terminator Meme’ gedeeld waarin het meisje wordt aangeduid als ‘Sjerry Bidet’ en de Terminator als ‘Antifa parapluminator’.

Zoals gezegd wordt de ideologie van de groepen actief verspreid in de verschillende groepen. Hiervoor worden teksten gebruikt, maar ook afbeeldingen en video’s. Zo gaat in de berichten van een van de anti-institutionele groepen veel aandacht uit naar verschillende overheden, die corrupt en crimineel zouden zijn. Hierbij worden diverse geluids- en videofragmenten gedeeld waarin dit narratief naar voren komt. In één van de audio-opnames wordt oorlogsterminologie gebezigd, iets wat we ook terugzien in een van de extreemrechtse groepen en in de jihadistische groepen:

"We zijn in een oorlog. Wij moeten met z'n allen druk zetten. In een oorlog moet je bereid zijn een offer te doen. Dat je weet dat het niet zonder slag of stoot gaat." (Groep 3)

Interessant is dat meerdere geanalyseerde groepen reclame maken voor andere groepen met eenzelfde ideologie. Er wordt bijvoorbeeld bekendheid gegenereerd door een kort bericht door te sturen over het doel van de andere groepering, of door een evenement te promotoren dat door de andere groepering georganiseerd wordt, zoals dit doorgestuurde bericht in (extreemrechtse) groep 1: *"[naam kanaal] is a channel focused on current events within the Netherlands as well as within the international sphere. Our posts will be focused on news, discourse and ideology. @[kanaal]"* of dit gedeelde bericht in (extreemlinkse) groep 7: *"Onze vrienden van [andere groep] organiseren [datum] een informatie- en benefietavond. [toelichting over de groep en het programma van de avond] Zeker de moeite waard!"*

Hoewel dergelijke berichten het bereik van de verschillende groepen kunnen vergroten en mogelijk nieuwe leden kan aantrekken, plaatst een respondent van de AIVD een kanttekening bij de online groepsvorming van extremistische groepen. Het online domein zou er namelijk voor zorgen dat de onderlinge samenhang van een groepering sterker kan lijken dan zij in werkelijkheid is. Zo kan het zijn dat iemand die lid is van een extremistische online groep de identiteit van andere leden niet kent, iets wat al werd benoemd in 4.1.1. Eenzelfde beeld komt naar voren in studies naar de Proud Boys. Proud Boys heeft verschillende online gemeenschappen waarin voornamelijk mannen hun radicale ideeën steeds verder ontwikkelen en offline acties kunnen voorbereiden (Kutner, 2020). In het artikel van Kutner (2020) worden deze online gemeenschappen niet nader gedefinieerd. Het is dus niet duidelijk of het gaat om officiële online platforms van de groepering, losse netwerken of aanhangers die online berichten plaatsen. Niet iedereen die online berichten plaatst over Proud Boys, hoeft namelijk lid te zijn van een dergelijke online gemeenschap, blijkt uit de studie van Nguyen en Gokhale (2022). Zij deden onderzoek naar de online dialogen rond acties van Proud Boys en vonden dat de netwerkstructuur van Proud Boys een lage dichtheid had, wat suggereert dat niet alle individuen die online berichten plaatsen over Proud Boys lid zijn van de groepering of zelfs online communiceren met gelijkgestemden. Dit is een belangrijke bevinding, omdat ze het door extremistische groepen voorgestelde plaatje van hechte groepen met een gedeelde ideologie nuanceert. Meer in het algemeen sluit deze bevinding aan bij studies naar online netwerken die aantonen dat dergelijke netwerken doorgaans veel diffuser en meer fluïde zijn dan offline netwerken. Zoals volgt uit de in hoofdstuk 2 geschetste theoretische modellen zijn het juiste deze kenmerken, en dan met name functionaliteiten als anonimiteit en a-synchroniteit, die de aantrekkingskracht van dit soort online gemeenschappen vergroot. Tegelijkertijd zijn het dezelfde kenmerken die maken dat de groepen ook kwetsbaar zijn, omdat leden 'easy in – easy out' kunnen zijn (zie ook 4.1.1).

4.2.1 Offline groepsvorming

Een manier om om te gaan met deze fluïditeit lijkt te zijn dat groepen in toenemende mate willen laten weten en zien dat ze ook in de offline wereld bestaan. Dit beeld komt zowel uit de interviews als de contentanalyse naar voren. Zo gaf een medewerker van de politie (politie_1) aan dat sommige online gemeenschappen op een gegeven moment de openbaarheid opzoeken en op verschillende platforms beeldmateriaal verspreiden van extremistische symboliek waarmee aandacht wordt gegenereerd voor het bestaan van de groep en het feit dat ze offline samenkomen. Dergelijke berichten dienen een bekrachtigende functie en creëren een gevoel van verbondenheid. Een duidelijk voorbeeld is een op

het platform gedeeld fragment van een Nederlands nieuwsprogramma waarin aandacht wordt besteed aan de groepering. Op deze post wordt door veel volgers gereageerd middels likes en emoji's. Andere voorbeelden:

"[Foto's] Leden op hun recente wandeltocht […] Onze [lokale afdelingen] houden maandelijkse uitjes en activiteiten. Word ook deel van ons broederschap, stuur een bericht naar [mailadres]" (groep 1, extreemrechts)

"[datum] organiseer ik een avond waarin je in plaats van zoomen fysiek aanwezig kunt zijn met een hapje en een drankje en vooral lekker kletsen met elkaar want ik voel die behoefte wel en ik hoop jullie ook." (groep 4, anti-institutioneel)

De door ons uitgevoerde contentanalyse illustreert het proces van groepsvorming middels de constructie van een gedeeld narratief en groepsactiviteiten. Het valt op dat alle onderzochte online groepen activiteiten organiseren, uiteenlopend van lezingen tot gezamenlijk sporten en protesten. Lezingen en presentaties lijken de meest voorkomende activiteiten te zijn onder de anti-institutionele, jihadistische en extreemlinkse groepen. De twee extreemrechtse groepen plaatsten in de onderzochte periode geen berichten over lezingen of presentaties, maar wel over andere soorten offline samenkomsten. Een andere activiteit die we terugzagen bij meerdere online groepen was gezamenlijk sporten, meer specifiek het gezamenlijk trainen in MMA/grappling. Hierover werd in zowel extreemrechtse als in jihadistische groepen berichten geplaatst.

Uiteindelijk wordt in verschillende onderzochte groepen ook daadwerkelijk een algemene oproep gedaan om lid te worden van de groep. Tijdens de onderzoeksperiode werden dergelijke oproepen met name in de extreemrechtse groepen en in een anti-institutionele groep geobserveerd, zoals: *"Wordt ook lid, meld je aan [link naar Telegramgroep]"* (groep 1) *en "Meld je anoniem aan via [link] of sluit je aan via [andere chatgroep] en stuur 'ik wil actief worden'"* (groep 2). Dergelijke brede uitnodigen voor lidmaatschap of deelname zijn gericht aan mensen die al lid zijn van de openbare online groep of die de groep volgen. Het gaat hierbij dus om het binnenhalen van individuen die al interesse hebben getoond in de groepering. Op basis van de geanalyseerde berichten wordt echter niet duidelijk wat lidmaatschap specifiek inhoudt en welke voorwaarden eraan vastzitten. Ook oproepen tot betrokkenheid bij activiteiten worden op vergelijkbare algemene wijze binnen de groepen gedeeld: *"Zoek in je omgeving mensen die ons helpen, die ook filmpjes willen maken […] In volle vaart vooruit!"* (groep 4).

Opvallend is dat in de geanalyseerde jihadistische groepen minder vaak oproepen tot actie of betrokkenheid worden gedaan dan in de andere geanalyseerde groepen. Daarnaast lijkt er in de jihadistische groepen meer te worden gehint op bepaalde acties zonder het daadwerkelijk te benoemen:

"Er is maar één oplossing voor de moslims, en we weten allemaal welke dat is, wie ermee bezig is, wat het vereist en wat ervoor nodig is. Kun je daar niets aan bijdragen, wees dan geen stem van zwakte en zieligheid, want we zijn in oorlog." (groep 6)

4.3 Specifieke rekrutering: gericht op subpopulaties en individuen

Naast generieke rekrutering ("kom bij de groep") maken groepen ook gebruik van op specifieke subpopulaties of individuen gerichte rekrutering voor groepen en activiteiten. Wetenschappelijk onderzoek naar specifieke rekrutering is tot op heden met name gericht op strategieën van de grotere internationale terroristische organisatie, zoals Al Qaida en IS. Uit de gevoerde interviews blijkt echter dat ook Nederlandse extremistische groepen of Nederlandse takken van internationale groepen meer gerichte rekrutering gebruiken. In wat nu volgt bespreken we eerst het gebruik van specifieke rekruterings-strategieën gericht op subpopulaties door grote internationale terroristische organisaties. Vervolgens zoomen we op basis van de interviews in op de Nederlandse context en rekrutering gericht op specifieke individuen. Hier beschrijven we hoe rekrutering kan worden gezien als een trapsgewijs proces, waar doorlichtingsprocedures een belangrijke rol in spelen.

4.3.1 Specifieke rekrutering door internationale terroristische organisaties

Diverse internationale terroristische organisaties gebruiken internet om bepaalde subpopulaties, zoals minderjarigen of vrouwen, te bereiken en hen vervolgens met doelgerichte rekruteringsstrategieën over te halen om zich aan te sluiten bij de organisatie. Dit is een proces dat ook wel 'narrowcasting' wordt genoemd (Bigio & Vogelstein, 2019; Ingram, 2016; Weimann, 2016). Deze methode springt vooral in het oog bij de rekrutering door en voor een aantal jihadistische groepen, zoals Al Qaida en Islamitische Staat. Voor deze wereldwijd opererende groepen geldt dat internet, en met name sociale media, een cruciale rol heeft gespeeld in de rekrutering van strijders. Al Qaida en IS zetten zowel in op generieke als actieve rekruteringsmethoden- en strategieën en aangezien er overlap bestaat tussen beide categorieën, bespreken we ze hier gezamenlijk.

Ondanks Al Qaida's afkeer tegen ontwikkelingen als modernisering en globalisering, die volgens aanhangers een bedreiging vormen voor het vasthouden aan een meer traditioneel bestaan, heeft de organisatie vrij snel internet omarmd als onderdeel van hun (rekruterings-)strategie (Guadagno et al., 2010). Eerder werd benoemd dat het grote bereik van internet diverse voordelen biedt ten opzichte van de offline wereld, en met de komst van internet was het voor extremistische organisaties zoals Al Qaida ineens mogelijk om potentiële rekruten uit alle delen van de wereld aan te trekken. Voorheen hadden enkel extremistische groeperingen met toegang tot een bepaald grondgebied en een grote hoeveelheid aanhangers een zekere mate van 'command and control' waardoor ze specifieke individuen konden rekruteren op basis van hun talenten. Al Qaida maakte hier bijvoorbeeld gebruik van door zich te richten op potentiële rekruten van technische universiteiten (Bloom, 2017). De komst van internet heeft deze processen vergemakkelijkt en het bereik vergroot. Online rekruteringsmateriaal werd vaak vertaald in vele talen waaronder in het Engels en Frans, in een poging om sympathisanten uit Westerse landen te rekruteren die beter toegang hadden tot bepaalde doelwitten (Guadagno et al., 2010).

Ook IS heeft veel successen geboekt op het vlak van online rekrutering en mobilisatie. Deze groep is er niet alleen in geslaagd om een grote hoeveelheid lokale strijders te rekruteren, maar ook tal van *foreign fighters* uit verschillende Europese landen en Noord-Amerika. Sociale media speelden een grote rol in de rekruteringsstrategie van IS (Vidino & Hughes, 2015; Whittaker, 2021). De groepering investeerde in een breed scala aan online platforms en content en heeft zelfs een speciale media productie-eenheid voor rekrutering uit Westerse landen. Net als Al Qaida, verspreidt IS extremistische

content in verschillende talen om een zo'n groot mogelijke doelgroep te bereiken (Aly et al., 2017; Weimann, 2016). Een veelvoorkomende tactiek van IS voor de online rekrutering van *foreign fighters* was het inschakelen van eerder gerekruteerde individuen om anderen over te halen zich aan te sluiten. Zo werd bijvoorbeeld in 2014 een video gedeeld op sociale media van *foreign fighters* die hun paspoorten verscheurden en anderen in hun moedertaal opriepen om zich aan te sluiten bij IS (Weimann, 2016).

Naast het gebruik van sociale media, speelden de rekruteringsnarratieven van IS een belangrijke rol bij het aantrekken van grote aantallen foreign fighters. IS gebruikte zeker in de periode direct na het uitroepen van het kalifaat Hollywood-achtige narratieven voor hun propagandaberichten. Zo gebruiken ze bijvoorbeeld heroïsche martelaarsnarratieven, die zich richtten op persoonlijke glorie en empowerment van een individu, in aanvulling op traditionele martelaarsnarratieven, waarbij de nadruk ligt op de plicht tot religie en verwantschap (Yoder et al., 2020). De mediastrategie van IS vermengt narratieven van bruut geweld met utopisch idealisme (Aly, 2017). Enerzijds wordt de nadruk gelegd op geweld, strijdlust en grieven van potentiële rekruten. Anderzijds wordt er veel aandacht besteed aan de positieve aspecten van deelname aan IS (Mitts et al., 2022). Rekruteringsvideo's van IS zetten *foreign fighters* vaak neer als heldhaftig, gelukkig, succesvol en glamoureus, en proberen de kijker te overtuigen van het goede leven dat iemand binnen het Kalifaat kan leiden. IS wordt neergezet als een legitieme organisatie die betekenisvolle kansen biedt, voldoende middelen heeft, en militair bekwaam is (Weimann, 2016; Windisch et al., 2018; Zelin, 2015). Het feit dat IS in het verleden zo veel nadruk legde op de sociale en materiele voordelen van lidmaatschap, kwam voor een groot deel omdat IS een functionerende staat had. Nu IS geen grondgebied meer heeft, kan hun retoriek mogelijk verschuiven naar een meer grieven-georiënteerde strategie, die erop gericht is de verloren glorie van het kalifaat terug te winnen (Rousis et al., 2022).

Zowel Al Qaida als IS heeft op subgroepen toegespitste rekruterings-strategieën ('narrowcasting') ingezet. Al Qaida zocht via het online domein rechtstreeks contact met minderjarigen, waarbij zij werden aangemoedigd om niet bij hun ouders te blijven en 'de luxe van thuis en het stadsleven in te ruilen voor jihad, net zoals de profeet Mohammed hen was voorgegaan' (Lennings et al., 2010; Weimann, 2016). Deze online propaganda gericht op minderjarigen nam de vorm aan van cartoons, muziekvideo's, strips of computerspellen. Vaak werden cartoons of kinderverhalen vermengd met extremistische narratieven. Al Qaida probeerde bijvoorbeeld kinderen te bereiken door middel van games die geweld verheerlijken en waarbij oorlogen worden gevoerd tegen internationale troepen (Weimann, 2016).

Ook vrouwen zijn een belangrijke doelgroep geweest voor specifieke rekruteringsstrategieën. Vrouwen werden vanaf 2014 door IS gerekruteerd voor verschillende rollen, van ondersteunende rollen tot grotere operationele rollen en bleken vooral zelf efficiënt als rekruteurs. Uit een studie van Manrique en collega's (2016) over online IS groepen kwam naar voren dat vrouwelijke rekruteurs een hogere netwerkdichtheid hebben dan mannen, waardoor ze doeltreffender zijn in het verspreiden van de boodschap van IS dan hun mannelijke tegenhangers. Door de deelname van vrouwen bleek ook de levensduur van online IS groepen toe te nemen, omdat het langer duurde totdat de groepen offline werden gehaald door platforms (Bigio & Vogelstein, 2019).

Dezelfde propaganda en extremistische narratieven die mannelijke (foreign) fighters leken aan te trekken werden vertaald naar een vrouwelijk publiek. Daarbij kwam de nadruk te liggen op de 'Muslim cause', een nieuwe 'utopische' staat, en jihadisten die bereid zijn om martelaren te worden als verplichting aan God. Sommige vrouwen zouden aangetrokken worden door een geromantiseerd beeld van 'het zijn van een vrouw van een jihadist die vecht voor het ultieme doel: het kalifaat' (Aly, 2017). De rekruteringsstrategie van IS om Westerse vrouwen aan te trekken, legde de nadruk op vriendschap, 'sisterhood' en mogelijkheden om te genieten van vrijheid en avontuur als leden van IS (Bigio & Vogelstein, 2019). Op sociale media werden afbeeldingen verspreid van IS-vrouwen die werkten als verpleegsters, leraren of politieagenten. Hierdoor trokken honderden westerse moslimvrouwen naar Syrië om 'hun religie uit te oefenen in een gunstige omgeving (Peresin, 2015; Valentini, Lorusso & Stephan, 2020). Zowel Al Qaida als IS wendde zich ook middels online magazines specifiek tot vrouwen (Weimann, 2016).

4.3.2 Zicht op de Nederlandse context: Een trapsgewijs proces van generieke naar specifieke rekrutering

Hoewel het bovenstaande interessante inzichten oplevert ten aanzien van online rekrutering door internationaal opererende terroristische groepen en organisaties, zijn deze niet a priori vertaalbaar naar de Nederlandse context. Er zijn immers verschillen tussen extremistische groepen, onder meer ten aanzien van het karakter van de groepering, de organisatiegraad, het bereik, en de doelen. Daarnaast zijn er ook *tussen* de groeperingen die in Nederland actief zijn verschillen. De studies geven bovendien relatief weinig informatie over verschillende fasen van rekrutering. De door ons uitgevoerde contentanalyse gaf enkel inzicht in beginfasen van rekrutering, aangezien er alleen naar openbare groepen is gekeken. De voor dit onderzoek gehouden interviews met professionals werpen echter wel licht op de verschillende fasen van rekrutering zoals zichtbaar in extremistische groepen vanuit de verschillende onderzochte stromingen.

Allereerst komt uit de interviews naar voren dat situaties waarin extremistische organisaties doelgericht op zoek gaan naar specifieke rekruten, of situaties waarin personen in eerste instantie offline in contact komen met extremistische groepen, in elk geval op dit moment en binnen de Nederlandse context minder vaak lijken voor te komen. Hierbij dient te worden opgemerkt dat wij voor dit onderzoek een beperkt aantal professionals hebben gesproken die niet allemaal even direct zicht hebben op online rekruteringsprocessen. Dit maakt het niet alleen lastig om harde uitspraken te doen over de verhouding tussen generieke en specifieke rekrutering, maar ook om een beeld te krijgen van hoe vaak specifieke rekrutering überhaupt voorkomt. Wel kunnen wij constateren dat de geïnterviewde professionals het er unaniem over eens waren dat personen in het algemeen in aanraking komen met een extremistische groep doordat ze zelf online op zoek gaan naar gelijkgestemden en vervolgens lid worden van een openbare groep.

De vraag is in hoeverre dit proces doelbewust is. De professionals die wij hebben geïnterviewd verschillen hierover van mening. Respondenten vanuit hulpverlenende instanties hebben het idee dat jongeren vaak niet doelbewust op zoek gaan naar gewelddadige of extremistische groepen om zich bij aan te sluiten. Een opeenstapeling van factoren, waaronder identiteitsvorming van adolescenten, de behoefte ergens bij te willen horen, een drang naar sensatie, positieve conditionering en algoritmes van online platforms, kunnen ervoor zorgen dat bepaalde personen steeds verder worden meegesleept in een extremistische groep zonder dat dat in eerste instantie de intentie was. Dit is

volgens respondenten terug te zien binnen jihadistische groeperingen, maar een respondent werkzaam bij Landelijk Steunpunt Extremisme (LSE) herkent dit ook bij accelerationisme:

"Bijvoorbeeld bij accelerationisme zien we vaak dat jongeren zich niet eens beseffen dat zij zich op fora begeven die dan wel strafbaar, dan wel zeer zorgelijk geacht worden. […] Dat mensen, zoals [respondent_LSE_1] zegt, niet heel bewust op zoek gaan naar 'waar is het extremistische sausje' maar soms heel makkelijk daar toch onbewust in terecht komen." (Respondent_LSE_2)

Medewerkers van opsporingsinstanties zijn hier sceptischer over. Bovengenoemde factoren kunnen volgens hen wel degelijk een rol spelen in radicaliserings- of rekruteringsprocessen, maar er is ook altijd sprake van een bepaalde mate van opzettelijk handelen en doelbewuste keuzes die gemaakt worden door de persoon in kwestie. Het één hoeft het ander niet uit te sluiten; individuen kunnen een bepaalde kwetsbaarheid hebben, maar toch een bewuste keuze maken om bij een groep betrokken te raken.

Na deze eerste fase waarin mensen toenadering zoeken tot een extremistische groep kunnen individuen verder verzeild raken in de groep. Een meerderheid van de professionals vanuit verschillende organisaties, zowel vanuit de opsporing als de hulpverlening, beschrijft dit als een trapsgewijs rekruteringsproces waarbij een individu telkens een stap verder gaat en daardoor steeds dieper in een extremistische groepering terechtkomt. Nadat een individu online op zoek is gegaan naar gelijkgestemden, komt hij of zij in een openbare, online groepering terecht. In deze omgeving vinden processen van generieke rekrutering plaats die onder 4.2 zijn besproken. Voor sommige individuen blijft het hier vervolgens bij, als ze in de open groep datgene vinden waarnaar ze op zoek zijn. Een respondent van de politie merkt hierover op:

"Ik denk eerlijk gezegd dat een heel groot deel van die groepen, die dus publiek zijn […] en waar behoorlijk veel mensen in kunnen zitten, dat die veel meer doel dan middel zijn. Dus dat het op zichzelf lid zijn van zo'n groep en daar af en toe wat dingen ingooien en dingen uithalen, dat dat al super is. Dat dat al helemaal is wat mensen zoeken." (Respondent_politie_1)

Daarentegen gaat het rekruteringsproces in sommige gevallen wel degelijk een volgende fase in, afhankelijk van bepaalde factoren die erop wijzen dat een individu een bijdrage zou kunnen leveren aan de groep. Hierbij kan worden gedacht aan de hoeveelheid uitspraken die iemand doet in lijn met het gedachtegoed van de groepering, de mate waarin iemand aangeeft zich in te willen zetten voor de groepering of laat merken bereid te zijn om over te gaan tot actie. Op zo'n moment kan een individu worden uitgenodigd voor een kleinere groep. Deze kleinere groep is doorgaans besloten. Dit proces herhaalt zich in sommige gevallen een aantal keer, waardoor het individu uiteindelijk terecht komt in de meest exclusieve 'harde kern' van de groepering. Vervolgens gaan de meeste groepen in het laatste stadium van het rekruteringproces over tot doorlichtingsprocedures middels online één-op-één of offline ontmoetingen.

Dit trapsgewijze rekruteringsproces zien respondenten terug bij uiteenlopende groeperingen binnen het rechtsextremisme, anti-institutioneel extremisme en jihadisme. Wel zijn er verschillen op te merken. Zo merken meerdere respondenten van de politie op dat sommige rechtsextremistische groepen eerder over lijken te gaan tot, of meer waarde te hechten aan, offline ontmoetingen dan

jihadistische groepen (hierop zal verder worden ingegaan in 4.5). Op basis van de interviewresultaten kan dus worden geconcludeerd dat extremistische groepen niet rekruteren op een concreet, duidelijk aanwijsbaar moment maar dat het eerder een geleidelijk proces is dat bestaat uit meerdere fasen, en dat sterk interactief van aard is. Een respondent van de politie zegt hierover het volgende:

"Het is natuurlijk een soort sneeuwbal waar je instapt en waar het op een gegeven moment niet meer duidelijk is wie nou precies wie benadert. Ook op het moment dat je lid wordt van een app- of chatgroep, benader jij dan de mensen die in die chatgroep zitten of is er pas sprake van benadering op het moment dat diegene in die chatgroep tegen jou zegt 'Hey, leuk dat je er bent. Zullen we nu samen AK-47's aanschaffen?" (Respondent_politie_1)

Opgemerkt dient te worden dat een dergelijk rekruteringsproces volgens respondenten vaak ook niet lineair verloopt. Een individu zou op en neer kunnen bewegen tussen verschillende 'treden' van rekrutering en de verschillende treden sluiten elkaar niet uit. Iemand kan bijvoorbeeld zowel actief zijn op een 'laagdrempelig' online platform, als offline bijeenkomen met anderen om concrete acties te plannen. Daarnaast staat het rekruteringsproces niet op zichzelf, maar is het verweven met netwerkvorming die plaatsvindt binnen extremistische stromingen.

4.3.3 Online en offline doorlichtingsprocedures bij rekrutering

Verschillende respondenten (o.a. politie_2, ESS_2, gemeente_3) noemen dat het trapsgewijze rekruteringsproces gepaard gaat met bepaalde 'doorlichtingsprocedures' waarin leden van de groep nagaan of specifieke personen geschikt zijn om lid te worden van hun groep. Een dergelijke doorlichtingsprocedure kan bestaan uit (kennis)vragen, maar een potentiële rekruut kan ook worden uitgenodigd om bijvoorbeeld een keer samen iets te gaan drinken of samen te sporten. Doorlichtingsprocedures hebben verschillende doeleinden, bijvoorbeeld ter authenticatie, om na te gaan of iemand beschikt over het 'juiste' gedachtegoed of om in te schatten of iemand bereid is om daadwerkelijk over te gaan tot actie:

"Eerst werden dus hele lange gesprekken online gevoerd, eigenlijk een soort lakmoesproef waarin werd nagegaan of deze persoon de juiste vorm van de 'echte' islam aanhing, in hoeverre diegene daadwerkelijk bereid was om een steentje bij te dragen aan de heilige zaak, en in hoeverre het ging om een echt persoon en niet om een AIVD agent of iets dergelijks." (Respondent_ESS_2)

Volgens de geïnterviewde professionals vinden deze doorlichtingsprocedures online vooral plaats in één-op-één chats en besloten groepen. In de door ons uitgevoerde content-analyse, gebaseerd op open groepen, zien wij hier dan ook weinig van terug. In twee van de geanalyseerde groepen zijn hiervoor echter wel aanwijzingen gevonden. In een extreemrechtse groepering wordt bijvoorbeeld beeldmateriaal gedeeld waarop te zien is dat leden een eed afleggen en zo als nieuwe leden worden ingezworen, en in een anti-institutionele groep wordt een aantal vragen gesteld aan een nieuwe deelnemer van de groep:

"Welkom [naam]! Zou jij je kunnen en willen voorstellen? En waar ken je [groep] van? Hoe zie je alles voor je? Wat denk je dat [groep] kan doen? Waar sta jijzelf allemaal voor?" (groep 3)

Zoals in bovenstaande citaten naar voren komt, kan ideologische kennis worden ingezet in de doorlichtingsprocedures tijdens het rekruteringsproces. Een persoon die volgens leden niet beschikt over het juiste gedachtegoed, wordt volgens de respondenten van onze interviews niet toegelaten tot een bepaalde (online) groepering en kan ook worden verwijderd uit een openbare online groep. Wel merken professionals op dat het ideologische aspect bij rechtsextremistische en anti-institutionele groeperingen een minder prominente rol speelt in online groepen dan zo'n vijf à tien jaar geleden. Bij jihadistische groepen zou het hebben van de 'juiste' ideologie wel nog een belangrijke rol spelen en regelmatig ter discussie staan. Dit komt ook naar voren in een van de door ons geanalyseerde jihadistische groepen (groep 6):

"Ik weet niet hoe lang deze onzin al rondgaat, maar kunnen degenen die niks weten van islamitisch (oorlogs)recht, hun mond dicht houden en niet klakkeloos flyers maken ter promotie van deze Teletubbie-oorlogvoering? Werkelijk Islamitisch recht: […]"

Tegelijkertijd merkt een aantal professionals op dat er binnen verschillende extremistische stromingen een opkomst zichtbaar is van heftig, vaak gewelddadig beeldmateriaal, uiteenlopend van onthoofdingsvideo's tot expliciete foto's van automutilatie. Enerzijds lijkt dit volgens respondenten stoerdoenerij te zijn, voortkomend uit het online ecosysteem waarin leden elkaar voortdurend willen overtreffen. Anderzijds lijkt dergelijk beeldmateriaal ook een rol te hebben in het doorlichtingsproces. Of een persoon bereid is om heftige video's te bekijken en de reactie op dergelijk beeldmateriaal kan bepalen of diegene wel of niet wordt toegelaten tot een bepaalde groep. Soms worden zelfs overhoringsvragen gesteld om na te gaan in hoeverre diegene het beeldmateriaal heeft bekeken. Er kan bijvoorbeeld aan een rekruut worden gevraagd naar een detail dat in een bepaald fragment van een video te zien was waarvoor de video aandachtig bestudeerd moet worden.

4.4 De doelen van online rekrutering

In het bovenstaande worden de verschillende fasen van het online rekruteringsproces besproken. De vraag is daarnaast voor *welke doeleinden* nieuwe leden worden gerekruteerd. Volgens de geïnterviewde professionals is het voornaamste doel om mensen te vinden die bereid zijn om zich op diverse manieren in te zetten voor de groep. In openbare online groepen zou het vooral draaien om het verspreiden van propaganda en informatie over de groep, met als oogmerk om zo veel mogelijk mensen te bereiken, het gedachtegoed te normaliseren en ruchtbaarheid te geven aan activiteiten. Uit de interviews komt verder naar voren dat nieuwe leden worden opgeroepen om bij te dragen aan het verspreiden van het gedachtegoed van de groep door uiteenlopende activiteiten, zoals stickers of flyers verspreiden in openbare ruimtes, deelnemen aan protesten of evenementen, video's monteren of verspreiden, brieven versturen naar instanties of geld doneren. In de door ons uitgevoerde contentanalyses was te zien dat dergelijke oproepen regelmatig gepaard gaan met concrete instructies, zoals in onderstaand voorbeeld:

"[…] ze zijn bezig met het weerspreken van het narratief van de mainstream media. Dat is iets wat je kunt doen. Je kunt natuurlijk ook feitelijke informatie delen, nieuwsberichten delen, analyses daarover maken, maar ook bestaande informatie verwerken tot hapklare brokken zodat het ook voor het sociale media publiek makkelijk is te consumeren. Er is dus heel veel wat je kunt doen. Wees een

soldaat van de informatieoorlog, maak gebruik van de technische middelen die je tot je beschikking hebt en zet hem op […]" (groep 5)

Het gaat in deze openbare groepen doorgaans om algemene verzoeken zonder dat aan specifieke leden wordt gevraagd zich op een bepaalde manier in te zetten voor de groepering. In de besloten online groepen is dit veel vaker wel het geval, zo zien respondenten van de politie en AIVD. In deze besloten groepen worden ook meer concrete en ernstige activiteiten besproken, zoals het delen van informatie om aan wapens te komen, instructies om bommen te maken en het plannen van extremistische acties.

Op basis van de interviews en contentanalyse zijn verschillen op te merken tussen extremistische groepen in de technieken en narratieven die zij gebruiken om mensen te rekruteren voor bepaalde acties. Zo komt naar voren dat extreemrechtse en -linkse groepen regelmatig stickers maken en verspreiden in openbare ruimtes. Onder anti-institutionele groepen zou dit minder vaak voorkomen, en jihadistische groepen zouden helemaal geen stickers verspreiden. Opgemerkt dient te worden dat dit per stad of regio kan verschillen, afhankelijk van waar bepaalde groepen actief zijn maar ook bijvoorbeeld het beleid dat gevoerd wordt door de gemeente. Zo geeft een gemeentemedewerker aan dat er in de regio waar de medewerker werkzaam is veel stickers van extreemrechtse en anti-institutionele groepen te vinden zijn terwijl een medewerker van een andere gemeente juist het volgende beeld beschrijft:

"Wat wij zelf hier veel zien is dat op links, als het gaat om activisme, dat staat veel meer 'aan' dan rechts of anti-institutioneel. Dus als je de stad in gaat en je gaat stickers checken dan zie je eigenlijk alleen maar stickers van [twee extreemlinkse groepen]. Die zijn gewoon erg actief in het stickeren en dat stukje activisme. Ik zie echt weinig stickers op rechts. Tegenwoordig ook veel minder anti-institutioneel. Je hebt ze nog wel maar de meesten zijn nog van de Covid-periode. Dat vind ik dus wel grappig want we hebben het heel weinig over links maar activistisch gezien zijn die best wel actief."
(Respondent_gemeente_1)

Uit de contentanalyse kwam een van de extreemrechtse groepen duidelijk naar voren als het gaat om het plakken van stickers. Deze groep plaatste in de geanalyseerde periode regelmatig foto's en video's waarin te zien is hoe stickers van de groepering op openbare plekken worden geplakt zoals in het openbaar vervoer en op lantaarnpalen en verkeersborden. In twee berichten is te zien hoe stickers van de groep over materiaal van extreemlinkse groepen heen wordt geplakt. Onder dergelijk beeldmateriaal staan vaak links naar een door de groep gemaakte handleiding met instructies hoe je stickers kan maken en op welk platform ontwerpen te vinden zijn. In de andere groepen worden tijdens de analyseperiode daarentegen geen berichten geplaatst waaruit blijkt dat de groepen gebruik maken van stickers voor het verspreiden van hun gedachtegoed of andere doeleinden.

4.5 Interactie tussen online en offline gedrag

In 4.1 werd beschreven dat rekrutering voor extremistische organisaties in de Nederlandse context doorgaans niet aanvangt met op het individu gerichte tactieken, maar veel vaker een meer algemeen proces betreft waarin in eerste instantie vooral de aantrekkingskracht van extremistische groepen een rol lijkt te spelen. Extremistische groepen gebruiken die aantrekkingskracht om vervolgens meer

generiek leden te werven voor de organisatie. In een trapsgewijs proces dat daarop volgt kunnen nieuwe geïnteresseerden vervolgens dieper de organisatie binnenkomen, waarbij regelmatig op enig moment ook offline ontmoetingen volgen. Juist deze interactie tussen de online en offline wereld is onderwerp van interesse van zowel de wetenschap als instanties. De aandacht gaat daarbij vaak uit naar de rol van het online domein in de aanloop naar offline geweld. Zoals in de inleiding al werd benoemd, lijken verschillende recente gebeurtenissen in de offline wereld hun oorsprong in het online domein te hebben. Hierbij werd onder meer gewezen op de bestorming van het Capitool in de Verenigde Staten en van overheidsgebouwen in Brazilië, een aanslag in Nieuw-Zeeland en getoonde antisemitische leuzen in Rotterdam. Hoewel in deze gevallen terugkijkend is vastgesteld dat de acties online zijn bedacht, voorbereid, aangekondigd en/of toegejuicht, is de directe invloed van de online gebeurtenissen op de offline acties altijd moeilijk vast te stellen. Daarbij komt dat de relatie online – offline veel complexer is dan soms wordt voorgesteld, en ook meerdere kanten kan opwerken. Meer specifiek kunnen de online en offline context niet worden gezien als twee zelfstandige domeinen (Gill et al., 2015; Mattheis, 2019; Herath & Whittaker, 2021). Deze liggen vaak in het verlengde van elkaar en vormen een 'continuüm'. Verschillende studies spreken dan ook over 'onlife' radicalisering, waarbij wordt gedoeld op het hybride online en offline domein waarin individuen en groepen zich bewegen (Valentini et al.,2020). Online betrokkenheid kan leiden tot offline activiteiten en vice versa. Beide contexten zijn sterk geïntegreerd en het is cruciaal om deze wisselwerking in acht te nemen (Nanninga et al., 2022).

Uit de literatuur, de interviews en de content-analyse komt naar voren dat er op minstens drie manieren naar de wisselwerking tussen online en offline werelden kan worden gekeken. Ten eerste kan de offline wereld van belang zijn in de aanloop naar online rekrutering voor extremistische groepen, waarbij de situatie in de offline wereld de vatbaarheid voor online rekrutering vergroot. Ten tweede kan online rekrutering en groepsvorming op een bepaald punt overgaan in 'onlife' rekrutering en groepsvorming, waarbij zowel online als offline rekruterings- en groepsvormingsprocessen plaatsvinden. Ten derde kan online rekrutering en groepsvorming een voorfase zijn van offline gewelddadigheden. Er bestaat ook nog een vierde manier waarin iemand offline in aanraking komt met een groep of ideologie door zijn of haar offline sociale netwerk en vervolgens via die weg op een online platform terechtkomt. Gelet op de focus van het huidige onderzoek gaan we in wat nu volgt hoofdzakelijk in op de eerste drie verbanden.

4.5.1. Oorsprong in de offline wereld

In hoofdstuk 2 werd gewezen op het vraagstuk rond beïnvloeding en selectie. Dit vraagstuk raakt direct aan de wisselwerking tussen online en offline processen. Zeker als het gaat om (zelf)selectie is het belangrijk om ook oog te hebben voor iemands offline situatie en netwerk. Ook verschillende studies wijzen hierop; in divers onderzoek wordt geconstateerd dat het online domein geen vervanging is voor het offline domein (Schils & Verhage, 2017; Simi & Futrell, 2006; Stevens & Neumann, 2009; Von Behr et al., 2013), en dat de digitale context – uitzonderingen daargelaten - onvoldoende is voor radicaliserings- en rekruteringsprocessen (Jones, 2017; Pauwels & Schils, 2016). Het is daarom belangrijk om op individueel niveau oog te hebben voor de wisselwerking tussen het offline en online domein. Meer specifiek kunnen "offline" omstandigheden ervoor zorgen dat iemand een groter risico loopt om online te radicaliseren of gerekruteerd te worden. Hierbij kan bijvoorbeeld worden gedacht aan school- of werkgerelateerde problemen, het ervaren van onrechtvaardigheid en/of discriminatie, sociale isolatie, en een zoektocht naar identiteit en/of betekenisgeving (Peeters et al., 2022; Sikkens

et al., 2017). Dit beeld wordt bevestigd in de interviews. Verschillende respondenten geven aan dat ze vanuit hun dagelijks werk merken dat individuen die zich online hebben aangesloten bij een extremistisch netwerk daaraan voorafgaand regelmatig al diverse problemen hadden (bv. interview AIVD_1, ESS, gemeente_1, LSE, politie_1), zoals problemen in de thuissituatie. Opvallend is dat meermaals wordt aangegeven dat deze kwetsbaarheden voor een belangrijk deel overeenkomen met kwetsbaarheden van andere doelgroepen, zoals jonge uithalers:

"Als het gaat om al die verschillende risicofactoren, dan zien wij dat daar echt wel overlap in zit, dus hoe kwetsbaar is een jongere ofwel voor drugscriminaliteit ofwel voor een extremistische organisatie. Daarin kunnen bepaalde factoren gelijk aan elkaar zijn. Ik denk dat in het voorstadium overeenkomsten te vinden zijn maar ik durf niet te zeggen of een organisatie vanuit de ondermijnende criminaliteit op dezelfde wijze te werk gaat als een organisatie vanuit een bepaalde ideologie. Het zou me niks verbazen. Je ziet vaak natuurlijk dat zo'n organisatie inzet op bepaalde dynamieken, dus bijvoorbeeld het groepsgevoel of het gevoel dat je ergens bij hoort of iets kan betekenen. Helemaal als je het gevoel hebt achtergesteld te worden of boos bent. Dat zijn allemaal van die thema's die dan aangehaald kunnen worden en ik kan me best voorstellen dat dat ook bij ondermijnende criminaliteit het geval is." (Respondent_gemeente_1)

Een zoektocht naar status, groepsvorming en soms ook spanning kan bijdragen aan de kans dat iemand zich online aangetrokken voelt tot een bepaalde groep. Belangrijk om te benoemen is dat dergelijke kwetsbaarheden geen causaal verband hebben met rekrutering; immers, heel veel mensen met soortgelijke kwetsbaarheden treden niet toe tot een extremistische groep. Wel kan worden gesteld dat deze kwetsbaarheden een van de risicofactoren zijn, en derhalve belangrijk om in ogenschouw te nemen.

4.5.2. Online en offline oproepen en promo's

Ook op groepsniveau is sprake van een voortdurende wisselwerking tussen de online en offline context op het gebied van organisatorische activiteiten, netwerken en propaganda, zo bleek ook al uit eerder onderzoek (Peeters et al., 2022; Van Wonderen et al., 2023). Het internet kan bijvoorbeeld gebruikt worden voor het grootschalig organiseren en adverteren van fysieke bijeenkomsten, waaronder vergaderingen en protestacties. In het verlengde hiervan ligt de netwerkfunctie van het online domein. Groepen kunnen via sociale media eenvoudiger met elkaar in contact komen en via deze weg hun invloed vergroten (Gaudette et al., 2022). Dit beeld wordt bevestigd in de interviews en de content-analyse. Hieruit blijkt dat verschillende groepen zich actief inzetten voor het werven van nieuwe leden in zowel het online als het offline domein. Vaak is daar duidelijk een wisselwerking tussen. Een veelvoorkomend voorbeeld is het plakken van stickers in openbare ruimten, alsook het online promoten van dat stickerplakken, zoals al besproken in 4.4 'De doelen van online rekrutering'. In een van de extreemrechtse groepen uit de contentanalyse werden regelmatig berichten geplaatst waarin te zien is dat leden van de groep stickers plakken in openbare ruimten. Een voorbeeld is een korte video waarin te zien is hoe verschillende stickers van de groepering op lantaarnpalen en containers worden geplakt in een Nederlandse stad. Op sommige stickers staat alleen de naam van de groepering, terwijl op anderen ook een QR-code en de naam van de Telegramgroep staat, of 'wist je dat' gevolgd door propagandateksten. Een andere video laat zien dat leden met een spandoek op een viaduct gaan staan. Op het spandoek staat de naam van de groepering en de naam van de Telegramgroep. Tegen het einde van de video gaat het volume van de muziek zachter om te laten horen dat voorbijkomende

auto's toeteren naar de leden met het spandoek. In het laatste shot wordt een sticker van de groepering geplakt op een verkeersbord vlakbij het viaduct. In deze berichten worden niet alleen wervingshandelingen getoond, maar wordt ook regelmatig de ideologie van de groep benadrukt. Via QR-codes en Telegram 'handles' kunnen mensen eenvoudig lid worden van de online groep, waarin vervolgens weer oproepen gedaan worden voor nieuwe acties. Van deze offline acties wordt na afloop verslag gedaan in de online groep.

Naast het promoten van lidmaatschap van de groep worden ook offline evenementen online aangekondigd en gepromoot. De verschillende platforms worden hier veelvuldig voor gebruikt. Aankondigingen van offline evenementen gaan regelmatig gepaard met ideologische uitingen, waarbij wordt gewezen op het belang van de groep en waar zij voor staat, zoals in onderstaand bericht dat in een van de geanalyseerde extreemrechtse groepen (groep 2) werd gedeeld:

"[datum] marks [naam groep] 30th consecutive global event. After a successful summer of activism, we are asking YOU to get involved in reawakening White racial consciousness and the fight for 14. 'It is perfectly healthy to fight for the survival of your extended racial family. Every other racial group on earth understands this.' 3 rallies left for this year: [data]. Message@[naam groep]chatbot."

Dergelijke berichten lijken een tweeledig doel te hebben; enerzijds wordt concrete informatie verstrekt over aanstaande evenementen. Anderzijds kan worden gesteld dat de ideologische componenten ook dienen ter bekrachtiging, om daarmee de aantrekkingskracht voor al bestaande maar mogelijk ook nieuwe leden te vergroten. Door tevens na afloop van offline evenementen met beeldmateriaal online verslag te doen van het betreffende evenement, wordt er niet alleen voor gezorgd dat leden die niet aanwezig waren op de hoogte blijven, maar het delen van dergelijke bijeenkomsten kan ook worden beschouwd als bekrachtiging van het bestaan van de groep en het vergroten van de zichtbaarheid. Dit zagen we in de contentanalyse hoofdzakelijk terug bij de extreemrechtse groepen. Een respondent van de politie zegt hierover:

"Dat wordt op een Telegram-kanaal gepost en die foto gaat dan heel snel ook op Twitter rond en op allerlei andere plekken dus dat is natuurlijk wel interessant. Op die foto zijn geen gezichten in beeld maar wel weer die openbaarheid. Dan weet je van hier zijn 15 mensen of zo samen geweest."
(Respondent_politie_1)

Hieraan gerelateerd wordt duidelijk dat extremistische groepen hun propagandistische narratieven verspreiden onder een breder publiek door online in te spelen op actuele sociaal-politieke gebeurtenissen, waarmee ze tegelijkertijd proberen om nieuwe leden voor de beweging te werven. Denk hierbij bijvoorbeeld aan de stikstofcrisis of de oorlog tussen Israël en Hamas. Volgens de geïnterviewde professionals komt het regelmatig voor dat extremistische groepen met verschillende ideologische overtuigingen inspelen op dezelfde actuele gebeurtenissen. Dit beeld wordt bevestigd door de contentanalyse, waarin extreemrechtse, extreemlinkse en jihadistische groepen aanhaken bij de oorlog tussen Israël en Hamas. Zo wordt er in een van de extreemrechtse groepen (groep 2) gerefereerd aan een complot over de invloed van een Joodse elite en hoe de witte medemens niet zou moeten opkomen voor, en deelnemen aan, de meest recente oorlog in Israël. Er wordt bijvoorbeeld beeldmateriaal gedeeld van leden van de groepering die spandoeken vasthouden waarop teksten staan als *"Do not die for Zionism, white man!"* en *"Israël is not our 'greatest ally'!".* Daarnaast kondigt

een extreemlinkse groep (groep 7) een benefietavond aan voor humanitaire hulp in de Gazastrook en wordt in een van de jihadistische groepen (groep 6) een schermafbeelding van de volgende Tweet gedeeld: *"~~Echte joden zijn onze vrienden~~. De zionistische beesten zijn de vijand van de gehele mensheid. #Gaza #Gaza_Genocide".* Volgens een respondent van de politie wordt in jihadistische groepen tevens opgeroepen om 'westerse berichtgeving' en berichten waarin met een zekere nuance over de situatie wordt gesproken, niet te geloven. Tot slot gebeurt het ook dat de actualiteit online wordt besproken in extremistische groepen, waarna deze groepen zich offline mengen in niet-extremistische bijeenkomsten, om aldaar leden te rekruteren. Een medewerker van LSE illustreert dit aan de hand van een voorbeeld:

"We weten dat er van die extreemrechtse groepen zijn […] die dan bijvoorbeeld hebben geprobeerd om te demonstreren of aan te schuiven bij demonstraties van lokale, bezorgde mensen over bijvoorbeeld een asielzoekerscentrum. In het verleden waren ze niet welkom, maar tegenwoordig wel. Daarmee kunnen ze eigenlijk hun eigen ideeën witwassen en dan niet alleen aanwezig zijn maar heel erg duidelijk aanwezig zijn met allerlei symbolen, vlaggen en leuzen. Daar kunnen ze dan meteen ook de mensen voorzien van een stukje informatie over wie ze zijn en hoe mensen zich kunnen aansluiten." (Respondent_ESS_2)

Tot slot komt uit de interviews naar voren dat de balans tussen het online en offline domein de laatste jaren enigszins lijkt te verschuiven. De rol van het online domein in rekruteringsprocessen blijft prominent maar tegelijkertijd heerst er onder extremistische groepen een toenemend veiligheidsbewustzijn (AIVD_1, gemeente_3, jongerenwerk_1, LSE, politie_1, politie_3). Extremistische groepen zijn zich steeds bewuster van het feit dat er een aanzienlijke kans bestaat dat (opsporings-)instanties meelezen op online platforms. Enerzijds gaan extremistische groepen hierdoor online voorzichtiger te werk door bijvoorbeeld subtieler te zijn in het uiten van hun gedachtegoed, codetaal te gebruiken, minder expliciet beeldmateriaal te delen en strengere eisen te stellen aan deelname en toelating. Een respondent van de gemeente zegt over dit laatste punt het volgende:

"Vroeger was het hoe meer zieltjes, hoe beter. Nu moet je eerst bijna een soort interview afleggen, een soort ballotagecommissie, voordat je in een groep mag die wat extremer is."
(respondent_gemeente_3)

Anderzijds zorgt het toenemende veiligheidsbewustzijn van extremistische groepen ervoor dat er hernieuwde waarde wordt gehecht aan fysiek contact, dat door sommige groepen als een veiligere manier van communiceren wordt gezien. Hieraan gerelateerd haalt een aantal respondenten ook rechtsextremistische 'active' groepen aan die bekend staan om hun focus op fysieke ontmoetingen. Een respondent van de politie geeft aan dat deze groepen een bereidheid om elkaar fysiek te ontmoeten en tot actie over te gaan ook vaak stellen als vereiste om überhaupt toegelaten te worden tot de groep (respondent_politie_2).

4.5.3. Online extremisme en offline gedrag

In paragraaf 4.3.2 werd beschreven hoe individuen doorgaans bij extremistische groepen terecht komen doordat ze aanvankelijk online op zoek gaan naar gelijkgestemden en vervolgens steeds dieper verzeild raken in een groepering. In een later stadium van dit proces kan worden overgegaan tot offline ontmoetingen en acties. Met betrekking tot de contentanalyse is het opvallend dat, ondanks de korte

analyseperiode, in alle geanalyseerde groepen berichten worden geplaatst over offline samenkomsten, uiteenlopend van lezingen tot gezamenlijk sporten en protesten (zie paragraaf 4.2.1 'Offline groepsvorming'). Uit een aantal interviews kwam daarbij naar voren dat rechtsextremistische groepen over het algemeen eerder lijken over te gaan tot fysieke bijeenkomsten dan andere groeperingen. Dit zien wij bijvoorbeeld terug in de contentanalyse. In beide extreemrechtse groepen worden met regelmaat offline bijeenkomsten aangekondigd en wordt ook verslag gedaan van offline bijeenkomsten. Zo wordt er in groep 1 bijvoorbeeld een foto gedeeld waarop een vijftal (onherkenbaar in beeld gebrachte) leden poseren met een vlag van de groepering met het volgende bijschrift: *"Some of our members recently came together to test their physical shape in preparation for #whiteboysummer. Tribe and Train!".* Deze offline samenkomsten moeten echter niet worden overschat. Meerdere respondenten plaatsten hier dan ook kanttekeningen bij. Een groot deel van de mensen die lid zijn van (openbare) online groeperingen zouden om uiteenlopende redenen nooit overgaan tot offline acties. Een respondent van de politie geeft hier een voorbeeld van:

"Het mobiliserende effect om echt met elkaar dingen te gaan doen die in de buitenwereld, in de echte wereld plaatsvinden, dat lijkt vaak veel groter dan het in potentie daadwerkelijk is. Bovendien zijn veel van die rechtse groepen super anoniem. Die jongens die schermen hun eigen identiteit gewoon hartstikke goed af. Dus dan is het ook heel moeilijk om te zien wie er eigenlijk in jouw groep zit. […] Dat betekent dat zij kunnen zeggen 'we kunnen volgende week om kwart over vier afspreken' 'Oké, prima, waar?' Wie durft er dan als eerste iets te zeggen? Dat is natuurlijk ook wel iets wat een tamelijk remmende werking heeft. Zeker als je er ook rekening mee houdt dat mensen bijvoorbeeld 16 kunnen zijn. Veel mensen van 16 gaan wel heel stoer zeggen 'prima, kom ik jouw kant op' maar als puntje bij paaltje komt, gaan ze bij wijze van spreken niet van Sneek naar Best reizen. Dan denken ze niet 'ik ga op goed geluk eens even kijken of daar ook andere mensen op dat dorpsplein staan'" (Respondent_politie_1)

Daarnaast geven meerdere respondenten aan dat het ook nog regelmatig voorkomt dat individuen via hun omgeving (vrienden, familieleden, buren etc.) of via fysieke evenementen (demonstraties, lezingen, verjaardagen etc.) terechtkomen bij extremistische groeperingen. Ondanks dit initiële offline contact, verloopt veel communicatie vervolgens wel weer digitaal. Uit de interviewresultaten bleek verder dat professionals verschillende visies hadden op de volgordelijkheid van online en offline acties:

"De pushfactoren zijn allemaal offline maar online zijn de pullfactoren dan weer te vinden. Op die manier zie ik de scheiding en de verbinding tussen online en offline. Dus alles wat je offline meemaakt zorgt ervoor dat je op het moment dat je exposed bent aan de pullfactor online, dat je daar dan ook snel verbinding mee vindt." (Respondent_ESS_1)

"Ik ben niet geneigd om te zeggen dat online altijd een voorstadium is voor offline. Dat is het gewoon niet. Dat is echt niet meer de logica van dit moment. Een heel groot deel van ons leven speelt zich nou eenmaal online af. Als je goed na gaat denken over je eigen contact is dat vaak ook zo. Hoe vaak spreek je die vrienden eigenlijk nog offline? En hoe vaak online? Dat evenwicht is helemaal naar online geslagen. […] Zo is het natuurlijk daar [in extremistische kringen] ook. Dan is er helemaal niet de intentie bij het uitwisselen van dat bericht om te zeggen 'nu begint de grote opmaat naar offline contact'" (Respondent_politie_1)

Zoals blijkt uit bovenstaande interviewresultaten, blijft het ingewikkeld om online gedrag te koppelen aan offline gedrag. Binnen de literatuur is er nog maar mondjesmaat zicht op de relatie tussen en de volgordelijkheid van online en offline acties, en ditzelfde geldt voor online en offline sociale netwerken (Von Behr et al., 2013; Winter et al., 2020). Eén van de weinige studies die erin geslaagd is om online berichten te linken aan offline gewelddadig gedrag is de studie van Scrivens (2022). De onderzoeker analyseerde posts van rechtsextremistische internetgebruikers. In samenwerking met een voormalige rechtsextremist wist hij vervolgens te achterhalen welke individuen achter de online users schuilden. Vervolgens wist hij te achterhalen wie van deze individuen naderhand in het echte leven extremistisch geweld hadden gepleegd. Vervolgens relateerde de onderzoeker de inhoud van de posts aan het gewelddadige gedrag dat daarop was gevolgd. Uit het onderzoek blijkt dat juist de niet-gewelddadige rechtsextremisten, vergeleken met de gewelddadige rechtsextremisten, meer ideologische berichten hadden geplaatst en dat ze actiever waren in het voorbereiden van deelname aan extremistisch geweld en het mobiliseren van anderen om dat ook te doen. De mensen die uiteindelijk geweld hadden gepleegd lieten online juist minder van hun ideologische gedrevenheid en voornemens tot geweld zien. In deze gevallen leverde de inhoud van de posts geen goede inschatting op van het risico op gewelddadig extremisme in de offline wereld.

Een soortgelijke bevinding kwam uit de studie van Wolfowicz en collega's (2021), die lieten zien dat de onderzochte niet-gewelddadige groep vaker actief bezig was met het zelf plaatsen van tekstberichten, terwijl een gewelddadige groep van veroordeelde terroristen zich vaker alleen bezighield met het delen van berichten. Keatley en collega's (2021) tonen aan dat, waar geweldloze extremisten de neiging hebben om hun opvattingen voornamelijk online te verspreiden en breed te delen met gelijkgestemde mensen, gewelddadige extremisten andere gewelddadige extremisten lijken op te zoeken, om vervolgens online van elkaar te leren en zich ook online beginnen voor te bereiden op hun aanvallen. In lijn met het onderzoek van Keatley en collega's en toegespitst op de Nederlandse situatie, laat onderzoek van Thijs en collega's (2024) zien dat, vergeleken met niet-gewelddadige terrorismeverdachten, gewelddadige terrorismeverdachten frequenter bezig zijn met het online leren over (bv. via online gevonden handboeken over wapens), en voorbereiden op, aanslagen (bv. aanvalsplannen bespreken met online contacten).

4.6 Tot slot

In dit hoofdstuk is een beeld geschetst van de aard, mechanismen en doorwerking van online rekrutering. Daarbij is duidelijk geworden dat een veelheid aan platforms wordt aangewend door extremistische organisaties om nieuwe leden te rekruteren. Dit zijn zowel mainstream sociale media platforms zoals Facebook en Instagram als meer low profile platforms als Telegram. Ook gamingplatforms worden gebruikt, al is het zicht daarop tot op heden beperkt. Uit de resultaten is gebleken dat rekrutering op verschillende manieren kan verlopen. In veel gevallen wordt het online domein gebruikt voor een proces dat wij hebben aangeduid als 'generieke rekrutering'; middels het delen van extremistische narratieven en propaganda en een simultaan proces van groepsvorming worden bezoekers aangemoedigd om lid te worden van de groepering. Daarnaast wordt het online domein gebruikt om gericht bepaalde groepen via een proces van narrowcasting te rekruteren voor de organisatie. Deze tactiek is in de laatste jaren met name aangewend door internationale jihadistische terroristische organisaties zoals IS en Al Qaida. In de Nederlandse context is de laatste tijd bovendien een proces zichtbaar waarbij individuen na initiële generieke rekrutering middels een trapsgewijs proces, waar doorlichtingsprocedures onderdeel vanuit maken, dieper tot een

extremistische organisatie doordringen. Daarbij is duidelijk dat deze processen niet los kunnen worden gezien van de offline wereld. Vatbaarheid voor online rekrutering wordt doorgaans gevormd door gebeurtenissen in het offline domein. Daarnaast bewegen online groepen zich regelmatig ook in de offline wereld, zowel voor sociale activiteiten als voor activiteiten die de ideologische doelen van de organisatie moeten bevorderen. Een belangrijke constatering is dat het offline domein recentelijk weer een prominentere rol lijkt te krijgen. Dit zou te wijten zijn aan een toegenomen veiligheidsbewustzijn van extremistische groepen en de realisatie dat opsporingsinstanties kunnen meelezen, wat leidt tot een kritischer toelatingsbeleid en een herwaardering van fysiek contact.

Opvallend is daarnaast dat er meer overeenkomsten dan verschillen lijken te bestaan tussen het gebruik van sociale media door de onderzochte groeperingen. Zo is in alle groeperingen sprake van online groepsvorming en worden de verschillende andere functionaliteiten van het online domein actief gebruikt, onder meer via het delen van extremistische content, extremistische memes en het verspreiden van de ideologie. Daarnaast organiseren alle groepen offline activiteiten, al varieert de aard van deze activiteiten tussen de groepen. Oproepen om lid te worden van de groep werden met name gezien in extreemrechtse en anti-institutionele groepen, terwijl doorlichtingsprocedures vooral worden ingezet door extreemrechtse, jihadistische en anti-institutionele groepen. Een kanttekening die bij deze vergelijking dient te worden gemaakt is dat we ons hier met name baseren op de voor dit onderzoek verrichte content-analyses en interviews. Tegelijkertijd ontstaat op basis van de wetenschappelijke literatuur het beeld dat op groepen gerichte specifieke rekrutering (hierboven aangeduid als narrowcasting) met name is ingezet door grote jihadistische terroristische organisaties.

Tot slot wordt het online domein soms aangewend om offline extremistische daden voor te bereiden, maar het zicht hierop is nog beperkt en deze relatie laat zich ook moeilijk wetenschappelijk onderzoeken. Al met al is duidelijk dat de online wereld een belangrijke schakel is tussen extremistische organisaties en potentiële nieuwe leden, en daarmee ook een belangrijk domein waarbinnen geïntervenieerd kan worden. In het volgende hoofdstuk bespreken we bestaande maatregelen ter preventie van online rekrutering en mogelijke handelingsperspectieven.

5. Maatregelen tegen online rekrutering en handelingsperspectieven

In dit hoofdstuk wordt aan de hand van inzichten uit de literatuur en de interviews een overzicht gegeven van de maatregelen die worden ingezet om online rekrutering door extremistische groepen tegen te gaan, hoe daar tegenaan wordt gekeken, welke maatregelen wel en niet (lijken te) werken en welke verbeterpunten mogelijk zijn. Belangrijk om te vermelden is dat de eerder benoemde conceptuele vermenging van online rekrutering en gerelateerde processen als online radicalisering ook terugkomt in veel van de hieronder genoemde maatregelen. Dat houdt in dat de maatregelen vaak niet specifiek gericht zijn op het tegengaan van online rekrutering, maar als onderdeel van een bredere focus op online radicalisering óók beogen online rekrutering tegen te gaan. In wat volgt schetsen we eerst enige achtergrond en de relevante beleidscontext. Vervolgens gaan we in op concrete maatregelen om (onder andere) online rekrutering tegen te gaan. Daarna bespreken we verbeterpunten en handelingsperspectieven. We beginnen de verschillende paragrafen met inzichten uit de literatuur en vullen die aan met interviewgegevens.

5.1 Achtergrond en beleidscontext

Het tegengaan van online rekrutering door en voor extremistische groepen is een belangrijk onderwerp voor beleidsmakers binnen het veiligheidsdomein en daarbuiten. Daartoe zijn in de laatste jaren verschillende (beleids)maatregelen genomen, zowel in nationale als in internationale context, die vaak in bredere zin beogen terrorisme en extremisme tegen te gaan. In Nederland is recentelijk de zogeheten “Versterkte Aanpak Online” middels een contourenbrief geformuleerd die zich voornamelijk richt op het tegengaan van extremistische en terroristische content en de effecten hiervan op radicaliseringsprocessen (Ministerie van Justitie en Veiligheid, 2023). Deze aanpak van preventieve en repressieve actielijnen bestaat uit vier pijlers: I) dialoog met de internetsector, II) een wettelijk instrumentarium, III) een lokale aanpak, en IV) internationale inzet. Binnen de eerste pijler wil de Nederlandse overheid een structurele dialoog met de internetsector (grote platforms, aanbieders van hostingdiensten en datacenters) om hun rol en verantwoordelijkheid bij het modereren van ‘legal yet harmful’ content meer te benadrukken. Daarnaast is er Europese wetgeving die bijdraagt aan deze aanpak. De verdere implementatie van de Verordening Terroristische Online-Inhoud (TOI), met als doel om terroristische content op het open internet te verwijderen, heeft prioriteit (p. 7). Daarnaast is recent de Digital Services Act (DSA) volledig in werking getreden. De DSA biedt verschillende mogelijkheden om de verspreiding van extremistische online content op grote online platforms beter te bestrijden (p. 6-7). Hier wordt later nader op ingegaan. De derde pijler betreft de lokale aanpak. Daarmee wordt bedoeld dat de komende jaren bijzondere aandacht moet uitgaan naar het integreren van het online domein in de lokale aanpak van radicalisering en extremisme, door “het delen van best practices te stimuleren en faciliteren, de ervaren knelpunten verder te onderzoeken, effectieve methoden voor een lokale (preventieve) aanpak van online extremisme en terroristische activiteiten verder te ontwikkelen en waar mogelijk uit te breiden.”(p. 7-8). De laatste pijler is de internationale inzet. “Het is noodzakelijk om in gezamenlijkheid tegenwicht te bieden aan de machtige internetbedrijven en andere geopolitieke spelers. Dit is de reden waarom Nederland vol inzet op een gezamenlijke EU-aanpak en toezicht op naleving van bestaande regelgeving zoals de Digitale Diensten Verordening. Daarnaast verkent Nederland mogelijkheden in Brussel om gepaste

wet- en regelgeving te initiëren." (p. 10). In het kort wordt met deze aanpak beoogd om de verantwoordelijkheid van de internetsector te vergroten, aansluiting te vinden bij nieuwe (internationale) coalities, interventies en het stimuleren van meer onderzoek te bevorderen, en het belang van onderlinge samenhang van online maatregelen te benadrukken.

5.2 Bestaande maatregelen om online rekrutering tegen te gaan

In deze paragraaf bespreken we een aantal van de bestaande maatregelen om online rekrutering tegen te gaan in meer detail. Daarbij behandelen we eerst een aantal maatregelen die als 'positieve maatregelen' worden aangeduid, namelijk preventieve aanpakken gericht op weerbaarheid en het inzetten van tegengeluiden. Daarna gaan we in op een aantal 'negatieve maatregelen', zoals aanpakken die gaan over regulering van de online omgeving en moderatie van online materiaal. Tot slot benoemen we een aantal uitdagingen in de aanpak van online rekrutering, zoals benoemd in de literatuur en door respondenten.

5.2.1 Preventie gericht op weerbaarheid

Preventieve aanpakken die zich richten op het vergroten van iemands weerbaarheid worden in de literatuur geschaard onder positieve maatregelen. Programma's gericht op weerbaarheid in de offline wereld bestaan al langer. Daarnaast zijn er inmiddels ook diverse programma's die specifiek op online weerbaarheid zijn gericht. Het gaat dan om online initiatieven die impact willen genereren door bijvoorbeeld het stimuleren van digitale betrokkenheid en educatie (Walker & Conway, 2015; Hodwitz, 2020; Henschke & Reed, 2021). Scholing over extremisme zou kunnen bestaan uit waarschuwingen over het betrokken raken bij gewelddadig extremisme en bewustwording over "grooming" gedrag (een vertrouwensband opzetten) van rekruteurs binnen extremistische groepen (Stevens & Neumann, 2009; Neumann, 2013). Ook het verbeteren van mediageletterdheid wordt genoemd als een manier om beter bestand te zijn tegen extremistische berichten. Het gaat dan om het ontwikkelen van vaardigheden om berichtgeving zelfstandig en kritisch te beoordelen, bronnen te evalueren en te bevragen, en informatie die plausibel en betrouwbaar is te onderscheiden van desinformatie. Ook de respondenten onderschrijven het belang van preventie gericht op weerbaarheid. Een respondent binnen de (lokale) overheid benoemt:

"…wij richten ons wel op hoe kun je ervoor zorgen dat iemand weerbaar en veerkrachtig genoeg is om niet zich opgeroepen te voelen om dat soort ideologieën... of in te gaan op avances van dat soort groepen." (Respondent_ESS_2)

Een tweetal respondenten binnen de rechtshandhaving geeft aan dat voor met name jongeren het online domein een groot deel uitmaakt van hun bestaan, waardoor het belangrijk is om op jonge leeftijd bewustzijn te creëren en weerbaarheidstrainingen te geven (Respondent_AIVD_1 en Respondent_AIVD_2). Dit wordt beaamd door de geïnterviewde jongerenwerkers.

Aangezien extremistisch materiaal en haat zaaiende uitlatingen online een reële bedreiging zijn geworden voor de nationale veiligheid, hebben sommige landen verschillende onderwijsprogramma's ingevoerd om hun burgers voor te bereiden op het opsporen en aanpakken van radicale online content (Akram & Nasar, 2023). Een voorbeeld hiervan is het geëvalueerde programma Operation250 in Massachusetts, Amerika, waarbij jongeren worden geïnformeerd over het risico om online te worden

gerekruteerd en uitgebuit door gewelddadige extremistische groeperingen (Erdemandi et al, 2024). Het initiatief toonde veelbelovende maar marginaal statistisch significante resultaten als het gaat over de impact op het bewustzijn van leerlingen over risicovol onlinegedrag.

In Nederland zijn ook dergelijke programma's ingevoerd. Zo hebben de gemeenten Enschede en Utrecht projecten die zich specifiek richten op het versterken van de digitale weerbaarheid van jongeren (Peeters et al., 2022). Een voorbeeld van een dergelijk lesprogramma is 'Under Pressure' van Diversion, waarbij jongeren door middel van een aantal lessen kennis en vaardigheden worden bijgebracht om desinformatie te kunnen herkennen. Dit programma zou jongeren echter niet langdurig weerbaar maken:

"Wat wij zelf geëvalueerd hebben als ESS, is de interventie Under Pressure van Diversion. […] Daaruit kwam naar voren dat het wel werkt maar het heeft een kortdurend effect. Het mist een langdurig effect. Aan de jongeren wordt wel kennis bijgebracht, ze worden wel wijzer maar ze worden niet per se langdurig competent." (Respondent_ESS_1)

Het rapport van de evaluatie toont dat, na het volgen van de lessen Under Pressure, de kennis en het bewustzijn van leerlingen waren toegenomen omtrent nepnieuws, desinformatie en sociale media algoritmes (Van Wonderen & Peeters, 2022). Voor echte gedragsverandering, dus het ook kunnen identificeren en/of weerbaarder worden, is echter meer tijd en oefening vereist. In de evaluatie wordt daarom onder andere aangeraden om jongeren meer tijd en ruimte te geven om praktische vaardigheden aan te leren, zoals het toepassen van de kennis uit de lessen en over een langere tijd te oefenen met het herkennen van nepnieuws, desinformatie en sociale media algoritmes.

Naast het onderwijsprogramma "Under Pressure", dat door twee respondenten werkzaam binnen de (lokale) overheid (Respondent_ESS_1 en Respondent_gemeente_1) wordt aangehaald, noemt een van deze respondenten nog het programma Radicalise van TerInfo (Respondent_gemeente_1) en een ander het programma Hack Shield (Respondent_gemeente_3). Deze programma's worden ook ingezet op scholen om meer online bewustzijn omtrent online radicalisering en andere online gevaren te creëren.

5.2.1.1 Preventie van rekrutering van jeugdigen en de rol van ouders

Hoewel het bij 'weerbaarheid' vaak om de weerbaarheid van individuen zelf gaat, wordt steeds vaker ook gewezen op het belang van het betrekken van ouders bij verschillende initiatieven, waar het vergroten van weerbaarheid vaak als rode draad doorheen loopt. Logischerwijs is dit met name van belang in het tegengaan van rekrutering van minderjarigen en jongvolwassenen, en dit zijn juist leeftijdsgroepen waar de laatste jaren toenemende zorgen om bestaan (DTN59). Uit de interviews wordt duidelijk dat respondenten het belang van ouders in de preventie van online rekrutering en, meer algemeen, online radicalisering onderstrepen. Bijna de helft van de respondenten geeft aan hoe belangrijk de rol van de ouders is in relatie tot het online domein. Daarbij kunnen ze bijvoorbeeld een belangrijke signalerende functie vervullen als het gaat om preventie van online radicalisering en rekrutering:

"Wat volgens mij het best helpt is als, in het geval van jongeren, de ouders het doorhebben en zelf actie ondernemen of er hulp bij vragen, eventueel van de politie als ze dat aandurven. Het hoeft ook niet altijd een strafrechtelijk onderzoek te [worden]." (Respondent_politie_3)

In het verlengde daarvan noemen twee respondenten dat ouders meer zicht moeten krijgen op het online leven van hun kinderen en meer kennis moeten opdoen over de online omgeving:

"*…we hebben een ouderavond waarin jongerenparticipatie zit, jongeren vertellen iets over waarom [het online domein] belangrijk is voor hen. Dan bereik je ze. En het is ook heel leuk […] 'dit is nou waarom ik het zo leuk vind. Dit is wat het met me doet en dit is wat ik daar zie. Ik ontmoet daar vriendjes."* (Respondent_jongerenwerk_2)

Een andere respondent binnen de (lokale) overheid geeft aan:

"In principe, alle projecten die we hebben, hebben momenteel allemaal een online component erin meegenomen. Dus ook projecten die zich bijvoorbeeld richten op ouders, ook daarin wordt online meegenomen dus: weet je wat je kind online allemaal doet? Hoe ga je daar het gesprek over aan?" (Respondent_gemeente_1)

Naast de belangrijke rol van ouders wijzen respondenten meer in het algemeen op het belang van het voeren van gesprekken met jongeren. Vier respondenten benoemen dat gesprekken zonder oordeel cruciaal zijn in het voorkomen dat jongeren verder afglijden richting extremisme en zich aansluiten bij extremistische organisaties. Een van de respondenten geeft aan:

"Ja, wat ik soms in de casuïstiek merk is dat je verhaal kwijt kunnen zonder dat iemand jou beoordeelt of al meteen overgaat op een interventie, dat is al een interventie op zich. Dat jij dus zonder consequenties wel een keer je verhaal kan neerleggen en daar normaal over in gesprek kan gaan." (Respondent_LSE_1)

Een jongerenwerker laat weten:

"Die jongens worden de hele dag gecorrigeerd terwijl ze gewoon iemand nodig hebben om mee te praten. Door ze een sparringpartner te geven, ontneem je de legitimiteit die ze vinden in internetconnecties." (Respondent_jongerenwerk_1)

Door het voeren van gesprekken ontstaat zicht op de belevingswereld van jongeren, en op hetgeen zij zoeken. Eerder werd in hoofdstuk 4 benoemd dat die zoektocht met name in de fase van generieke rekrutering een belangrijke rol speelt; het is in die fase dat jongeren vatbaar zijn voor groepslidmaatschap, en dus voor online rekrutering. Het is daarom belangrijk om juist in deze fase te weten wat jongeren aantrekt in de online groepen. Een respondent binnen de (lokale) overheid zegt hierover het volgende:

"…als je informatie zoekt over de islam, gewoon als geïnteresseerde, dan kom je tegenwoordig eerder jihadistische ideologieën online tegen, dan […] een regulier aanbod, maar slechts een kleine fractie van radicalen zijn vatbaar voor de ideologieën. Dus onze boodschap is: staar je daar niet blind op,

richt je op die voedingsbodem, concentreer daarop, ga het gesprek aan…vanuit professionals, ouders, scholen. Iedereen kan een schild vormen over zo iemand." (Respondent_ESS_2)

5.2.2 Aanpak gericht op online tegengeluiden

Online initiatieven die impact willen genereren door het aanbieden van "tegengeluiden" of "counter-messaging" worden in de literatuur ook onder positieve maatregelen geschaard (Walker & Conway, 2015; Hodwitz, 2020; Henschke & Reed, 2021). Zoals eerder benoemd zijn dergelijke initiatieven niet specifiek gericht op het voorkomen van online rekrutering, maar beogen ze verschillende aan extremisme gerelateerde processen te voorkomen, waaronder ook online radicalisering. Gelet op het eerder beschreven trapsgewijze proces van online rekrutering waarbij ook elementen als groepsvorming, de verspreiding van een ideologie en extremistische narratieven een rol spelen, zijn aanpakken gericht op online tegengeluiden echter wel degelijk relevant om te bespreken in relatie tot de preventie van online rekrutering.

Wanneer specifiek wordt gekeken naar communicatie-campagnes gericht op het verspreiden van tegengeluiden kunnen volgens Henschke en Reed (2021) drie categorieën worden onderscheiden: het kan gaan om (1) strategische communicatie van de overheid gericht op het vergroten van het bewustzijn van wat de overheid doet en het corrigeren van desinformatie, (2) alternatieve verhalen, om gewelddadige extremistische verhalen te ondermijnen met positieve boodschappen van sociale inclusie en (3) tegenverhalen om het verhaal van gewelddadige extremisten op een directe manier in diskrediet te brengen (p. 3). Naast deze generieke communicatie-campagnes is er ook een aanpak waarbinnen één-op-één gesprekken centraal staan. Hier worden individuen die online blijk geven van radicalisering direct benaderd voor een gesprek. Een voorbeeld van een dergelijk project is de "Online Civil Courage initiative" (OCCI), dat wordt uitgevoerd door Facebook en the Institute of Strategic Dialogue (ISD).[2] Het inzetten op één-op-één gesprekken kwam ook naar voren in de interviews:

"Je spreekt ze aan in hun belevingswereld, op een plek waar ze zich toch wel relatief veilig voelen. Ik merk zelf ook dat je in bepaalde situaties die jongens gewoon veel beter kan aanspreken. Dus als dat [het online domein] hun wereld is, is het ook goed als je daar de hulp kan verlenen."
(Respondent_LSE_1)

Veel van de programma's omtrent het bieden van tegengeluiden met betrekking tot gewelddadig extremisme worden uitgevoerd door het maatschappelijk middenveld (Ganesh & Bright, 2020; Henschke & Reed, 2021). Zo worden bijvoorbeeld organisaties die zich bezighouden met reclame, public relations en mediaproducties ingezet door overheden om tegenverhalen en -materiaal te produceren (Ganesh & Bright, 2020). Dit geldt ook voor EU's Civil Society Empowerment Programme, dat ondersteuning biedt aan organisaties door ze in staat te stellen alternatieven te bieden tegen extremistische boodschappen en ideeën te ondersteunen die propaganda tegengaan. Dergelijke programma's zijn echter veelal gefinancierd door de overheid. De samenwerking met overheidsinstellingen levert een dilemma op voor maatschappelijke organisaties, aangezien een dergelijke samenwerking het risico met zich meebrengt dat zij als minder onafhankelijk en betrouwbaar worden gezien (Henschke & Reed, 2021).

[2] Zie website Institute of Strategic Dialogue: https://www.isdglobal.org/action-training/dialogue-deradicalisation/ (laatst geraadpleegd: 7 mei 2024)

Hoewel het gebruik van tegengeluiden veelvuldig wordt ingezet, is onduidelijk in hoeverre de inzet van dergelijke campagnes effectief is. Er is voor zover bij ons bekend tot op heden geen sterk empirisch onderzoek uitgevoerd naar de daadwerkelijke effecten van het gebruik van tegengeluiden. Daarbij dient te worden opgemerkt dat een dergelijk onderzoek ook moeilijk te realiseren is, omdat er diverse gemeten en ongemeten factoren zijn die het uiteindelijk ingewikkeld maken om bepaalde effecten aan de inzet van tegengeluiden toe te schrijven. Desalniettemin zijn er wel degelijk manieren denkbaar (bijvoorbeeld via experimenteel onderzoek) om de werkzaamheid van dergelijke aanpakken te onderzoeken. Hier komen we in de aanbevelingen op terug.

Uit de literatuur blijkt dat niet alleen onbekend is of de campagnes effectief zijn, maar ook is er veel onbekendheid over eventuele onbedoelde en ongewenste neveneffecten (Archetti, 2015; Briggs & Feve, 2013; Brouillette-Alarie et al, 2022; Ferguson, 2016; Carthy et al, 2020; Bélanger et al, 2020). Op basis van de interviews ontstaat het beeld dat respondenten doorgaans niet op de hoogte zijn van (1) óf een interventie werkt en (2) zo ja, wat dan de werkzame elementen van een interventie zijn. Bij een gebrek aan wetenschappelijke evidentie hebben respondenten uiteenlopende meningen gevormd over de werking van de inzet van tegengeluiden. Een respondent van de AIVD geeft aan bedenkingen te hebben bij de inzet van tegengeluiden. Tegengeluiden kunnen het eigen standpunt/gedachtegoed namelijk versterken, zo zou uit onderzoek blijken. Wanneer iemand online continu wordt geconfronteerd met het standpunt van ‘de tegenpartij’, kan dat ervoor zorgen dat iemand extremer wordt over het eigen standpunt, zo benoemt de respondent. Een andere respondent (ESS) benoemt echter dat de inzet van zogeheten “counter influencers”, ook wel 'credible messengers’ genoemd, wel degelijk kan werken. Het zou dan specifiek gaan om de inzet van influencers die dus al bekend zijn en veel volgers hebben. Ook hier is echter op basis van wetenschappelijk onderzoek nog onvoldoende zicht op. Een van de respondenten stipt daarbij nog aan dat terroristische en extremistische organisaties hun leden soms waarschuwen voor berichtgeving vanuit bepaalde hoeken, waarmee het mogelijke effect van tegengeluiden op voorhand al wordt ondermijnd:

“…wat echt is en wat niet, dat is misschien ook het probleem met die counter narratives. Op het moment dat het vanuit westerse media, politici, journalisten komt, is het voor jihadisch salafisten al nep […] hoef je er al niet meer naar te luisteren. Dat zie je dus bijvoorbeeld nu ook met de Israël-Hamas oorlog. Wat er ook wordt geschreven over Gaza met een zekere nuance, dat hoef je niet te lezen. Je broeders worden gedood, punt. Of dat ziekenhuis nou door Hamas of door Israël of door islamitische jihad is kapotgemaakt en hoeveel doden daar zijn gevallen, maak niet uit. Je hoeft westerse media niet te geloven.” (Respondent_politie_3)

5.2.3 Aanpak gericht op regulering en moderatie

Hierboven zijn maatregelen besproken die als ‘positieve maatregelen’ worden beschouwd. Onder negatieve maatregelen vallen maatregelen die tot doel hebben om online extremistisch materiaal te reguleren, verbieden of verwijderen en om mensen te straffen die dergelijke content plaatsen of gebruiken (Walker & Conway, 2015). Te denken valt aan het materiaal filteren, verstoppen, versleutelen of verwijderen, en aan de vervolging van personen die materiaal plaatsen en/of verder verspreiden (Stevens & Neumann, 2009; Hodwitz, 2020). Kort gezegd gaat het om het “ontregelen” van propaganda (Henschke & Reed, 2021). Ook hier geldt dat de maatregel een effect beoogt dat breder is dan het voorkomen van online rekrutering, maar daar uiteindelijk wel een bijdrage aan zou

kunnen leveren. Immers, extremistische content draagt op verschillende manieren bij aan de aantrekkingskracht van een extremistische groep, zo bleek in hoofdstuk 4, en het reguleren van dergelijke content kan derhalve een rol spelen in het voorkomen van online rekrutering.

5.2.3.1 Maatregelen door overheden en Europese organisaties

Een manier om extremistisch materiaal tegen te gaan is door het filteren van het internetverkeer, zoals China doet via door de overheid gecontroleerde internetproviders, of door het manipuleren van zoekresultaten of verwijderen van aanbevolen suggesties voor video's en websites waar terrorisme en extremisme wordt gepromoot (Neumann, 2013). Overheden van democratische landen zijn qua preventiemogelijkheden afhankelijk van benaderingen waarbij regulering van online materiaal zo min mogelijk in strijd is met bepaalde vrijheden, zoals het recht op vrijheid van meningsuiting (Holt et al, 2020). Toch zijn er ook verschillen tussen democratische landen. Anders dan bijvoorbeeld in de Verenigde Staten is online "hate speech" of haat zaaien in veel landen wel aangemerkt als misdrijf (Holt et al, 2020). Daarnaast hebben verschillende landen nationale wetgeving aangaande terrorisme, op basis waarvan in sommige gevallen ook online activiteiten kunnen worden vervolgd. Een voorbeeld hiervan is de UK Terrorism Act 2000, die het mogelijk maakt om individuen die in het bezit zijn van online propaganda of elektronische trainingsinstructies gerelateerd aan terrorisme te vervolgen.

Ook richten verschillende Europese organisaties zich op deze thematiek en is internationale wetgeving ingevoerd. Het bekendste voorbeeld in dit kader is Europol's Internet Referral Unit (IRU) (Henschke & Reed, 2021). Deze eenheid identificeert en monitort extremistisch materiaal online en deelt deze informatie met partnerorganisaties zoals internetproviders en sociale mediabedrijven, zodat zij zelf dergelijk materiaal kunnen verwijderen. Dit is nog los van wat bedrijven zelf identificeren en verwijderen van hun platforms. Daarnaast coördineert IRU inspanningen vanuit de EU om de verspreiding van online terroristische propaganda aan te pakken (Europol, 2023). Ook geldt binnen de EU de European Convention on Cybercrime (CoC) die het plaatsen of verspreiden van "hate speech" strafbaar stelt (Holt et al, 2020). Verder werkt de EU nauw samen met de lidstaten en de Europese Commissie voor de ontwikkeling van PERCI, die een technische oplossing biedt om de implementatie van EU-wetgeving ter bestrijding van de verspreiding van terroristische online-inhoud te vergemakkelijken (Europol, 2023). Volgens Europol (2023) zal PERCI "het uitvaardigen van verwijzingen en het doorgeven van verwijderingsbevelen aan aanbieders van hostingdiensten coördineren, terwijl de fundamentele rechten en vrijheden worden gewaarborgd."(p. 86). Verder is binnen de EU onlangs de Digital Services Act (DSA) ingevoerd. De DSA trad op 17 februari 2024 volledig in werking met als doelen "een betere bescherming van grondrechten, de aanpak van online misleiding en gebrekkige informatie, een gelijk speelveld voor bedrijven en digitale handel makkelijker maken" (Rijksoverheid, 2023). Ten aanzien van online extremisme geldt dan dat de DSA ervoor moet zorgen dat illegale inhoud en producten, uitingen van haat en desinformatie beter worden aangepakt door digitale diensten, in het bijzonder door (1) beter te controleren wat gebruikers online zien, en meer kennis over de advertenties die zij zien, (2) illegale inhoud of producten, haatuitingen en desinformatie gemakkelijk te kunnen markeren, (3) een middel voor platforms te bieden om samen te werken met "betrouwbare flaggers", en (4) verplichtingen op te leggen rond het inwinnen van informatie over bedrijven (handelaren) op onlinemarktplaatsen" (DSA verordening, NL samenvatting). Anders dan vóór de inwerkingtreding van de DSA worden platforms nu dus gedwongen om op te treden tegen illegale content (NOS, 2022). Als tech-bedrijven de fout ingaan, kunnen ze boetes krijgen tot 6 procent van de

jaaromzet. In eerste instantie ligt de verantwoordelijkheid voor de uitvoering van de nieuwe regels bij de platforms zelf. In geval van discussie gaan uiteindelijk rechters in de lidstaten erover.

Ondanks bovenstaande inspanningen en wetgeving merken verschillende respondenten op dat er een spanningsveld is tussen wet- en regelgeving en dat wat er in de praktijk gebeurt of kan gebeuren. Een respondent binnen de lokale overheid benoemt hoe het als overheid lastig is om iets te doen aan betere regulering en moderatie:

"Ik denk dat er echt veel te weinig momenteel gebeurt [door tech-bedrijven] en dat je als overheid daar iets mee moet. Maar dan heb je het meteen over als Nederland zijnde kun je heel weinig dus dan moet je gaan samenwerken [met de EU]…Ja dus dat weten we allemaal wel, dat dat moet, maar dat het heel lastig is. Het gaat heel traag en het is allemaal moeilijk." (Respondent_gemeente_1)

Een andere respondent binnen de lokale overheid benoemt de spanning tussen meer zicht krijgen op de online wereld vanuit hun werkzaamheden en wet- en regelgeving:

"*Ondertussen hebben we in 2018 de AVG gekregen, de politie trekt zijn troepen terug qua delen [van informatie], de GGZ en de zorg deelt al helemaal niet. Dan hebben we straks een wet op PGA [persoonsgerichte aanpak], een wettelijke grondslag, maar we worden helemaal de mond gesnoerd omdat de privacy zo hoog in het vaandel staat. Dan hebben we ook nog [de] online component. Soms denk ik, ik zeg het je eerlijk en ik doe dit al [meer dan 10 jaar], hoe moet ik in vredesnaam mijn werk doen? …Het word je onmogelijk gemaakt door al onze wet- en regelgeving. We moeten echt niet cowboyen en we moeten niet mensen zo maar op een lijst zetten, en natuurlijk moet je hier integer mee omgaan, maar het wordt ons wel heel moeilijk gemaakt."* (Respondent_gemeente_3)

5.2.3.2 Maatregelen door private en publieke partijen

Private partijen, zoals sociale mediabedrijven en internetproviders, spelen ook een belangrijke rol in preventie en interventie aangaande online rekrutering. De verantwoordelijkheid voor het controleren en verwijderen van materiaal ligt grotendeels bij hen (Holt et al, 2020). Voor het modereren maken zij gebruik van arbeidskrachten en geautomatiseerde hulpmiddelen om extremistische inhoud te identificeren, gebaseerd op de eigen richtlijnen van elk platform (Fishman, 2019). Platforms zijn verantwoordelijk voor het handhaven van deze richtlijnen en verwijderen regelmatig inhoud en blokkeren gebruikers die in strijd handelen met de richtlijnen die zij hebben opgesteld op het gebied van ongepaste inhoud, haat zaaiende uitlatingen, ondersteuning of viering van terrorisme, of spam (Ganesh & Bright, 2020). Daarnaast is er ook de optie om online extremistisch materiaal moeilijker vindbaar te maken (Henschke & Reed, 2021).

Waar private partijen eerder vaak aangaven gebruikers en groepen niet te willen beperken in hun rechten, en daarom bijvoorbeeld gebruikers niet te censureren, zijn sommige sociale mediabedrijven toch actiever geworden in dat opzicht. Onder druk van verschillende overheden, die benadrukken dat de sociale media platforms worden aangewend als radicaliserings- en rekruteringsmiddel, waren verschillende bedrijven ook al voor de invoering van de DSA proactief gebruikers aan het verwijderen (Holt et al, 2020, p. 132). In de literatuur worden verschillende voorbeelden beschreven van vrij rigoureuze schorsings- en verwijderingsacties door bepaalde platforms. Zo wijzen twee Amerikaanse onderzoekers op een aantal blog-posts uitgebracht door voormalig Twitter. In 2016 werd in een

dergelijke post beschreven dat het bedrijf sinds 2015 meer dan 125.000 accounts had geschorst vanwege het dreigen met of promoten van terroristische acties, met name gerelateerd aan IS. In een latere post gaf het bedrijf weer dat het grootschalig schorsen van 'pro-IS-accounts' continueerde in 2016 en 2017 tot op het punt dat in 2018 kon worden gesteld dat 'IS's presence on most major sociale media platforms is a tiny fraction of what it once was' (zie Scrivens & Conway, 2019). Een belangrijke vraag is dan in hoeverre dergelijke acties effectief zijn in het tegengaan van online rekrutering en aanverwante processen. Op basis van wetenschappelijk onderzoek uitgevoerd tijdens de bovengenoemde grote schorsingsacties, ontstaat het beeld dat dergelijke acties in ieder geval effect hebben op de reikwijdte van de terroristische organisatie, op de netwerkvorming en op de hoeveelheid extremistisch materiaal. Zo analyseerden Berger en Perez (2016) op Twitter een online netwerk van Engelstalige IS-aanhangers in 2015. Op basis van het onderzoek concludeerden de onderzoekers onder meer dat de schorsingen effectief waren in de zin dat er (logischerwijs) veel minder IS-accounts waren, dat de betreffende accounts daarna veel minder volgers hadden, dat nieuw aangemaakte accounts veel minder volgers aan zich wisten te verbinden en dat de schorsingen met zich meebrachten dat extremistische content sterk verminderde (omdat bij een schorsing ook alle oude berichten worden verwijderd). Hoewel de invloed van dergelijke ontwikkelingen op de terroristische organisatie in het geheel moeilijk meetbaar is, wordt in de literatuur wel genoemd dat deze aanpak IS een slag heeft toegebracht (Berger & Perez, 2016).

Ook in de Nederlandse context wordt gewezen op het belang van contentmoderatie door platforms, al wordt geconstateerd dat de echt extremistische content al snel heeft plaatsgemaakt voor borderline content die zich moeilijker laat modereren. Een respondent die werkt binnen de rechtshandhaving zegt hier het volgende over:

"Het heeft natuurlijk ook te maken met de controles op de platforms…In het verleden zag ik op Facebook ook echt wel de bloederige filmpjes, nou dat zie je nu eigenlijk gewoon niet. Maar op Facebook zie je wel preken, de oproepen tot doneren, de oproepen tot bidden voor, tot je steun uitspreken voor, en door verwijzingen dus, naar Telegram. Dat maakt het soms ook, dat men op Facebook die verschillende profielen in stand kan houden, heeft ook te maken met dat ze gewoon met heel veel omhaal van woorden…En de theologische onderbouwing. Terwijl op Telegram heb je meer de pats boem instructiemateriaal, oproepen tot. Ook wel theologische onderbouwing, maar zeker ook een combinatie met gewoon de korte instructies tot bommen maken, messen pakken, auto's en aan de slag. Dat zie je natuurlijk op Facebook niet, want dan verdwijn je heel snel ervan."
(Respondent_politie_3)

Verder hebben sociale mediabedrijven ook relaties ontwikkeld met specifieke maatschappelijke organisaties die zij hebben geselecteerd als 'trusted flaggers' van potentieel extremistisch materiaal (Fishman, 2019, p. 93). Trusted flaggers kunnen worden omschreven als "instanties of personen met bijzondere expertise en competentie voor het opsporen, identificeren en melden van illegale content of andere overtredingen van de wet op onder meer sociale mediaplatforms" (Van Wonderen e.a., 2023, p. 9). Deze rol kan in potentie worden vervuld door een brede variatie aan instanties of personen. Van Wonderen en collega's wijzen bijvoorbeeld op de mogelijkheid om jeugdwerkers in te zetten als trusted flaggers, aangezien "zij het beste weten wat bij de jeugd actuele polariserende en radicaliserende content is" (p. 11). Uit de DSA volgt dat meldingen van deze Trusted Flaggers met voorrang moeten worden behandeld door de platforms (artikel 19). Dit vraagt evenwel om een

professionaliseringsslag onder professionals die nu al expertise hebben rond illegale extremistische content, waarbij zij ook worden getraind in het identificeren en melden van borderline content.

Het Global Internet Forum to Counter Terrorism (GIFCT) is een verdere ontwikkeling in dit kader. Het gaat hierbij om een gedeelde database met vingerafdrukken van afbeeldingen (of 'hashes') om snelle verwijdering van extremistische inhoud op platforms en websites mogelijk te maken (Ganesh & Bright, 2020). Een van de respondenten benoemt GIFCT ook:

"*Die hebben zo'n online tool en daarmee trekken zij dus elke keer alle hate speech, extremistische content, eruit en dan gaat er een melding naar Facebook en dan zijn zij verplicht volgens mij om dat binnen zoveel tijd te verwijderen. Zij doen echt super goed werk.*" (Respondent_gemeente_1)

Ook zijn computerwetenschappers en computerlinguïstiekspecialisten binnen de academische wereld en industrie bezig om betrouwbare systemen te ontwikkelen die extremistische uitingen op sociale media kunnen detecteren (Ganesh & Bright, 2020), met behulp van technieken voor tekst "mining", classificatie en beeldherkenning (zie bijvoorbeeld: Burnap & Williams, 2016; Djuric et al., 2015; Scrivens, Davies, & Frank, 2018; Van der Vegt, Mozes, Kleinberg & Gill, 2021). Daarnaast is er een toename van initiatieven uit de particuliere sector die kunstmatige intelligentie (artificial intelligence (AI)) gebruiken om extremistische inhoud op te sporen en te helpen modereren (Gallacher, 2020).

5.4 Uitdagingen om online rekrutering tegen te gaan

De hierboven besproken maatregelen en aanpakken bieden professionals op papier verschillende handvatten om een bijdrage te leveren aan het tegengaan van online rekrutering. Tegelijkertijd blijkt uit de literatuur en de interviews dat er in de realiteit diverse uitdagingen zijn die er ofwel voor zorgen dat bestaande programma's niet of niet optimaal kunnen worden uitgevoerd, ofwel vragen om een andere aanpak of doorontwikkeling van bestaande aanpakken. We bespreken hieronder een aantal van de belangrijkste uitdagingen.

Een eerste uitdaging aangaande online rekrutering is dat bijna alle online platforms eigendom zijn van, en worden gecontroleerd door, particuliere bedrijven, met daarbij als extra beperking dat de bedrijven vaak vallen onder een andere jurisdictie dan waar de gebruikers van de platforms zich bevinden. Een ontwikkeling die preventie en interventie ook bemoeilijkt is dat gedecentraliseerde platforms zoals Telegram, die extra lagen van anonimiteit en gegevenscontrole bieden, aan populariteit winnen binnen gewelddadige extremistische en terroristische kringen (Europol, 2023). Video gaming platforms (bijvoorbeeld gaming communicatie apps), versleutelde communicatie toepassingen (bijvoorbeeld end-to-end versleuteling) en de zojuist benoemde gedecentraliseerde technologieën worden uitgebuit door extremistische organisaties met als doel rekrutering en het verspreiden van propaganda (Europol, 2023, p. 19). Het gebruik van deze platforms bemoeilijkt bestaande maatregelen om extremistische en terroristische content te identificeren en verwijderen.

Een tweede uitdaging is dat er een schijnbaar oneindige hoeveelheid extremistische propaganda is gepubliceerd op verschillende platforms, en dat het onmogelijk is om al deze propaganda te identificeren en verwijderen (Zeiger & Gyte, 2021, p. 359). Een van de respondenten uit de rechtshandhaving benoemt:

"En weer dat probleem van die enorme hoeveelheid dus waar kijk je naar en vindt dan die Nederlands haakjes..." (Respondent_politie_3)

Ook al is een aantal platforms strenger geworden in wat wel en niet op hun platform kan worden geplaatst, dan vinden gebruikers manieren om dat te omzeilen en lijken platforms minder strikt de afgelopen jaren:

"[Op] Twitter [inmiddels X] zie je ook nog steeds heel makkelijk [problematisch materiaal]. Facebook is een tijdje wat minder geweest, heb ik het idee. Ik heb het over een jaar, twee jaar geleden, en is nu weer… alles staat erop. En niet zo zeer dat het op Facebook zelf staat, maar het verwijst weer door naar Telegram of naar andere groepen. Dingen als Pastebin en dat soort sites waar dan de propaganda achter zit…. ik denk aan de ene kant dat ze wat manieren hebben gevonden om algoritmes te omzeilen. Dus minder expliciete IS-plaatjes bijvoorbeeld en meer signalen naar elkaar toe dat ze op die weg zitten. Dat is één en in de tweede plaats zal er vast een capaciteitsgebrek daar zijn. Dat kan niet anders, ja, [problematisch materiaal] staat [er] zo weer op." (Respondent_politie_3)

Een andere respondent werkzaam bij de lokale overheid benoemt iets soortgelijks:

"Telegram is natuurlijk Russisch dus daar hebben we natuurlijk geen enkele invloed op, maar dan ontstaat er wel weer een nieuw kanaal denk ik. Dat hebben we in de afgelopen jaren zo vaak gezien. Het is goed dat het op grote kanalen zoals YouTube en WhatsApp, dat Meta dat doet, want dan kan je ook een gros van de jeugd beschermen. Als kinderen en jongeren online zitten en ze kijken op de reguliere kanalen dan worden ze daar niet aan blootgesteld maar de mensen die het echt zoeken worden heel snel doorgeleid…" (Respondent_gemeente_3)

Wat de respondenten beschrijven sluit aan bij het idee dat zogeheten "borderline" content of "legal yet harmful" content zeer moeilijk tegen te gaan is. Het gaat dan niet om juridisch strafbaar materiaal, maar wel om materiaal dat de veiligheid van burgers en instituties mogelijk ondermijnt, "bijvoorbeeld doordat het aanzet tot haat of opruiing of omdat de content extremistisch gedachtegoed normaliseert" (Ministerie van Justitie en Veiligheid, 2023, p. 2). Dit type content is nog veelvuldig makkelijk vindbaar en dat bemoeilijkt ook de moderatie. Afgaande op hoofdstuk 4, waarin we vaststellen dat dit type materiaal een belangrijke rol kan spelen in de eerste fase van het proces van online rekrutering, is dit een van de belangrijkste uitdagingen.

Een derde belemmering is capaciteitsgebrek bij organisaties die zich bezighouden met (online) radicalisering en rekrutering. Verschillende respondenten die werken binnen de Nederlandse rechtshandhaving merken op dat bijvoorbeeld moderatie hierdoor ingewikkeld is. Een van hen geeft aan: het aanbod van (mogelijk) extremistische content en online groeperingen is gigantisch, waardoor je nooit genoeg medewerkers hebt om dit te monitoren. Bovendien gaat maar een heel klein deel van de mensen die extremistisch materiaal plaatsen over tot offline actie. Met monitoring wordt niet het onderliggende probleem opgelost. Dit capaciteitsgebrek speelt niet alleen in relatie tot content-moderatie, maar ook in de andere aanpakken. In relatie tot weerbaarheid en preventie, noemt een aantal respondenten het wegbezuinigen van jongerenwerk. Daarnaast benoemen ze dat professionals

zoals eerstelijnswerkers vaak al veel taken hebben, en dat het daarom lastig is om de online component mee te nemen in hun werk.

Als vierde uitdaging komt naar voren dat sommige professionals en organisaties zich nog onvoldoende bewust zijn van online gevaren en wat ze online wel en niet mogen in het kader van hun werkzaamheden. Verschillende respondenten merken op dat het ontbreekt aan richtlijnen over wat jongerenwerkers, gemeenten en eerstelijnswerkers mogen op het gebied van het online domein, en dat er behoefte is aan duidelijke handvatten en handelingsperspectieven. Uit verschillende interviews komt naar voren dat zowel professionals als ouders worstelen met een gebrek aan zicht op de online leefwereld van jongeren, en dat dat voor een deel voortkomt uit een onwetendheid over wat het online domein precies inhoudt en wat zich daar kan afspelen. Zo benoemt een respondent:

"Er wordt ook gezegd dat heel veel last gelegd wordt bij de ouders, maar dat de ouders eigenlijk zelf ook geen idee hebben hoe ze hun kinderen moeten begeleiden met betrekking tot online, want in hun tijd was dat er allemaal niet, dat hebben ze niet gezien, niet gekregen van hun eigen ouders dan, dus die zijn ook een beetje aan hun lot overgelaten." (Respondent_ESS_1)

Een vijfde uitdaging is het gebrek aan inzicht over de effectiviteit van bestaande aanpakken. Onderzoek naar de effectiviteit van de preventie en bestrijding van online rekrutering en mobilisatie is er tot op heden maar mondjesmaat (o.a., Chatfield, Reddick & Brajawidagda, 2015, p. 243). Het effect van campagnes om online propaganda en radicalisering tegen te gaan is nog nauwelijks onderzocht.[3] Dit geldt ook voor preventie- en interventiemaatregelen aangaande het tegengaan van gewelddadige radicalisering in het algemeen (zie bijvoorbeeld de systematische review van Brouilette-Alarie et al, 2022), nog los van de online component. Waar het gaat om het inzetten van contra-narratieven/boodschappen online blijkt dat het moeilijk is vast te stellen of ze daadwerkelijk (het gewenste) effect hebben (Archetti, 2015; Briggs & Feve, 2013; Brouillette-Alarie et al, 2022; Ferguson, 2016; Carthy et al, 2020; Bélanger et al, 2020) en zijn er indicaties dat ze soms zelfs het tegenovergestelde effect hebben (Carthy et al, 2020; Bélanger et al, 2020). Tot slot beoordelen de evaluaties van online "countering violent extremism (CVE)"-campagnes veelal niet de impact van de campagnes op de houding en/of het gedrag van de doelgroep (Helmus & Klein, 2018).

5.5 Aanvullende mogelijkheden en verbeterpunten

Op basis van de ervaringen van de respondenten en de uitdagingen waar zij tegenaan lopen, zijn gedurende de interviews verschillende mogelijke verbeterpunten aangevoerd. Daarnaast worden in de literatuur ook suggesties gedaan voor de (door)ontwikkeling van programma's ter preventie van online rekrutering. We bespreken de belangrijkste punten hieronder.

[3] Eerder in dit hoofdstuk wordt een tweetal evaluaties ("Operation250", "Under Pressure") aangehaald waaruit naar voren komt dat er wel iets meer bewustzijn wordt gecreëerd onder jongeren, maar dat bijvoorbeeld de duur van het effect onduidelijk is.

5.5.1 Aanbevelingen uit de literatuur

In de literatuur wordt veel aandacht besteed aan technische mogelijkheden om extremistisch materiaal tegen te gaan. Met betrekking tot het detecteren van online extremistisch materiaal wordt aangeraden om regelmatig trefwoorden, zoeklijsten en datasets bij te werken (zie bijvoorbeeld: Ul Rehman et al, 2021; Araque & Iglesias, 2020). Dit zou kunnen helpen extremistische inhoud op sociale media in realtime te identificeren (Akram & Nasar, 2023). Daarnaast kan strategische communicatie ook helpen bij het aan het licht brengen en tegengaan van door extremisten gebruikte strategieën voor het aanleveren van materiaal en de betrokkenheid bij de doelgroep (Ganesh & Bright, 2020). Ganesh en Bright (2020) stippen aan hoe open-source AI-middelen voor de detectie van extremistisch materiaal de mogelijkheden en beperkingen van technische systemen in 'preventing and countering violent extremism'-beleid blootleggen. Tevens benoemen ze het belang van het identificeren van uitdagingen die deze AI-software moet overwinnen voordat het kan worden ingezet als alternatief voor door mensen beheerde moderatie (zie ook: Hall et al, 2020).

Waar het gaat om online rekrutering benadrukken Williams en Tzani (2022) de noodzaak van verder onderzoek naar het taalthema 'algoritmische taal'. Zo kunnen potentiële problemen worden geïdentificeerd in de huidige algoritmische software waar extremisten misbruik van maken voor rekrutering. In hun overzichtsstudie naar online extremistische communicatie en discussie tonen ze ook de geregelde aanwezigheid van positieve framing door extremisten online, waarbij een extreme ideologie op een humorvolle en joviale manier wordt gepresenteerd via positief taalgebruik (zie bijvoorbeeld: Huey, 2015). Williams en Tzani beargumenteren dat dit in toekomstig onderzoek moet worden meegenomen bij het verkennen van thema's en trefwoorden die kunnen worden opgenomen in hun algoritmen voor het detecteren van extremisme in online-omgevingen. Daarnaast noemen ze dat door problemen binnen algoritmische software te identificeren, zoals welke taaltypologieën en extremistische terminologieën niet worden gedetecteerd, de software kan worden aangepast zodat nauwkeuriger extremistisch materiaal wordt gedetecteerd waardoor vervolgens de kans verkleind wordt dat gebruikers van deze sites worden blootgesteld aan extremistisch materiaal. Waar het gaat om rekrutering kunnen taalsubsets van het taalkundige thema 'rekruteringstaal' worden gebruikt als identificatiemarkeringen voor online extremistische rekruteurs, waardoor websitebeheerders en wetshandhavers worden geholpen bij het opsporen van deze gebruikers, en zo hebben zij ook de optie om platformgebruikers voor te lichten over hoe zij online extremisten kunnen herkennen.

5.5.2 Verbeterpunten op basis van interviewresultaten

Naast het doorzoeken van literatuur is ook tijdens de interviews gevraagd naar wat nodig is om online rekrutering voor extremistische groepen tegen te gaan. Het gaat dan vooral over wat de respondenten vanuit hun dagelijkse werkervaring zien als verbeterpunten ten aanzien van online rekrutering en meer in het algemeen online radicalisering. Ten eerste geven vijf respondenten (Respondent_LSE_1, Respondent_politie_2, Respondent_AIVD, Respondent_gemeente_1, Respondent_gemeente_2) aan dat het zou helpen als platforms zelf beter en meer ingrijpen. Eén van hen (Repondent_politie_2) geeft aan dat de vrijheid van meningsuiting op fora/apps niet in verhouding staat tot de hoeveelheid ernstige strafbare feiten (in algemene zin) die hun oorsprong vinden op dit soort fora/apps. Twee respondenten benoemen het belang van signaleren door platforms zelf, waarbij het niet alleen gaat om het verwijderen van materiaal maar ook om daar melding van te maken. Zo noemt een medewerker binnen de lokale overheid:

"Ik denk dat daar wel een beetje de kern van het probleem ligt. Op heel veel platforms als Facebook en Instagram moet je eerst melding maken. Dan is het al gezien. Ik denk dat daar ook een beetje de crux zit vaak. Uiteindelijk wordt het wel verwijderd maar dan ben je twee weken verder."
(Respondent_gemeente_2)

Eerder in dit hoofdstuk verwezen we in dit kader naar het belang van de DSA. Daarnaast beschreven we ook de contourenbrief die recent is verschenen over een "Versterkte Aanpak Online" in Nederland. Daarin wordt benoemd dat de Nederlandse overheid een structurele dialoog met de internetsector (grote platforms, aanbieders van hostingdiensten en datacenters) wil opzetten om hun rol en verantwoordelijkheid bij het modereren van 'legal yet harmful' content meer te benadrukken.

Ten tweede benoemen verschillende respondenten het verbeteren of intensiveren van samenwerking tussen instanties, waarbij meer informatie kan worden gedeeld en verschillende expertises worden gebundeld.

"In omringende landen gebeuren hele interessante zaken als het gaat over samenwerkingen. Als hulpverlenende instantie kunnen we natuurlijk niet gaan OSINT'en; op bepaalde fora rond gaan hangen om daar informatie uit te krijgen. Maar bijvoorbeeld in Duitsland zie je dat bepaalde bureaus en NGOs zijn opgestart die de hele dag niks anders doen dan kijken naar retorieken, benoemingsmethoden, en symboliek. Een soort fenomeenanalyse overhandigen aan een exit organisatie […] waardoor je eigenlijk dagelijks inzage hebt in die verandering daarin. Dat is in Nederland niet maar dat is heel handig." (Respondent_LSE_2)

Een respondent vanuit de rechtshandhaving oppert om ook de samenwerking tussen rechtshandhavingsdiensten te verbeteren, want nu wordt onderzoek soms twee keer uitgevoerd omdat informatie niet mag worden gedeeld. De verdeling van werkzaamheden komt ook terug in een opmerking vanuit de lokale overheid:

"Ik denk dat de crux moet zitten in duidelijkheid van bevoegdheden, wie, wanneer. En dat de samenwerkingsverbanden goed vastgelegd worden in zo'n PGA, radicaliseringsmethodiek. Dat je [die] online component heel goed meeneemt ook als je een casus weegt. Anders zit je alleen maar met blinde vlekken casuïstiek te draaien."
(Respondent_gemeente_2)

Als het gaat om die online component mee kunnen nemen in het werk noemen respondenten werkzaam bij de overheid, ten derde, de meerwaarde van duidelijke richtlijnen over wat zij wel en niet mogen op het gebied van het online domein. Bijvoorbeeld of zij inzicht mogen hebben in online bezigheden of accounts van mogelijk geradicaliseerden. Deze richtlijnen lijken nu te ontbreken en daardoor ook de verdere professionalisering op dat vlak. Een van de respondenten benoemt:

"Ja, beleid helpt altijd wel en dan bedoel ik, veel manifesteert zich natuurlijk lokaal maar het helpt ook als je landelijk beleid hebt die als richtlijnen kunnen dienen voor gemeenten."
(Respondent_ESS_2)

Een ander geeft aan:

"…het [is] heel vaag wat we wel en niet mogen…Wij zijn denk ik ook door [de] AVG […] heel terughoudend geworden. Dat we eigenlijk zoiets hebben van: "Dan doen we wel helemaal niks", terwijl we volgens mij wel iets meer kunnen dan wat we nu doen. Alleen omdat we gewoon bang zijn dat we het fout doen, doen we niks. Ik denk een stukje opheldering van waar zit nou eigenlijk die scheidslijn, ik denk dat we daar wel veel behoefte aan hebben." (Respondent_gemeente_1)

In het kader van verdere professionalisering werd nog een aantal andere suggesties gedaan tijdens de interviews. De onderstaande suggesties kwamen niet, zoals de bovengenoemde aanbevelingen, veelvuldig naar voren tijdens de interviews. Desalniettemin worden ze hier benoemd, omdat ze op basis van de eerdere bevindingen mogelijk kunnen bijdragen aan bestaande initiatieven.

Allereerst geeft een respondent binnen de (lokale) overheid aan dat het belangrijk is dat er meer duidelijkheid is over waar je terecht kunt als je als professional die veel met jongeren werkt, bijvoorbeeld voetbaltrainers, signalen opvangt van online problematische gedrag. Een andere respondent uit hetzelfde domein stipt aan dat de lokale overheid meer mensen zou moeten aantrekken die veel verstand hebben van internet en IT, waardoor gemeenten bijvoorbeeld meer interne kennis in huis hebben over de online wereld.

Eerder in dit hoofdstuk werd benoemd dat het belangrijk is om te praten met jongeren over hun gedachtegoed, zonder hen te veroordelen. Verschillende respondenten benoemen dat het belangrijk is dat instanties zich meer gaan richten op de context/voedingsbodem van online radicalisering en rekrutering, in plaats van te focussen op de strafbaarheid van (online) gedrag. Voor de rechtshandhaving gaat het dan vooral over meer kijken naar netwerken en de context waarin uitingen worden gedaan, voor lokale overheden en eerstelijnswerkers gaat het ook over perspectief bieden aan jongeren en volwassenen die vastlopen in een extreem gedachtegoed. Daar is volgens hen winst te behalen. Twee respondenten vanuit de rechtshandhaving merken ook op dat mensen niet meteen door een strafrechtelijke molen moeten gaan. Zo beschrijft een van hen:

"…gewoon bij iemand op de stoep staan en zeggen 'hallo, ik ben van de politie. Jij bent een ongelooflijke, opruierende figuur op internet. We kunnen twee dingen doen, we nemen jouw computer mee of we gaan eens even een goed gesprek voeren'. Dat soort dingen, dat vind ik een aantrekkelijker perspectief dan mensen helemaal door die strafrechtelijke molen te laten gaan. Zeker als ze nog superjong zijn. Want dan voelen ze misschien ook wel dat ze een tweede kans krijgen. Ik denk dat dat ook heel belangrijk is. Maar die tweede kans moet niet na de spreekwoordelijke 14 dagen voorarrest en een voorwaardelijke straf van twee maanden komen die nog [een paar jaar] blijft staan of zo…Dat vind ik niet echt de oplossing…Ik zou veel liever hebben dat je tegen zo iemand zegt 'oké goed, jij gaat vanaf nu echt intensief praten over dit gedachtegoed. En niet meer met je vrienden maar met ons of met iemand uit de hulpverlening'." (Respondent_politie_1)

Als iemand wel in de strafrechtelijke molen is beland, dan benoemt diezelfde respondent het volgende:

"…een soort langdurig begeleidingstraject vind ik veel aantrekkelijker dan een gevangenisstraf bijvoorbeeld. Met zo'n begeleidingstraject gaat het ook om mensen die naar ze luisteren en een

gesprek met ze aan kunnen gaan en die dus ook een soort moreel weerwoord kunnen bieden. Dat is denk ik ook af en toe wel heel belangrijk want veel van deze mensen krijgen alleen maar te horen 'mag niet, strafbaar feit, foute boel' maar hun gedachtegoed blijft natuurlijk hetzelfde en daar zijn die strafbaar feiten uit voortgekomen." (Respondent_politie_1)

Tevens wordt benoemd dat kennis over het online domein moet worden vergroot onder professionals en ouders. Diverse respondenten benoemen daarbij het belang van het betrekken van degenen die het meest vatbaar zijn voor online rekrutering, en dat zijn vaak jongeren. Twee respondenten (Respondent_ESS_1, Respondent_jongerenwerker_2) benadrukken het belang van jongerenparticipatie expliciet. Een van hen verwoordt het als volgt:

"Ik vind die alliantie vormen gewoon heel belangrijk. Dat we er samen aan werken want dat is toch democratie, dat als je het met z'n alle doet en iedereen is vertegenwoordigd… vooral de jongeren natuurlijk. We zeggen vaak jongerenparticipatie maar de uitvoering is best wel slecht. Dat gesprek toen met TikTok daar zaten de jongeren ook niet aan tafel. Dan wordt er wel gezegd dat zij werken aan jongerenparticipatie maar niet goed genoeg." (Respondent_jongerenwerk_2)

Een andere respondent benoemt de wens vanuit professionals om input te krijgen van jongeren:

"…[een] eerste bijeenkomst gehad waar we de behoeftes hebben opgehaald van waar is behoefte aan vanuit de gemeente en professionals…tijdens elke sessie, elke ronde is nadrukkelijk gezegd dat de jongeren daarbij betrokken moeten worden. Dat ze dat heel erg missen op alle vlakken, alle niveaus. Heel veel jongerenwerkers zeiden 'we weten niet hoe het werkt, wat de trends zijn, wat er leeft'. Docenten gaven het ook aan. En dan was heel erg de neiging om te zeggen 'laat de jongeren dan weer leren wat er nu gaande is, wat je nodig hebt op het gebied van online'. Ook met beleid, dat je ze erbij moet betrekken want het gaat om hun leefwereld en wij proberen dan allerlei dingen te bedenken om ze te tegenhouden of preventieve maatregelen in te voeren, maar laten we met een gesprek gaan, wat zij nodig hebben, waar zij tegenaan lopen of wat zien zij dan. Maar dat kwam echt heel nadrukkelijk elke keer naar voren, betrek jongeren erbij." (Respondent_ESS_1)

Ook zien twee respondenten (Respondent_LSE_1, Respondent_jongerenwerker_2) meerwaarde in zelf meer zichtbaar aanwezig zijn in het online domein, als aanspreekpunt voor jongeren maar ook om zicht te krijgen op wat er online gebeurt:

"We hebben in [stadsdeel] Snapchatspecialisten, ook in [ander stadsdeel] trouwens. Een aantal jongerenwerkers die zijn gewoon heel bedreven […] en die zitten midden in die Snapchsatgroepen eigenlijk." (Respondent_jongerenwerk_2)

5.6 Tot slot

Met de realisatie dat het online domein een belangrijke rol kan spelen in radicaliserings- en rekruteringsprocessen zijn steeds meer initiatieven ontwikkeld om dergelijke processen te voorkomen. Naast verschillende internationale initiatieven, zoals de DSA, is een Nederlands voorbeeld hiervan de eerder besproken "Versterkte Aanpak Online" waarin wordt beoogd om de verantwoordelijkheid van

de internetsector te vergroten, aansluiting te vinden bij nieuwe (internationale) coalities, interventies en het stimuleren van meer onderzoek te bevorderen en het belang van onderlinge samenhang van online maatregelen te benadrukken.

De in dit hoofdstuk beschreven maatregelen zijn gericht op het vergroten van (online) weerbaarheid, het bieden van tegengeluiden en het modereren en reguleren van de online wereld. Elke aanpak kent verschillende voordelen, maar ook diverse uitdagingen, zo bleek op basis van de interviews en de literatuur. Een belangrijke constatering is dat programma's gericht op het vergroten van weerbaarheid via schoolprogramma's en het inzetten van tegengeluiden een zeer beperkte dan wel ontbrekende evidence-base hebben, waardoor vaak ook onduidelijk is wat de eventuele werkzame elementen van deze aanpakken zijn. Professionals benoemen dan ook behoefte te hebben aan meer kennis over 'wat werkt'. Daarom is het belangrijk dat programma's en aanpakken die worden ingevoerd in het kader van het tegengaan van online radicalisering en online rekrutering gedegen en structureel worden geëvalueerd, zodat duidelijk wordt wat de werkzame elementen zijn en waar mogelijkheden liggen ter doorontwikkeling.

Ten aanzien van bestaande programma's werd voorts benoemd dat deze over het algemeen kortdurend zijn, bijvoorbeeld in de vorm van een aantal lessen op scholen over online risico's. Meerdere respondenten wezen op het belang van meer structurele preventieprogramma's om bewustwording en gedragsverandering ten aanzien van online gevaren te bewerkstelligen. Hierbij werd tevens genoemd dat de snelle ontwikkelingen maken dat ouders en professionals niet altijd over voldoende kennis en vaardigheden beschikken ten aanzien van het online domein. Preventieprogramma's zouden daarom nog meer handvatten moeten bieden aan ouders en professionals ten aanzien van het bijhouden van digitale kennis en het zicht houden op de activiteiten van jongeren in de online wereld. Een aantal respondenten wees op het belang van jongerenparticipatie, zodat een beter beeld kan worden verkregen van de online leefwereld en de mogelijk schadelijke content waar de jongeren aan worden blootgesteld. Belangrijk om te noemen is dat een heel aantal jongeren in aanraking komt met 'legal yet harmful' materiaal, maar het grootste deel van deze jongeren sluit zich niet aan bij een extremistische groep. Om die reden lijkt het ook van belang om in vervolgonderzoek te kijken naar welke factoren er bij hen voor zorgen dat ze dit pad niet inslaan.

Veel aandacht is tot slot besteed aan nationale en internationale wet- en regelgeving op basis waarvan in de komende jaren meer verantwoordelijkheid wordt gelegd bij de online platforms zelf als het gaat om moderatie en regulering. Gelet op het eerder besproken belang van de verspreiding van 'legal yet harmful' materiaal in generieke rekruteringsprocessen is het belangrijk dat platforms meer aandacht gaan besteden aan dergelijke content. Dat wordt zowel uit de literatuur als op basis van de interviews duidelijk. De uitdaging daarbij is wel om dergelijke content tegen te gaan zonder belangrijke rechten en vrijheden zoals de vrijheid van meningsuiting met voeten te treden en te blijven nadenken over welke mate van regulering en moderatie wenselijk is. Dit dilemma kwam ook naar voren tijdens de expertmeeting, waarin we met een groep onderzoekers en professionals (zie ook hoofdstuk 3) hebben gereflecteerd op de resultaten en geïdentificeerde uitdagingen. Er wordt op dit moment meer wet- en regelgeving ingevoerd, maar daarbij is het belangrijk om de proportionaliteit van de maatregelen in ogenschouw te blijven nemen.

6. Slothoofdstuk

In de laatste jaren is steeds duidelijker geworden dat internet en sociale media een cruciale rol spelen in processen van radicalisering en rekrutering. In de Nationale Contraterrorisme Strategie 2022-2026, het meest recente Dreigingsbeeld Terrorisme Nederland (DTN60; NCTV, 2024) en het recente jaarverslag van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD; 2024) wordt op verschillende manieren verwezen naar de rol van internet en sociale media. Zo wordt in de Nationale Contraterrorisme Strategie benoemd dat “de rol die internet en sociale media spelen bij radicalisering en terroristische voorbereiding niet genoeg kan worden benadrukt” (p. 15) en wordt in het dreigingsbeeld gewezen op de rol van de online wereld in onder meer radicaliseringsprocessen, netwerkvorming en het aantrekken van jongeren met een al bestaande “geweldslust en drang om te choqueren” (NCTV, 2024, p. 4). In de bespreking van een aantal verijdelde aanslagplots benoemt de AIVD voorts dat verijdelde aanslagen in sommige gevallen waren gepland door “nieuwe, online gevormde groepen, die in Europa waren geradicaliseerd en die contact zochten met ISIS” (p. 9). Deze voorbeelden maken het belang duidelijk van een evidence-base op basis waarvan preventie- en interventieprogramma’s kunnen worden (door)ontwikkeld. Hoewel er vanuit wetenschappelijk onderzoek al veel bekend is over online radicalisering, is het zicht op processen van online rekrutering nog veel beperkter. Het huidige onderzoek had daarom als doel om in kaart te brengen hoe online rekrutering door en voor rechts-extremistische, jihadistische, anti-institutionele en links-extremistische groeperingen verloopt. Op basis van een literatuuronderzoek, interviews, een kwalitatieve contentanalyse van sociale media platforms en een expertmeeting zijn de volgende overkoepelende onderzoeksvragen opgesteld:

1) Wat is uit de literatuur en de praktijk bekend over de aard en mechanismen van online rekrutering en mobilisatie?

2) In hoeverre is er een wisselwerking tussen online rekrutering en offline gedrag?

3) Welke handelingsperspectieven en aanpakken zijn beschikbaar/geschikt voor instanties die zijn belast met de aanpak van extremisme?

In dit samenvattende slothoofdstuk bespreken we eerst de basiskenmerken van de gevolgde onderzoeksmethode. Vervolgens bespreken we de belangrijkste onderzoeksresultaten met betrekking tot de drie overkoepelende onderzoeksvragen. In het laatste deel van dit slothoofdstuk gaan we in op een aantal beperkingen van het uitgevoerde onderzoek en worden de aanbevelingen op basis van het onderzoek geconcretiseerd (ze kwamen voor een deel al aan bod in hoofdstuk 5).

6.1 Onderzoeksmethode

Ter beantwoording van de onderzoeksvragen zijn verschillende onderzoeksmethoden gecombineerd. Allereerst is een verkenning gedaan van relevante wetenschappelijke literatuur en beleidsstukken over online rekrutering door en voor extremistische groepen. Hiertoe zijn verschillende databases geraadpleegd. Bij de zoekstrategie is rekening gehouden met de gevarieerde terminologie die wordt gebruikt in de literatuur over rekrutering in relatie tot extremisme. Bij het analyseren van de literatuur

is echter wel steeds kritisch onderscheid gemaakt tussen studies die echt gericht waren op rekrutering en studies die naar aanverwante processen keken, bijvoorbeeld online radicalisering. Op basis van de literatuur is vervolgens een topiclijst opgesteld voor interviews met twee groepen professionals, te weten medewerkers die in het kader van de handhaving, opsporing en vervolging in hun primaire werkzaamheden met online rekrutering te maken hebben en medewerkers die vanuit andersoortige functies (bijvoorbeeld in het sociaal domein) zicht krijgen op deze thematiek en problematiek. In totaal is gesproken met 14 professionals, te weten drie medewerkers van de Nationale Politie, twee van de AIVD, twee van het Landelijk Steunpunt Extremisme (LSE), twee van de Expertise-unit Sociale Stabiliteit (ESS), drie professionals werkzaam bij gemeenten en twee jongerenwerkers. Naderhand zijn de interviews systematisch gecodeerd en geanalyseerd.

Om zicht te krijgen op de mechanismen rondom online rekrutering door en voor extremistische groepen is vervolgens een kwalitatieve contentanalyse van zeven openbare online platforms uitgevoerd. Om een zo breed mogelijk beeld te krijgen hebben we ons hierbij op vier ideologische stromingen gericht, namelijk extreemrechts, extreemlinks, anti-institutioneel en jihadisme. De keuze voor specifieke groepen is gebaseerd op recente Dreigingsbeelden Terrorisme Nederland (DTN's) van de NCTV, jaarverslagen van de AIVD en mediaberichtgeving over specifieke groepen. Qua platforms hebben we ons beperkt tot Telegram en Facebook omdat deze platforms worden genoemd in het meest recente dreigingsbeeld ten tijde van de contentanalyse. Gedurende een vooraf bepaalde analyseperiode hebben we van alle geplaatste berichten schermafbeeldingen gemaakt, die vervolgens met behulp van een vooraf opgesteld codeerschema met het programma ATLAS.ti zijn geanalyseerd. Ook beeldmateriaal en videofragmenten zijn geanalyseerd. Het codeerschema is gebaseerd op de wetenschappelijke literatuur en op de eerste interviews met professionals.

Tot slot hebben we een expertmeeting met professionals en wetenschappers georganiseerd om gezamenlijk te reflecteren op de voorlopige onderzoeksresultaten, op basis waarvan we de aanbevelingen voor beleid en de praktijk konden aanscherpen.

6.2 Belangrijkste bevindingen

In hoofdstuk 4 hebben we ons gericht op de eerste onderzoeksvraag over de aard en mechanismen van online rekrutering en op de tweede onderzoeksvraag over de wisselwerking tussen online rekrutering en offline gedrag. In hoofdstuk 5 hebben we ons gericht op de derde onderzoeksvraag en onderzocht wat voor soort aanpakken er beschikbaar zijn om online rekrutering tegen te gaan, welke aanwijzingen er zijn voor eventuele effecten van deze aanpakken en welke handelingsperspectieven en verbeterpunten uit de literatuur en de interviews naar voren komen. De resultaten van beide hoofdstukken vormen de aanzet tot de overkoepelende aanbevelingen die we later in dit hoofdstuk presenteren. In wat nu volgt, geven we een overzicht van de belangrijkste bevindingen.

6.2.1 Het online domein als een unieke omgeving

Uit eerder onderzoek naar rekrutering in de offline wereld, zowel voor extremistische organisaties als voor de georganiseerde misdaad en cybercriminele groepen, blijkt dat er verschillende mechanismen zijn die kunnen leiden tot toetreding tot bepaalde groepen, met een aantal overeenkomende elementen. Leeftijdsgenoten en vrienden die al deelnemen aan een groep spelen een belangrijke rol

en dit kan de kans dat iemand zich ook aansluit vergroten. Daarentegen kan er ook sprake zijn van zelfselectie, waarbij iemand met een bepaalde achtergrond of levensloopontwikkeling er zelf voor kiest om zich aan te sluiten bij een bepaalde groep, zonder dat daar bepaalde beïnvloedingsprocessen vanuit de groepering aan vooraf zijn gegaan. In beide gevallen volgt op deze initiële stappen richting toetreding een belangrijke tweede fase, waarin nieuwe leden worden getest op betrouwbaarheid en 'echtheid'. Daarnaast kunnen personen ook zelf het initiatief nemen voor het opzetten van een eigen groep en daarbij weer anderen betrekken of rekruteren.

In ons onderzoek hebben we vervolgens gekeken in hoeverre online rekrutering specifiek door en voor extremistische groepen soortgelijke patronen kent. Voordat die vraag werd onderzocht, is allereerst gekeken naar kenmerken die uniek zijn voor de online omgeving, waarbij ook de faciliterende werking van online platforms is meegenomen. Uit de resultaten blijkt allereerst dat elders beschreven gebruiksmogelijkheden van internet en sociale media, zoals toegankelijkheid, anonimiteit, gedeelde connecties, gemakkelijke communicatie en content-uitwisseling ook een rol spelen in online rekrutering. Professionals benoemden dat de drempel om online toe te treden tot een extremistische groep veel lager ligt dan offline, bijvoorbeeld vanwege een beperktere tijdsinvestering (iemand kan met één klik lid worden van een groep en daar vervolgens een aantal berichten in delen) en het gemak waarmee iemand ook weer uit een groep kan stappen. Ten aanzien van de laagdrempeligheid werd samenvattend aangegeven dat online 'easy in – easy out' is. Een tweede belangrijk kenmerk die een rol speelt bij online rekrutering is de anonimiteit van het online domein. Deze anonimiteit werkt verschillende kanten op. Online toetreding tot een extremistische organisatie kan gebeuren zonder dat iemands offline sociale netwerk daarvan op de hoogte is en daarnaast maakt de anonimiteit dat iemand zich in de online wereld vrijer voelt om gedrag te vertonen dat hij of zij in de offline wereld niet zou vertonen. Een derde en misschien wel het meest onderscheidende kenmerk dat door respondenten uit diverse organisaties werd benoemd, betreft het feit dat internet grensoverstijgend is, waardoor fysieke nabijheid geen vereiste meer is om te rekruteren of gerekruteerd te worden. Tot slot werd als vierde factor benoemd dat het online domein een vertekend beeld kan geven van groepscohesie, de grootte en de reikwijdte van een groepering, waardoor potentiële rekruten zich eerder aangetrokken voelen tot een bepaalde groep.

Hoewel het bovenstaande betrekking heeft op het online domein in het algemeen, blijkt uit de analyse dat extremistische groepen gebruik maken van een scala aan platforms, elk met hun eigen gebruiksmogelijkheden. Hierbij gaat het zowel om mainstream sociale mediaplatforms zoals Facebook, X (voorheen Twitter), TikTok, YouTube en Instagram, als ook 'low profile' platforms zoals Telegram en Discord. Een belangrijk verschil tussen de eerste en de tweede categorie is de mate van beveiligingsmaatregelen, privacyrichtlijnen en content-moderatie. Telegram is volgens de respondenten op dit moment het meest gebruikte platform door extremistische groepen, juist omdat dit platform moeilijk te modereren is. Uit de interviews en literatuur blijkt echter dat de mainstream platforms ook belangrijk zijn, aangezien deze platforms regelmatig als doorgeefluik naar Telegram fungeren. Vanaf deze platforms worden potentiële nieuwe leden, als onderdeel van het trapsgewijze proces (zie verder onder 6.2.2), uitgenodigd voor dan wel doorverwezen naar bepaalde besloten Telegramgroepen of -kanalen.

6.2.2 Online rekrutering: Generiek en specifiek

Bij het in kaart brengen van processen van online rekrutering bleek al snel de noodzaak om te onderscheiden naar twee varianten van online rekrutering, namelijk 'generieke rekrutering' gericht op het aantrekken van een brede waaier aan individuen en 'specifieke rekrutering' gericht op bepaalde categorieën personen. Hoewel deze twee varianten in sommige gevallen in elkaar overgaan, worden ze ook afzonderlijk ingezet.

Voor wat betreft generieke rekrutering blijkt dat extremistische groepen sociale media met name gebruiken om aan 'community building' te doen en om mensen in het algemeen aan de groep te verbinden. Belangrijke aspecten van groepsvorming zijn het bevorderen van sociale cohesie binnen de groep, de vorming van een gedeeld narratief en het hebben van een gezamenlijk doel. Hierbij wordt veelvuldig gebruik gemaakt van extremistische memes en de verspreiding van ideologische berichten. Opvallend is dat de groepsvorming zich niet beperkt tot de online wereld; in alle door ons onderzochte online groepen wordt op enig moment melding gemaakt van offline groepsactiviteiten, variërend van lezingen tot gezamenlijk sporten en de organisatie van en/of deelname aan protesten. Regelmatig wordt van deze activiteiten online weer verslag gedaan. Gedurende de analyseperiode werden ook diverse berichten geplaatst waarin, in algemene zin, deelnemers en bezoekers concreet werden uitgenodigd om lid te worden van de groep.

Naast generieke rekrutering maken groepen ook gebruik van op specifieke subpopulaties gerichte rekrutering voor groepen en activiteiten. Wetenschappelijk onderzoek naar specifieke rekrutering is tot op heden met name gericht op strategieën van de wat grotere terroristische organisaties in de wereld, zoals Al Qaida en IS. Deze organisaties gebruiken internet om bepaalde subpopulaties, zoals minderjarigen of vrouwen, te bereiken en hen vervolgens met doelgerichte rekruteringsstrategieën over te halen om zich aan te sluiten bij de terroristische organisatie. Dit is een proces dat ook wel 'narrowcasting' wordt genoemd. Zo heeft Al Qaida veelvuldig gebruik gemaakt van internet om specifiek studenten en medewerkers van technische universiteiten uit de hele wereld te rekruteren. Daartoe werd online rekruteringsmateriaal in diverse talen vertaald en verspreid. Ook is IS er met behulp van sociale media in geslaagd om vele individuen, zowel lokale strijders als uitreizigers uit Europese landen en Noord-Amerika, online te rekruteren. Via het verspreiden van extremistisch wervingsmateriaal en online wervingsactiviteiten van al gerekruteerde IS-leden zijn honderden nieuwe IS-leden online gerekruteerd. Zowel Al Qaida als IS hebben in hun online strategieën ingespeeld op de belevingswereld van sociale mediagebruikers (en dus potentiële rekruten). Een duidelijk voorbeeld betreft de pogingen van Al Qaida om minderjarigen te rekruteren. De organisatie zocht online direct contact met minderjarigen en verspreidde daarbij cartoons en kinderverhalen waar extremistische narratieven in vermengd waren. Om vrouwen te rekruteren werden vrouwen direct online benaderd en ook hier speelde propaganda een belangrijke rol.

De literatuur biedt vooral zicht op specifieke rekrutering door grote internationale terroristische organisaties. Uit de interviews en content-analyse ontstaat het beeld dat dergelijke specifieke rekrutering op dit moment, binnen de Nederlandse context, niet veel voorkomt. De geïnterviewde professionals waren het er unaniem over eens dat individuen in Nederland in het algemeen in aanraking komen met een extremistische groep doordat ze zelf online op zoek gaan naar gelijkgestemden en vervolgens lid worden van een openbare groep. Indien iemand bereid blijkt zich in te willen zetten voor de groep, kan diegene worden uitgenodigd voor een besloten groep. Doorgaans

volgt daarop een doorlichtingsprocedure. Deze procedure vindt ofwel in een besloten groep plaats, ofwel offline en bestaat uit onder meer gesprekken, kennisvragen over de ideologie en vragen over de bereidheid om bij te dragen aan de doelen van de groep.
Een belangrijke constatering is dat er meer overeenkomsten dan verschillen lijken te bestaan tussen het gebruik van sociale media door de onderzochte groeperingen. Zo is in alle groeperingen sprake van online groepsvorming, worden de verschillende gebruiksmogelijkheden van het online domein actief gebruikt (onder meer via het delen van extremistische content) en wordt de ideologie verspreid. Op basis van de interviews is vastgesteld dat het hierboven genoemde trapsgewijze rekruteringsproces inclusief doorlichtingsprocedures bij uiteenlopende groeperingen binnen het rechtsextremisme, anti-institutioneel extremisme en jihadisme wordt gezien. Hoewel de geïnterviewde respondenten het gebruik van memes vooral aan extreemrechtse groeperingen toeschreven, blijkt uit de contentanalyse dat binnen alle bestudeerde groeperingen memes worden gebruikt. Op basis van de contentanalyse kan tevens worden opgemaakt dat alle groeperingen melding maken van offline activiteiten, al varieert de aard van de activiteiten per stroming. Zowel de extreemrechtse groepen als de jihadistische groepen plaatsten in de onderzochte periode berichten over gezamenlijk trainen in MMA/grappling, iets dat we niet terugzagen bij de andere twee stromingen. Een ander verschil werd gevonden in de mate waarin de groeperingen gebruikers oproepen om lid te worden van de groepering. Dergelijke oproepen werden met name gezien in de extreemrechtse en anti-institutionele groepen. Tevens werd in deze groepen vaker een concrete oproep tot actie gedaan. Hoewel we net verwezen naar eerdere grote rekruteringsacties door onder meer IS en Al Qaida, zien we dergelijke acties op de onderzochte openbare jihadistische platforms niet terug.

6.2.3 De wisselwerking tussen online en offline leefwerelden

Uit het voorgaande blijkt dat online rekrutering, in elk geval in de Nederlandse context, vaker een meer algemeen proces is waarin in eerste instantie vooral de aantrekkingskracht van extremistische groepen een rol lijkt te spelen. Door middel van die aantrekkingskracht wordt vervolgens meer generiek gepoogd leden te werven voor de organisatie. In een trapsgewijs proces dat daarop volgt kunnen nieuwe geïnteresseerden vervolgens dieper de organisatie binnenkomen, waarbij regelmatig op enig moment ook offline ontmoetingen volgen. Juist deze interactie tussen de online en offline wereld is onderwerp van interesse van zowel de wetenschap als veiligheidsinstanties en organisaties in het sociaal domein. Uit het onderzoek komt naar voren dat er op minstens drie manieren naar de wisselwerking tussen online rekrutering en de offline wereld kan worden gekeken. Ten eerste kan de offline wereld van belang zijn in de aanloop naar online rekrutering voor extremistische groepen, waarbij de situatie in de offline wereld de vatbaarheid voor online rekrutering vergroot. Respondenten uit verschillende organisaties gaven aan dat jongeren die zich aansluiten doorgaans bepaalde kwetsbaarheden hebben, variërend van psychologische kwetsbaarheden tot problemen in de thuissituatie. Daarbij werd tevens aangegeven dat deze kwetsbaarheden voor een belangrijk deel overeenkomen met kwetsbaarheden van andere groepen, zoals jongeren die worden gerekruteerd voor de georganiseerde misdaad. Belangrijk om op te merken is dat dergelijke kwetsbaarheden niet direct leiden tot groepslidmaatschap. Immers, vele mensen met soortgelijke kwetsbaarheden voelen zich niet aangetrokken tot extremistische groepen. Desalniettemin kunnen ze wel worden beschouwd als risicofactor.

Ten tweede kan online rekrutering en groepsvorming op een bepaald punt overgaan in ‘onlife’ rekrutering en groepsvorming, waarbij zowel online als offline rekruterings- en

groepsvormingsprocessen plaatsvinden. Er is, met andere woorden, een continue wisselwerking tussen de online en offline context op het gebied van organisatorische activiteiten, netwerken en propaganda. Online worden offline evenementen aangekondigd en vervolgens wordt daar online ook weer verslag van gedaan (al dan niet gepaard gaand met een oproep aan bezoekers om zich bij de groep aan te sluiten). Opvallend is dat, hoewel de nadruk in diverse dreigingsbeelden ligt op het online domein, respondenten aangeven dat ze merken dat het offline domein de laatste tijd juist ook weer een prominentere rol in lijkt te nemen, zeker in latere fasen van rekrutering. Als reden wordt een toegenomen veiligheidsbewustzijn genoemd en dan met name de realisatie van groepen dat er kan worden meegelezen door (opsporings-)instanties. Volgens een aantal respondenten leidt dit ertoe dat extremistische groepen kritischer zijn op wie er worden toegelaten tot de meer besloten groepen en ook tot een herwaardering van fysiek contact en offline ontmoetingen.

De derde relatie tussen online rekrutering en de offline wereld betreft het overgaan tot daadwerkelijke offline acties. Uit zowel de literatuur als de interviews blijkt dat de relatie tussen online en offline activiteiten ingewikkeld vast te stellen is. Er zijn enkele uitzonderingen, bijvoorbeeld de eerder genoemde rekruteringsstrategieën van onder meer Al Qaida en IS. In deze gevallen was online rekrutering duidelijk de opmaat naar offline terroristische daden, bijvoorbeeld het strijden voor een terroristische organisatie. Veel vaker is de relatie echter complexer en ook hier speelt de conceptuele vermenging een rol. Zo zijn sommige studies gericht op het verband tussen online activiteiten (en niet specifiek rekrutering an sich) en offline gewelddadigheden. Uit deze studies blijkt dat gewelddadige extremisten, meer dan niet-gewelddadige extremisten, het online domein aanwenden om onder meer voorbereidingen te treffen voor offline extremistische acties. Meer onderzoek naar hoe online rekrutering samenhangt met online mobilisering en daadwerkelijke offline gewelddadigheden is echter nodig om deze processen beter in kaart te brengen.

6.2.4 Bestaande aanpakken en handelingsperspectieven

Met de toenemende aandacht voor processen van online rekrutering hebben ook maatregelen ter preventie daarvan zich in de laatste jaren snel ontwikkeld. Daarbij is een onderscheid te maken naar de preventieve aanpak gericht op het vergroten van online weerbaarheid, de aanpak gericht op online tegengeluiden en de aanpak gericht op regulering en moderatie.

Met betrekking tot de preventieve aanpak gericht op het vergroten van de weerbaarheid blijkt dat in Nederland en ook daarbuiten met name sprake is van programma's waarmee wordt getracht om jongeren te informeren over gewelddadig extremisme, bewustwording van 'grooming' gedrag te vergroten en mediageletterdheid te verhogen. Een belangrijk overkoepelend doel is de ontwikkeling van vaardigheden om berichtgeving zelfstandig en kritisch te beoordelen, bronnen te evalueren en te bevragen en informatie die plausibel en betrouwbaar is te onderscheiden van desinformatie. Uit de analyse blijkt dat het evalueren van dergelijke programma's nog in de kinderschoenen staat, waardoor nog geen harde uitspraken kunnen worden gedaan over de werkzaamheid ervan. De evaluaties die wel zijn uitgevoerd, lijken aan te tonen dat bewustwordings- en informatieprogramma's op de korte termijn positieve effecten hebben op het bewustzijn van leerlingen ten aanzien van onder andere nepnieuws. Wel blijkt dat een meer structurele inzet nodig wordt geacht om jongeren langdurig weerbaar te maken. Verschillende respondenten onderschreven het belang van een aanpak gericht op weerbaarheid, waarbij de wens werd geuit voor verdere doorontwikkeling en handvatten voor de praktijk. Daarbij werd ook meermaals de rol van ouders aangestipt, die volgens respondenten een

cruciale rol hebben als het gaat om 'digitale opvoeding' en het online weerbaar maken van kinderen, alsmede het signaleren van ongewenste ontwikkelingen. Zeker nu kinderen op steeds jongere leeftijd online actief zijn, begint het vergroten van de weerbaarheid achter de voordeur. Respondenten benoemden daarbij dat de huidige generatie ouders daarin ook ondersteund moet worden, gelet op de snelle ontwikkelingen in het online domein.

De inzet van de tweede aanpak, online tegengeluiden, wordt uitgevoerd door zowel overheden als het maatschappelijk middenveld. Initiatieven die hiervan gebruik maken, zijn doorgaans niet specifiek gericht op het voorkomen van online rekrutering, maar beogen verschillende aan extremisme gerelateerde processen te voorkomen, waaronder ook online radicalisering. Uit onderzoek blijkt dat het onduidelijk is in hoeverre de inzet van online tegengeluiden (het gewenste) effect heeft, wat ook naar voren kwam uit de interviews. Daarnaast is er nog veel onbekend over eventuele onbedoelde en ongewenste neveneffecten, zoals de mogelijkheid dat individuen door het aanbod van tegengeluiden juist extremer worden in de eigen standpunten. Tot slot is er nog veel onbekend over de voorwaarden waaronder tegengeluiden een positief effect zouden kunnen hebben. Uit de interviews alsmede de literatuur komt daarom een behoefte naar voren tot meer wetenschappelijke kennis hieromtrent.

De derde aanpak, inzetten op het modereren en reguleren van online materiaal, gebeurt op verschillende niveaus. Zo zijn land-overstijgende organen (EU, Europol), overheden, private partijen (sociale mediabedrijven, internetproviders), maatschappelijke organisaties die worden ingezet als trusted flaggers (bijvoorbeeld GIFCT) en computerwetenschappers hier mee bezig. Door de onlangs ingevoerde Digital Services Act (DSA) worden private partijen binnen de EU gedwongen op te treden tegen illegale content, al zijn grote sociale mediabedrijven zoals Meta al een aantal jaren bezig met het modereren en reguleren van online materiaal. Dit heeft als gevolg dat expliciet beeld- en instructiemateriaal steeds meer lijkt te verplaatsen naar besloten groepen op *low profile* platforms als Telegram, zo blijkt uit de literatuur en de interviews. Nieuwe technologische ontwikkelingen, zoals technieken voor beeldherkenning en kunstmatige intelligentie, kunnen bijdragen aan het steeds beter opsporen en modereren van extremistische uitingen in het online domein.

Op basis van de interviews is een aantal obstakels en uitdagingen geïdentificeerd die de daadwerkelijke of optimale implementatie van de verschillende aanpakken in de weg staan. Ten eerste werd benoemd dat online platforms eigendom zijn van particuliere bedrijven die vallen onder andere jurisdicties dan waar hun gebruikers zich bevinden. Ten tweede werd gewezen op de enorme hoeveelheid extremistisch en terroristisch materiaal en de onmogelijkheid om al dit materiaal te modereren dan wel te verwijderen. Extra complex wordt het als het gaat om borderline content. Ten derde werd gewezen op een capaciteitsgebrek binnen zowel de rechtshandhaving als bij andere organisaties die zich bezighouden met (online) radicalisering. Ten vierde ontbreken duidelijke richtlijnen over de bevoegdheden van verschillende professionals en organisaties, onder meer ten aanzien van online activiteiten en het delen van informatie. Ten vijfde blijkt meer algemeen een gebrek aan inzicht in de algehele effectiviteit van bestaande aanpakken en de eventuele werkzame elementen daarbinnen.

6.3 Beperkingen van het onderzoek

Alvorens we nog wat uitgebreider ingaan op de aanbevelingen voor vervolgonderzoek, beleid en de praktijk, is het belangrijk om een aantal beperkingen van het huidige onderzoek te noemen. Deze beperkingen dienen in het achterhoofd te worden gehouden bij het interpreteren van de resultaten.

Met betrekking tot de interviews is een beperking dat we per instantie slechts een aantal medewerkers hebben gesproken. De inhoud van deze gesprekken hoeft niet per definitie een afspiegeling te zijn van de algehele opvattingen en ervaringen van de medewerkers van de betreffende instanties. Hieraan gerelateerd dient te worden opgemerkt dat hoewel de diversiteit aan respondenten een meerwaarde is van dit onderzoek, de resultaten afhankelijk kunnen zijn van de ervaring van de respondenten en sterk kunnen verschillen per context. Om deze reden hebben we ons in de analyse steeds gericht op gedeelde observaties en de gesprekken met de verschillende respondenten in onderlinge samenhang geanalyseerd. We beschouwen het ook als een beperking dat we geen respondenten hebben kunnen interviewen uit de tech-sector. De ondoorzichtigheid over wie zich bij de verschillende tech-bedrijven bezighouden met de thema's van het huidige onderzoek maakte het ingewikkeld om respondenten te benaderen. Daarnaast waren verschillende bedrijven niet bereid om interviews te geven, zoals bleek uit algemene statements van de bedrijven.

Ten tweede is de omvang van de contentanalyse beperkt voor wat betreft de periode van onderzoek en daaraan gerelateerd het aantal geanalyseerde berichten. Op voorhand was bepaald dat dit onderdeel van het onderzoek een sterk exploratief karakter zou hebben. Een langere analyseperiode en meer geanalyseerde berichten had mogelijkerwijs tot meer inzichten in rekruteringsprocessen geleid. Hieraan gerelateerd is een beperking van het huidige onderzoek dat we in de contentanalyse alleen berichten op open platforms hebben meegenomen. Ethische aspecten maken het doen van onderzoek op besloten platforms onverantwoord. Afgaande op de interviews en de literatuur speelt online rekrutering zich voor een deel af in besloten groepen, maar deze kennis hebben wij niet kunnen illustreren aan de hand van de berichten op besloten platforms. Ten derde hebben we een verkennende in plaats van systematische literatuurstudie uitgevoerd, die we vervolgens hebben verwerkt in de resultaten. Het is niet uitgesloten dat er studies bestaan die niet zijn meegenomen, maar die wel belangrijke inzichten leveren in online rekrutering of de preventie daarvan. Tot slot is binnen het huidige onderzoek niet gekeken naar de ervaringen van gerekruteerde leden van extremistische organisaties zelf en van mensen die anderen hebben gerekruteerd.

6.4 Aanbevelingen voor vervolgonderzoek

Op basis van de huidige stand van de wetenschap kan een aantal aanbevelingen voor vervolgonderzoek worden gedaan. Hierbij gaan we af op de resultaten van het huidige onderzoek, aangevuld met de nodige aanbevelingen die in diverse andere wetenschappelijke publicaties worden aangereikt. We geven eerst aanbevelingen voor vervolgonderzoek naar het fenomeen zelf, dus de aard en mechanismen van online rekrutering. Daarna doen we aanbevelingen voor onderzoek naar de aanpak van online rekrutering.

Allereerst dient de in dit onderzoek gebruikte methode van contentanalyse in vervolgonderzoek te worden uitgebreid. Van belang is om daarbij beter zicht te krijgen op de verschillende rollen die online gebruikers vervullen, hun interactiepatronen en netwerkvorming. Door een langere en uitgebreidere

contentanalyse van de berichten in online extremistische groepen uit te voeren kan ook kennis worden verworven over de permanentie van de groepen en de verandering over de tijd. Uit een gedurende de pandemie uitgevoerd onderzoek naar 'anti-vaxx'-groepen op Telegram (Schlette, Van Prooijen, Blokland, & Thijs, 2022) bleek dat slechts een heel klein deel van de online gebruikers verantwoordelijk was voor het grootste deel van de posts, dat de frequentie van posten snel toenam en dat de groepen erg fluïde waren. Het zou interessant zijn om na te gaan in hoeverre dit ook geldt voor radicale en extremistische groeperingen.

Verder is uitgebreider onderzoek nodig naar de technieken en methoden die extremistische en terroristische groepen gebruiken om de attitudes en persoonlijkheden van sociale mediagebruikers te achterhalen en zo te bepalen wie potentieel vatbaar zijn voor hun online propaganda (zie de review van Akram & Nasar, 2023). Daarbij kan het nuttig zijn om kennis en inzichten te gebruiken uit de communicatiewetenschappen, zoals Lawrence en Robertson (2023) voorstellen. Zij stippen aan dat een communicatielens ons mogelijk nog meer kan leren over de manier waarop extremisten opereren bij rekrutering, wat vervolgens ook zou kunnen leiden tot effectiever beleid.

Verder bevelen we aan om nader onderzoek te doen naar de rol van gamingplatforms in online radicalisering en online rekrutering. Uit het huidige onderzoek werd duidelijk dat gamingplatforms een belangrijke rol kunnen spelen bij verschillende aan extremisme gerelateerde processen, variërend van online radicalisering tot online rekrutering, maar onduidelijk bleef hoe die platforms deze processen faciliteren. Een complicerende factor lijkt te zijn dat sommige platforms de mogelijkheid bieden om een eigen spel en bijbehorende server te creëren. Via deze server kunnen gebruikers in real-time met elkaar communiceren, zonder dat het gamingplatform daar zicht op heeft. Daarnaast is er een grote diversiteit in het soort platforms en dit heeft mogelijkerwijs tot gevolg dat radicaliserings- en rekruteringsprocessen verschillen per platform. Wetenschappelijk onderzoek naar de rol van deze platforms en de mechanismen die mogelijk bijdragen aan radicalisering en rekrutering is belangrijk, zeker gezien de grote populariteit van interactieve games onder jongeren.

Het is ook van belang om meer onderzoek te doen naar specifiek online mobilisatie. Eerder werd benoemd dat het grootste deel van de mensen die zich online aansluiten bij een extremistische organisatie niet overgaat tot offline extremistische of terroristische acties. In de Nederlandse context zagen we ook groepen die voor een belangrijk deel alleen online blijven interacteren en de offline wereld met name betraden voor sociale activiteiten, protesten en het rekruteren van nog meer nieuwe leden. Tegelijkertijd zijn er gevallen bekend waarin mensen via online rekrutering direct online werden gemobiliseerd voor offline gewelddadigheden. Vervolgonderzoek dient zich te richten op online mobilisatie voor offline gewelddadige acties, maar ook online mobilisatie voor offline acties in bredere zin, zoals openbare ordeverstoringen.

Vervolgonderzoek dient zich daarnaast te richten op de ervaringen van mensen die online zijn gerekruteerd of zelf anderen hebben gerekruteerd. Wetenschappelijke interviews zijn cruciaal om mechanismen te ontwarren die tot bepaalde uitkomsten leiden. Kennis over de ervaringen van gerekruteerden en rekruteurs kan belangrijke inzichten opleveren in onder meer de timing van rekrutering en welke (levensloop-)gebeurtenissen daaraan vooraf zijn gegaan, de volgordelijkheid en het precieze verloop van bepaalde processen, waar de aantrekkingskracht van de organisatie precies zit, de modus operandi van rekruteurs en de motivatie om te rekruteren. Hoewel het werven van leden

van extremistische organisaties doorgaans een uitdaging is, zijn er wel degelijk studies waarin dit gelukt is. Daarnaast kan worden gesproken met zogenaamde 'formers', voormalige leden van extremistische groeperingen, iets dat steeds vaker in onderzoek wordt gedaan. Degelijke gesprekken hebben al tot diverse belangrijke inzichten geleid ten aanzien van risicofactoren voor toetreding tot extremistische groepen (Logan, Windisch & Simi, 2024). Om meer zicht te krijgen op individuele rekruteringsprocessen kan daarnaast ook worden gedacht aan het gebruik van andere, aanvullende informatie. Zo zijn in Nederland alternatieve bronnen beschikbaar waarin informatie staat over door individuen doorgemaakte rekruteringsprocessen, zoals strafvonnissen.

Ten aanzien van de aanpak van online rekrutering werd geconstateerd dat er nog maar weinig zicht is op de effectiviteit van bestaande programma's en de werkzame elementen daarvan. Uitzonderingen daargelaten zijn ideeën over de effectiviteit vaak nog gebaseerd op 'anekdotisch bewijs'. Het is daarom ook belangrijk om meer onderzoek te doen naar de onderliggende evidence-base en effectiviteit van bestaande maatregelen en campagnes die al worden ingezet door overheden en andere instanties. Er zijn tot nu toe weinig evaluatiestudies verricht, terwijl bijvoorbeeld campagnes die zich richten op tegengeluiden potentieel ook een averechts effect kunnen hebben. In lijn met deze aanbevelingen stellen Windisch en collega's (2022) dat het in tot nu toe verrichte evaluaties vaak gaat over hoe accuraat computer algoritmes extremistisch materiaal kunnen classificeren en identificeren, in plaats van over de effectiviteit van online interventies om juist dat materiaal tegen te gaan. Meer nadruk zou volgens hen moeten liggen op de effectiviteit van programma's die de creatie en overdracht van dergelijk materiaal trachten te voorkomen. Daarnaast meten sommige studies offline gedrag in plaats van online gedrag na interventies. Windisch en collega's moedigen onderzoekers aan om de theoretische kaders die tot hun online interventie en/of campagne hebben geleid duidelijk te specificeren. Met betrekking tot de ontwikkeling van nieuwe interventies opperen ze dat toekomstige studies zich moeten concentreren op het verkennen van online interventies voor individuen die mogelijk al zijn blootgesteld aan, of zijn geradicaliseerd door, extremistische ideologieën en/of die zijn overgestapt naar radicalere platforms met minder regels rondom de creatie van haatzaaiende inhoud.

Hoewel er tot op heden nog beperkt zicht is op de effectiviteit van campagnes die beogen de online weerbaarheid te verhogen, bleek uit de wetenschappelijke literatuur naar effecten van verhoogde weerbaarheid op andere uitkomsten dat er reden is om aan te nemen dat het verhogen van weerbaarheid ook de kans op online rekrutering kan verkleinen. Naast effectiviteitsstudies is het echter zaak om te achterhalen *hoe* dit precies werkt en wat de werkzame elementen zijn van initiatieven die zijn gericht op weerbaarheid. Het verdient daarbij aanbeveling om in dergelijk onderzoek te vertrekken vanuit studies naar weerbaarheid in andere contexten, aangezien er al een rijke literatuur is binnen onder meer de pedagogische wetenschap.

Tot slot zou vervolgonderzoek de mogelijkheden die overheidsinstanties en tech-bedrijven hebben om online content te modereren en platforms te reguleren in kaart moeten brengen, alsmede hoe dergelijke instanties en bedrijven in de praktijk gebruik maken van deze mogelijkheden. Daarbij dient niet alleen te worden gekeken naar duidelijk illegale content maar ook naar borderline content en hierbij dienen zowel de praktische, technische en juridische mogelijkheden en onmogelijkheden te worden onderzocht. Het is in dit kader belangrijk om te onderzoeken hoe de Digital Service Act wordt geïmplementeerd en waar de uitdagingen en knelpunten liggen.

6.5 Aanbevelingen voor beleid en praktijk

Op basis van de resultaten van het onderzoek kunnen verschillende aanbevelingen voor beleid en de praktijk worden geformuleerd. Een aantal aanbevelingen is reeds in hoofdstuk 5 op basis van de interviews met de professionals opgetekend. Andere aanbevelingen volgen uit de literatuur en uit de contentanalyse.

Allereerst wordt aanbevolen om programma's ter vergroting van de online weerbaarheid verder te ontwikkelen. Hier dienen professionals vanuit verschillende instanties buiten het strafrechtelijk domein nadrukkelijker bij te worden betrokken, variërend van jongerenwerkers tot leerkrachten. Uit de diverse bronnen van het onderzoek komt naar voren dat bepaalde kwetsbaarheden de vatbaarheid voor online rekrutering kunnen vergroten. Belangrijk daarbij is dat bezoekers van online platforms vaak niet via illegale content maar via processen van groepsvorming worden aangetrokken tot (lidmaatschap van) een groep. Dergelijke processen laten zich niet modereren, maar spelen tegelijkertijd wel een belangrijke rol in de fase die hierop kan volgen, waarbinnen iemand dieper in de organisatie komt. Een preventieve aanpak gericht op weerbaarheid is in deze eerste fase derhalve cruciaal om verdere rekrutering te voorkomen. In hoofdstuk 5 werden diverse initiatieven genoemd om de online weerbaarheid te vergroten, waarbij de nadruk ligt op het omgaan met de online wereld.

Gelet op de genoemde kwetsbaarheden verdient het verder aanbeveling om dergelijke aanpakken te combineren met reeds bestaande programma's ter vergroting van de weerbaarheid in de offline wereld. In de afgelopen jaren is flink ingezet op de ontwikkeling en implementatie van dergelijke programma's. Soms zijn die programma's in algemene zin gericht op het verhogen van weerbaarheid, in andere gevallen zetten programma's in op het voorkomen van bepaalde uitkomsten. Een voorbeeld uit deze laatste categorie is Diamant, een erkende interventie "die de weerbaarheid tegen radicalisering beoogt te versterken bij islamitische migrantenjongeren en -jongvolwassenen tussen 12 en 23 jaar bij wie verschillende risicofactoren aanwezig zijn" (Salama, Aarts & Lucassen, 2020). Daarnaast is in november 2022 het programma 'Preventie met gezag' van start gegaan, gericht op het wegnemen van de voedingsbodem voor georganiseerde en ondermijnende criminaliteit. Onderdeel van dit programma is het weerbaar maken van jongeren tegen criminaliteit of het daarin verder afglijden. Beide programma's zijn breed uitgerold en binnen de programma's wordt samengewerkt door verschillende ketenpartners vanuit verschillende gemeenten. Hieraan gerelateerd wordt in de aanpak op verschillende domeinen ingezet. Zo geeft Halt, één van de partners binnen Preventie met Gezag, aan dat ze inzet op groepsgerichte interventies, individuele interventies, huisbezoeken, advies, participatie en kennisdeling. Juist deze diversiteit aan activiteiten maken dat een probleem vanuit verschillende kanten kan worden belicht en aangepakt, iets dat op basis van de resultaten uit het huidige onderzoek ook belangrijk lijkt ter voorkoming van online rekrutering en het doorgroeien in extremistische organisaties.

Het verdient voorts aanbeveling om de samenwerking tussen instanties te intensiveren, waarbij verschillende expertises worden gebundeld. Uit de interviews bleek namelijk dat professionals behoefte hebben aan meer kennis ten aanzien van online rekrutering en signalen daarvan, maar tegelijkertijd niet altijd goed weten welke bevoegdheden ze hebben om deze kennis daadwerkelijk in te zetten. Het opstellen en communiceren van duidelijke richtlijnen per instantie, bijvoorbeeld in hoeverre zij inzicht mogen hebben in online activiteiten of accounts van mogelijk geradicaliseerde

individuen, zou daarom van meerwaarde zijn. Aan een stap in deze richting wordt reeds gewerkt. Vanuit het Meerjarenplan Richtlijnen Jeugd wordt momenteel een 'Richtlijn Radicalisering' ontwikkeld. De richtlijn, die naar verwachting in het najaar van 2024 gepubliceerd wordt, beoogt jeugdprofessionals handvatten te bieden voor het signaleren en aanpakken van radicalisering bij jeugdigen.

Waar binnen de persoonsgerichte aanpak (PGA) al veel gebruik wordt gemaakt van gecombineerde expertises en informatie over bepaalde casussen in gezamenlijkheid wordt besproken, wordt in het geval van online rekrutering en meer in het algemeen online radicalisering nog wat minder samengewerkt tussen instanties. Hierbij gaat het niet alleen om samenwerking in individuele gevallen, maar zeker ook om de uitwisseling van kennis over online processen. Dergelijke kennis kan dan worden meegenomen wanneer een individuele casus wordt gewogen in de offline wereld. Deze uitwisseling lijkt eens te meer belangrijk voor de zogenaamde 'onlife' rekrutering; vastgesteld werd dat online processen van rekrutering (en overigens ook radicalisering) doorgaans niet los kunnen worden gezien van offline processen die daaraan voorafgaan noch van offline processen die daarop volgen. De persoonsgerichte aanpak heeft daarom baat bij gebundelde expertise ten aanzien van zowel offline als online processen.

Een gerelateerde aanbeveling die uit de interviews naar voren kwam, was het regelmatig betrekken en bevragen van jongeren bij de (door)ontwikkeling van preventieprogramma's om zo een beter beeld te krijgen van waar jongeren online mee in aanraking komen. Ook deze aanbevelingen sluiten aan bij de ervaringen die inmiddels zijn opgedaan rond het eerdergenoemde programma 'Preventie met Gezag'. Ook hier staat samenwerking tussen lokale en regionale instanties centraal. Juist deze samenwerking lijkt cruciaal voor de uitwerking van het programma, aangezien de verschillende instanties verschillende expertises en informatieposities hebben. Een concrete aanbeveling die voortvloeit uit de interviews is om binnen de lokale overheid meer mensen aan te stellen die technische expertise hebben ten aanzien van het online domein, die vervolgens ook worden meegenomen in de PGA.

Naast aanbevelingen die zijn gericht op de aanpak ter voorkoming dat individuen online worden gerekruteerd, volgen uit de resultaten ook aanbevelingen over het online domein zelf. Met betrekking tot illegale extremistische content wordt aanbevolen om in samenwerking met tech-bedrijven verbeteringen te blijven doorvoeren voor het detecteren van online extremistisch materiaal. Dit kan worden gedaan door regelmatig trefwoorden, zoeklijsten en datasets bij te werken. Van belang daarbij is dat niet alleen naar individuele trefwoorden wordt gekeken maar ook naar combinaties van trefwoorden. Bovendien dient rekening te worden gehouden met de context waarin bepaalde trefwoorden worden gebruikt. Te denken valt aan de namen van plaatsen waarin aanslagen zijn gepleegd (Utoya, Wenen, Christchurch). Deze namen kunnen niet automatisch worden verwijderd. Wel zouden platforms naar een werkwijze kunnen streven waarin dergelijke woorden worden geïdentificeerd, waarna een menselijke beoordeling plaatsvindt om na te gaan in welk verband het woord wordt gebruikt. In de literatuur wordt daarnaast de mogelijkheid benoemd om een database te ontwikkelen waarin 'rekruteringstaal' wordt bijgehouden, waarmee websitebeheerders en wetshandhavers kunnen worden geholpen om gevallen van rekrutering te signaleren. Een dergelijke database kan alleen van toegevoegde waarde zijn indien de database constant wordt geactualiseerd. Om dit laatste mogelijk te maken, is het belangrijk dat opsporingsinstanties voortdurend samenwerken

met professionals met inhoudelijke en actuele expertise op het gebied van online communicatie door extremistische groepen.

Een moeilijker vraagstuk betreft de aanpak van de zogenaamde borderline content, ook wel aangeduid als 'legal yet harmful' of 'lawful but awful'. Dergelijke content speelt, zo blijkt ook uit het huidige onderzoek, een belangrijke rol in processen van groepsvorming, de verspreiding van extremistische narratieven en uiteindelijk ook de rekrutering van nieuwe leden voor groeperingen vanuit verschillende ideologische stromingen. Ook een recente fenomeenanalyse naar het gebruik van memes door extreemrechts (NCTV, 2024) onderstreept het belang van een concretere aanpak van dergelijke content. In de analyse wordt gesteld dat memes een dermate belangrijk communicatiemiddel vormen dat ze kunnen worden beschouwd als 'online wapen', een zeer moeilijk te detecteren wapen bovendien. Gesteld wordt dat "hoe meer contentmoderatie op een platform plaatsvindt, hoe subtieler de extreemrechtse boodschap in de meme verpakt moet zijn. Alleen zo kan een meme met extreemrechtse boodschap de grotere platforms bereiken, de moderatie omzeilen en uiteindelijk een groter publiek aanspreken" (p. 33). Hierboven werd benoemd dat het belangrijk is om internetgebruikers weerbaar te maken tegen de mogelijke invloeden van dergelijke content. Het is echter ook belangrijk om een deel van de verantwoordelijkheid bij de platforms zelf neer te leggen. Uit de DSA volgt dat online platforms verplicht zijn om verslagen te publiceren over hun activiteiten die zijn gericht op het verwijderen en ontoegankelijk maken van informatie die als illegale inhoud of in strijd met de algemene voorwaarden kan worden beschouwd (artikel 23 DSA). Juist in de formulering van deze algemene voorwaarden ligt een kans voor de online platforms om ook in te gaan op de borderline content. Dit zou het dan in beginsel mogelijk maken om nadrukkelijker in te zetten op de moderatie van content die niet strafbaar is, maar wel volgens vooraf gespecificeerde richtlijnen als onwenselijk wordt beschouwd. Zoals eerder aangestipt door Van Wonderen en collega's (2023) ligt hier een belangrijke taak voor zogenoemde Trusted Flaggers, die momenteel al een rol spelen in het identificeren en melden van illegale online content op de platforms. Uit de DSA volgt dat meldingen van deze Trusted Flaggers met voorrang moeten worden behandeld door de platforms (artikel 19). Dit vraagt evenwel om een professionaliseringsslag onder professionals die nu al expertise hebben rond illegale extremistische content, waarbij zij ook worden getraind in het identificeren en melden van borderline content. Daarnaast zijn er verschillende initiatieven om met behulp van machine learning en natuurlijke taalverwerking te komen tot een systeem waarbinnen onder meer online hate speech kan worden gedetecteerd. Het resultaat van dergelijke ontwikkelingen kunnen op termijn mogelijk ook bijdragen aan het modereren van ongewenste borderline content.

Een belangrijke kanttekening die hierbij dient te worden gemaakt is dat een intensievere moderatie van borderline content als risico met zich meebrengt dat de grenzen van belangrijke rechten, zoals het recht op vrijheid van meningsuiting, worden opgezocht. Dit spanningsveld laat zich niet gemakkelijk oplossen en daarom sluiten wij af met een laatste, belangrijke aanbeveling om een 'taskforce borderline content' op te richten. Binnen deze taskforce zouden professionals vanuit de praktijk en beleid en de tech-sector plaats moeten nemen, alsmede een breed pallet aan wetenschappers inclusief extremisme-experts, juristen en ethici. Gezamenlijk zouden de professionals zich moeten buigen over de vraag hoe de ongewenste gevolgen van borderline content kunnen worden tegengegaan met inachtneming van belangrijke rechten en vrijheden.

6.6 Tot slot

In de inleiding van dit rapport verwerkten we een passage uit een openbaar vonnis in een zaak tegen een verdachte die lid was van Assault Division en The Base, twee rechts-extremistische groeperingen. In de betreffende passage wordt beschreven hoe de betreffende groeperingen het online domein aanwenden om onder meer aan te zetten tot rassenhaat en antisemitisme, geweldplegers te verheerlijken en mensen samen te brengen. Deze casus is slechts één voorbeeld waaruit blijkt dat internet in het algemeen en sociale media in het bijzonder een belangrijke rol kunnen spelen in het rekruteren door en voor extremistische organisaties. Het huidige onderzoek heeft laten zien dat dit voorbeeld niet op zichzelf staat en dat groeperingen vanuit verschillende ideologische stromingen de gebruiksmogelijkheden van sociale media gebruiken om nieuwe leden te rekruteren. Anders dan soms wordt gedacht speelt specifieke rekrutering daarbij, in elk geval in het huidige extremistische landschap in Nederland, een beperkte rol, zo blijkt uit de resultaten. Veel gangbaarder is een proces van generieke rekrutering waarbij individuen zelf online op zoek gaan naar bijvoorbeeld kennis of contact met gelijkgestemden en vervolgens via een proces van groepsvorming en het delen van ideologische narratieven worden aangetrokken tot een groep en daar lid van worden. De in dit onderzoek geïdentificeerde aanpakken om online rekrutering tegen te gaan zijn divers, variërend van aanpakken gericht op het vergroten van weerbaarheid, het bieden van online tegengeluiden en het modereren van online content. Voor veel aanpakken geldt echter dat er nog weinig zicht is op de effectiviteit in het algemeen en de werkzame elementen in het bijzonder. Het is belangrijk om in de komende jaren structureel in te zetten op het toetsen van de interventies op effectiviteit. Dat gezegd hebbende kan op basis van de resultaten worden gesteld dat vooral de preventieve aanpak veelbelovend is om de vatbaarheid voor online rekrutering weg te nemen. Daarnaast is het belangrijk om tenminste een deel van de verantwoordelijkheid voor het tegengaan van online rekrutering ook bij de platforms zelf te leggen. Hoewel het niemand kan worden verboden om aansluiting te zoeken bij een online groep en vrijheid van meningsuiting een groot goed is in een democratische rechtstaat, is ongebreidelde groei van organisaties met een extremistisch gedachtegoed en verspreiding van extremistische, vaak kwetsende en soms ondermijnende content, onwenselijk en een gevaar voor diezelfde rechtstaat. De in dit rapport beschreven inzichten en aanbevelingen dragen hopelijk bij aan een evidence-based aanpak die met inachtneming van belangrijke rechten en vrijheden kan bijdragen aan het voorkomen van online rekrutering door en voor extremistische groeperingen.

Summary

Background and research questions

In recent years, it has become increasingly clear that the internet and social media play a crucial role in processes of radicalization and recruitment by and for extremist groups. In the National Counterterrorism Strategy 2022-2026, the most recent Terrorist Threat Assessment for the Netherlands (DTN) and the recent annual report of the General Intelligence and Security Service (AIVD), various references are made to the role of internet and social media. For instance, the threat assessment report mentions that the online world plays an important role in radicalization processes, the formation of networks and attracting often young people with 'an existing lust for violence and urge to shock'. In discussing a number of foiled attack plots, the AIVD notes that some of these were planned by groups that fully originated online. These and other developments highlight the importance of scientific knowledge on which prevention and intervention programs can be developed. Although scientific research has already provided much insights into the mechanisms of online radicalization, knowledge on processes of online *recruitment* remains limited.

The current study attempts to fill this gap by examining how online recruitment for and by right-wing extremist, jihadist, anti-institutional and left-wing extremist groups takes place. Online recruitment is defined as "the process by which an individual is encouraged online to join a group, organization, or movement". We depart from theories that presume that recruitment consists of different phases. Additionally, we use theories that specifically address how social media characteristics align with the users' world to facilitate both desired and undesired developments. To enhance knowledge about online recruitment, we answer the following overarching research questions:

1. What is known from both the scientific literature as well as from practice about the nature and mechanisms of online recruitment?
2. To what extent do online recruitment and offline behavior interact?
3. What perspectives and approaches are available/suitable for agencies tasked with preventing and responding to online recruitment?

Method

To answer the research questions, various research methods were combined. First, scientific literature and policy documents on online recruitment by and for extremist groups was collected. For this purpose, several databases were consulted. Based on the literature, a topic list was then drawn up for interviews with professionals who have insights into online recruitment. A total of fourteen professionals were interviewed, namely three employees from the National Police, two from the General Intelligence and Security Service, three from the National Support Center for Extremism, two from the Social Stability Expertise Unit, three from municipalities and two youth workers. Transcripts of the interviews were systematically coded and analyzed using the ATLAS.ti program.

Subsequently, a qualitative content analysis was conducted on Telegram and Facebook. To get a broad overview of recruitment processes we examined seven online public groups with different ideologies, namely far-right, far-left, anti-institutional and jihadism. The choice for the specific groups was based

on recent Terrorist Threat Assessments (DTNs), the recent annual report of the AIVD and media reporting on specific groups. During the research period, messages posted in the groups were collected. Next, the messages were coded and analyzed using the ATLAS.ti program. Visual material and video clips were also analyzed. Finally, an expert meeting with professionals and scientists was organized to discuss the preliminary research results and reflect on the recommendations.

Results

The online domain as a unique environment

The results first show that the online domain has several characteristics that can contribute to the process of online recruitment. Professionals indicated that the online domain is 'easy in - easy out'; the threshold for joining and leaving extremist groups online is much lower than offline. According to the interviewees, this is mainly due to the anonymity of the internet and the fact that individuals initially need to invest less (time) in the group. As such, someone can join an extremist group without their offline social network knowing. Moreover, the threshold to exhibit behavior in the online world that is less accepted in the offline world is often lower. During the interviews, it was also repeatedly emphasized that the online domain crosses borders. Hence, physical proximity is no longer a requirement to recruit or be recruited. Finally, it was mentioned that the online domain can give a distorted, more positive picture of a group's cohesion, size, and reach, increasing the attractiveness of joining the group.

As for the types of platforms, the analyses showed that extremist groups use a wide variety of platforms, including mainstream social media platforms such as Facebook and YouTube and 'low profile' platforms such as Telegram. Gaming platforms such as Roblox are also used, although the view on recruitment at gaming platforms is still very limited. According to professionals, Telegram is currently the most used platform among extremist groups. One of the reasons could be that this platform offers more anonymity and is less active in terms of content moderation. Mainstream platforms are still important however; they are frequently used to spread ideological narratives and often serve as a gateway to low profile platforms.

Online recruitment: Generic and specific

When mapping the actual processes of online recruitment, it quickly became necessary to distinguish between two variants of online recruitment: 'generic recruitment' and 'specific recruitment.' Generic recruitment is a recruitment process aimed at a broad audience. Within this process, individuals are recruited through a process of community building and the spreading of ideological narratives. Specific recruitment, on the other hand, targets specific subpopulations of individuals. Although these two variants sometimes overlap, they also occur separately.

Regarding generic recruitment, extremist groups engage in online community building by creating and promoting social cohesion, shared narratives and common goals through extremist memes (humorous images, videos, or text fragments shared online) and ideological messages. Notably, the group formation process is not limited to the online domain. All the online groups we examined reported on offline group activities, ranging from giving and attending lectures to exercising together and organizing and attending protests. During the research period, various messages were posted to concretely invite users to become members of the group.

Specific recruitment, on the other hand, targets certain subpopulations, such as women, minors, or technically skilled individuals. Scientific literature shows that specific recruitment, often referred to as 'narrowcasting', has been widely used by large terrorist organizations such as Al Qaeda and Islamic State (IS). Examples include the large-scale mobilization of foreign fighters by IS and the recruitment of technical students and employees by Al Qaeda. According to the findings of the present study, such specific recruitment strategies currently seem rare in the Dutch context. According to the interviewed professionals, most people come into contact with an extremist group by independently searching online for like-minded people and joining a public online group. In a step-by-step process, interested individuals can delve deeper into the group by being invited to closed groups and going through screening procedures, including answering knowledge questions about the group or ideology and being asked about the willingness to meet offline or contribute to the group's goals.

An important observation is that there seem to be more similarities than differences in the use of social media by the studied groups. For example, all groups employ community building activities and actively use the various other functionalities of the online domain, including sharing extremist content, memes, and spreading the ideology. Additionally, all groups organize offline activities, although the nature of these activities varies between groups. Lectures and presentations appear to be the most common activities among anti-institutional, jihadist, and far-left groups. In addition, the far-right and jihadist groups also report, unlike the other two movements, about engaging in joint training and martial arts. Calls for membership are particularly common in far-right and anti-institutional groups. Screening procedures are primarily used by far-right, jihadist and anti-institutional groups.

The interaction between online and offline worlds

The interaction between the online and offline world is of interest to scientists, policymakers and practitioners. The research shows that there are at least three ways to view the relationship between online recruitment and the offline world. First, someone's offline circumstances, such as a difficult home situation, can increase a susceptibility to online recruitment, which appears to be especially prominent among young people. Although such vulnerabilities do not directly lead to membership, they can be considered a risk factor.

Second, online recruitment can transition into 'onlife' recruitment, where there is a continuous interaction between online and offline processes. For example, offline meetings are announced online, which are then reported on online, often accompanied by calls to join the group. Despite increased attention for the online domain, respondents note that the offline domain has recently regained a more prominent role, especially in later recruitment phases. This is due to increased security awareness among extremist groups and the related realization that law enforcement can read along, leading to more critical admission policies and a renewed appreciation for physical contact.

The third relationship between online recruitment and the offline world involves transitioning to actual (violent) extremist offline actions. Both the literature and the interviews show that this relationship is a difficult one to study, let alone establish. Exceptions are the recruitment strategies of Al Qaeda and IS, where online recruitment for specific tasks clearly led to offline terrorist actions. Often, however, the relationship is much more complex.

Existing approaches and action perspectives

With increased attention for online recruitment processes, measures to prevent it have also quickly developed in recent years. Based on the scientific literature, the present study mainly zoomed in on measures focused on resilience, online counter-narratives and regulation and content moderation.

Preventive resilience programs in the Netherlands and abroad mainly target young people, aiming to inform them about violent extremism, raise awareness of 'grooming' behavior and increase their media literacy. A key overarching goal is to develop skills to critically assess news reports, evaluate different sources and distinguish between reliable information and misinformation. Although many programs aimed at increasing online resilience have not yet been evaluated, various respondents endorse the importance of resilience-oriented approaches and call for further development and practical tools. The role of parents was repeatedly emphasized, as they play a crucial role in digital upbringing and promoting online resilience. Respondents however mentioned that the current generation of parents also needs support in this regard, given the rapid developments in the online domain.

The deployment of the second approach, online counter-narratives, is carried out by governments and civil society. Most of these initiatives do not specifically aim to prevent online recruitment but address various related processes, including online radicalization and the spread of fake news. The scan of the literature and interviews show that the effect of online counter-narratives is unclear. Little is also known about unintended side effects or downright counterproductive effects, such as the reinforcement of extremist viewpoints.

The third approach, moderating and regulating online material, happens at different levels by international bodies (EU, Europol), national governments, private parties (social media companies, internet providers) and civil society organizations and individuals who are capable of detecting illegal online content and report it (so-called ‘trusted flaggers’). The recently introduced Digital Services Act (DSA) forces private parties within the EU to act against illegal content, although large social media companies like Meta have already been moderating and regulating online material for several years. As a result, the practice of sharing explicit visual and instructional material has increasingly moved to closed groups on low-profile platforms like Telegram, according to the literature and interview results. New technological developments, such as image recognition techniques and artificial intelligence, can help to (better) detect and moderate extremist expressions in the online domain.

Lastly, several other obstacles and challenges that hinder the (optimal) implementation of the various approaches came to the fore during the interviews. First, it was noted that online platforms are owned by private companies that fall under different jurisdictions than where their users are located. Second, the enormous amount of extremist and terrorist material and the impossibility of moderating or removing all this material was highlighted. Even more problematic is the handling of so-called borderline content, also known as 'legal yet harmful' content. This content cannot easily be moderated but plays a crucial role in radicalizing and recruiting new members. Third, and related to this, there is a lack of capacity within both law enforcement and other organizations involved in preventing radicalization, extremism and terrorism. Fourth, there is a need for more substantive expertise and clear guidelines on the powers of various professionals and organizations, including sharing information. Fifth, there is a general lack of insight into the overall effectiveness of existing approaches and any effective elements within them.

Conclusion and recommendations

Based on the results and the identified challenges, several recommendations for further research, policy and practice have been made. Before mentioning these recommendations, it is important to outline the limitations of the current study. Firstly, only a limited number of employees were interviewed per agency. Secondly, the content analysis was limited in scope, both in terms of the time period and the number of messages that was analysed. Thirdly, we did not interview recruited (former) members of extremist groups, nor did we interview recruiters. Nonetheless, the research results provide several overarching insights that lead to the following recommendations. We first present recommendations for further research, followed by recommendations for policy and practice.

Regarding further research, it is recommended to expand the content analysis method used in this study. Research with a longer analysis period and the inclusion of more messages will lead to additional insights, including insights into the different roles that online users play, interaction patterns and network formation. Given the popularity of interactive games and the still limited understanding of recruitment processes the take place on or via such platforms, it is important that follow-up studies also include gaming platforms. Additionally, future research should include the experiences of people who have undergone a recruitment process or who have functioned as recruiter themselves. Based on this, more insights can be gained into the sequence of recruitment processes, the attractiveness of online groups, the modus operandi of recruiters and motivations to recruit others. Such research can also be used to gain a better understanding of the relationship between online recruitment and offline extremist actions.

Concerning the approach to online recruitment, it was found that there is little knowledge on the effectiveness of existing programs. Evaluation research is needed to map out the evidence-base and effectiveness of the programs. As for the evaluation of approaches aimed at enhancing (online) resilience, it is recommended to start from the now rich scientific literature on resilience in other contexts and scientific disciplines. Finally, follow-up research should map out the possibilities that governmental agencies and tech companies have to moderate online content (illegal and borderline content) and regulate platforms, as well as how these agencies and companies actually make use of these possibilities, how they implement the Digital Services Act (DSA) and what the effects are.

Regarding policy and practice, we come to the following recommendations. Firstly, it is recommended to further develop evidence-based programs to increase online resilience. Professionals from various agencies outside the criminal justice domain, ranging from youth workers to teachers, should be (more) explicitly involved in this. Regularly involving young people in the development of programs is considered important to get a better understanding of what young people encounter online. It is important to note that these programs should not only target young people but also their parents and caregivers, as they play a crucial role in 'digital upbringing'. As mentioned, the current generation of parents does not always have the right knowledge and skills to adequately do so. In recent years, various initiatives have been developed to support parents and provide tips. Such initiatives should be communicated and disseminated even more actively. It is important to roll out these kinds of initiatives widely, as to lower the burden for specific institutions who are often tasked with disseminating a lot of programs (e.g. schools) and to make sure the initiatives have a broader reach.

Given the previously mentioned vulnerabilities, it is also recommended to combine the focus on online resilience with existing programs to increase resilience in the offline world. The current research has found that (online) recruitment processes by and for extremist groups have several similarities with

recruitment processes for organized crime and cybercriminal organizations. It seems sensible to investigate which resilience-focused elements from programs to prevent youth involvement in these types of organisations are applicable to preventing online recruitment for extremist organisations.

Secondly, it is important to further professionalise the approach to preventing online recruitment. The present study has shown that professionals are in need of more clarity on where professionals in various roles, ranging from football coaches to teachers, can turn to in case of concerns about problematic online behavior. In training sessions, which professionals believe should have a more structural character, attention could be paid to signs of recruitment and knowledge about one's own capacities. Working with the 'Guideline Radicalization' could be part of this training. This guideline is currently being developed as part of the 'Multi-year plan Guidelines Youth' and aims to provide professionals with tools for identifying and responding to radicalization among young people.

Related to this, it is recommended to intensify cooperation between agencies, particularly combining expertise on offline radicalization and recruitment with expertise on online processes. Knowledge about online processes is crucial when assessing individual cases in the offline world. There is a call for the addition of professionals with this knowledge to the person-centered approach (PGA) in various municipalities. More generally, it is recommended to significantly increase knowledge about the online domain and technological developments within local governments.

In addition to recommendations aimed at preventing individuals from being recruited online, the results also yield recommendations regarding the online domain itself. Concerning illegal extremist content, it is recommended to continue making improvements in collaboration with tech companies regarding the detection of online extremist material. A concrete recommendation from the literature is to build a database tracking 'recruitment language'. To make this possible, it is important that law enforcement agencies continuously work with professionals with substantive and especially timely expertise in online communication by extremist groups. Given the rapidly changing field, this collaboration between policy, practice and science is also important more broadly, especially considering the recommendations for further research mentioned above. Specifically, research on how the DSA is implemented and what challenges arise has a highly applied character with direct relevance for practice.

Lastly, current research and recent other studies underscore the importance of a more concrete approach to borderline content. Given the tension between moderating borderline content on the one hand and safeguarding fundamental rights and freedoms on the other, it is recommended to establish a 'taskforce borderline content'. This taskforce should include policymakers, practitioners and tech-professionals, as well as a broad range of scientists, including extremism experts, lawyers, and ethicists. Together, these professionals should address the question of how the undesired consequences of borderline content can be combatted while respecting important rights and freedoms. An answer to that question is urgently needed, especially now that current research has shown that the recruitment process typically begins on public platforms where it is not so much illegal content but rather borderline content that contributes to the attractiveness of and subsequent joining of extremist groups.

Dankwoord

Onze grote dank gaat uit naar de leden van de begeleidingscommissie. Wij waarderen de tijd die de leden hebben genomen om vanuit hun expertise met ons mee te denken gedurende het onderzoek. De feedback die wij gedurende de constructieve bijeenkomsten hebben ontvangen was bijzonder waardevol.

Daarnaast zijn we veel dank verschuldigd aan de respondenten van deze studie en de deelnemers aan de expertmeeting, die allen tijd hebben vrijgemaakt om hun kennis en ervaringen met ons te delen. De inzichten die we tijdens de verschillende gesprekken hebben opgedaan, zijn van grote waarde geweest bij de totstandkoming van dit onderzoeksrapport.

Referenties

Aasback, A. W. (2022). Platform social work - a case study of a digital activity plan in the Norwegian Welfare and Labor Administration. *Nordic Social Work Research, 12*(3), 350–363. https://doi.org/10.1080/2156857X.2022.2045212

Adamse, I., Nguyen, Q., Boertien, E., van Deuren, S., Eichelsheim, V., & Blokland, A. (2023). *EPIC: Explaining, preventing, and intervening in organized crime involvement: Resultaten systematische literatuurreviews.* Amsterdam: NSCR.

Adena, M., Enikolopov, R., Petrova, M., Santarosa, V., & Zhuravskaya, E. (2015). Radio and the rise of the Nazis in prewar Germany. *The Quarterly Journal of Economics*, *130*(4), 1885-1939. https://www.jstor.org/stable/26372641

AFP. (2023). Holiday season warning: Extremists infiltrating online and gaming platforms to recruit young Australians. https://www.afp.gov.au/news-centre/media-release/holiday-season-warning-extremists-infiltrating-online-and-gaming

AIVD (2023). *Anti-institutioneel extremisme in Nederland: een ernstige dreiging voor de democratische rechtsorde?* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

AIVD (2024). *AIVD-jaarverslag 2023.* Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023). Online Veiligheid en Criminaliteit 2022. Den Haag: Centraal Bureau voor de Statistiek.

Akram, M., & Nasar, A. (2023). Systematic review of radicalization through social media. *Ege Academic Review, 23*(2), 279-296. https://doi.org/10.21121/eab.1166627

Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2017). Introduction to the special issue: Terrorist online propaganda and radicalization. *Studies in Conflict & Terrorism*, *40*(1), 1-9. https://doi.org/10.1080/1057610X.2016.1157402

Apau, R. (2018). Youth and violent extremism online: Countering terrorists exploitation and use of the Internet. *African Journal on Terrorism, 7*(1), 16-23.

Araque, O., & Iglesias, C. A. (2020). An approach for radicalization detection based on emotion signals and semantic similarity. *IEEE access*, *8*, 17877-17891. https://doi: 10.1109/ACCESS.2020.2967219

Archetti, C. (2015). Terrorism, communication and new media: Explaining radicalization in the digital age. *Perspectives on Terrorism*, *9*(1), 49–59. http://www.jstor.org/stable/26297326

Arun, A., Chhatani, S., An, J., & Kumaraguru, P. (2024). X-posing free speech: Examining the impact of moderation relaxation on online social networks. *arXiv preprint arXiv:2404.11465*

Baccarella, C. V., Wagner, T. F., Kietzmann, J. H., & McCarthy, I. P. (2018). Social media? It's serious! Understanding the dark side of social media. *European Management Journal*, *36*(4), 431–438. https://doi.org/10.1016/j.emj.2018.07.002

Bastug, M. F., Douai, A., & Akca, D. (2020). Exploring the "demand side" of online radicalization: Evidence from the Canadian context. *Studies in Conflict and Terrorism*, *43*(7), 616–637. https://search.informit.org/doi/10.3316/agispt.20200528030969

Bekkers, L. J. M., & Leukfeldt, E. R. (2023). Recruiting money mules on Instagram: a qualitative examination of the online involvement mechanisms of cybercrime. *Deviant Behavior, 44*(4), 603-619, DOI: 10.1080/01639625.2022.2073298

Bekkers, L. M. J., Moneva, A., & Leukfeldt, E. R. (2022). Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology*, online first. https://doi.org/10.1007/s11292-022-09537-7

Bélanger, J. J., Nisa, C. F., Schumpe, B. M., Gurmu, T., Williams, M. J., & Putra, I. E. (2020). Do counter-narratives reduce support for ISIS? Yes, but not for their target audience. *Frontiers in Psychology*, 11, 1059. https://doi:10.3389/fpsyg.2020.01059

Bermingham, A., Conway, M., McInerney, L., O'Hare, N., & Smeaton, A. F. (2009). Combining social network analysis and sentiment analysis to explore the potential for online radicalisation. *2009 International Conference on Advances in Social Networks Analysis and Mining*, Athens, Greece, 231-236. https://doi: 10.1109/ASONAM.2009.31

Bigio, J. & Vogelstein, R. (2019). *Women and terrorism: Hidden threats, forgotten partners*. New York: Council on Foreign Relations. https://www.cfr.org/report/women-and-terrorism

Bloom, M. (2017). Constructing expertise: Terrorist recruitment and "talent spotting" in the PIRA, Al Qaeda, and ISIS. *Studies in Conflict & Terrorism*, *40*(7), 603-623. https://doi.org/10.1080/1057610X.2016.1237219

Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence*, *31*(6), 1242-1254. https://doi.org/10.1080/09546553.2017.1339695

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (ed.), *Networked self: Identity, community, and culture on social network sites*, 39-58. Oxfordshire: Routledge. https://doi.org/10.4324/9780203876527

Braun, V. & Clarke, V. (2006). Using thematic analysis psychology. *Qualitative Research in Psychology 3*(2), 77–101. doi: 10.1191/1478088706qp063oa

Brewer, M. B. (1999). The psychology of prejudice: Ingroup love and outgroup hate? *Journal of Social Issues, 55*(3), 429-444.

Briggs, R., & Feve, S. (2013). *Review of programs to counter narratives of violent extremism. What works and what are the implications for government?* London: Institute for Strategic Dialogue.

Brouillette-Alarie, S., Hassan, G., Varela, W.,...& Pickup, D. (2022). Systematic review on the outcomes of primary and secondary prevention programs in the field of violent radicalization. *Journal for Deradicalization, 30*, 117-168.

Brzuszkiewicz, S. (2020). *Incel radical milieu and external locus of control.* International Centre for Counter-Terrorism (ICCT). http://www.jstor.org/stable/resrep29445

Burnap, P., & Williams, M. L. (2016). Us and them: Identifying cyber hate on Twitter across multiple protected characteristics. *EPJ Data Science*, 5(11). https://doi.org/10.1140/epjds/s13688-016-0072-6

Carruthers, S. L. (2000). *The media at war. Communication and conflict in the twentieth century.* Hampshire, UK: Palgrave.

Carthy, S. L., Doody, C. B., Cox, K., O'Hora, D., & Sarma, K. M. (2020). Counter-narratives for the prevention of violent radicalisation: A systematic review of targeted interventions. *Campbell Systematic Reviews, 16*(3), 1-37. doi:https://doi.org/10.1002/cl2.1106

Chaliand, G. (1985). *Terrorism: From popular struggle to media spectacle*. London: Saqi Books

Chatfield, T., Reddick, C. G., & Brajawidagda, U. (2015). Tweeting propaganda, radicalization and recruitment: Islamic state supporters multi-sided Twitter networks, *Proc. 16th Annu. Int. Conf. Digit. Government Res.*, 239–249. https://doi.org/10.1145/2757401.2757408

Chermak, S., & Gruenewald, J. (2015) Laying a foundation for the criminological examination of right-wing, left-wing, and Al Qaeda-inspired extremism in the United States, *Terrorism and Political Violence, 27*(1), 133-159. https://doi.org/10.1080/09546553.2014.975646

Collin, B. (1997). Future of cyberterrorism: Physical and virtual worlds converge. *Crime and Justice International*, 13(2), 15–18.

Conway, M. (2006) Terrorism and the Internet: New media, new threat? *Parliamentary Affairs*, *59* (2), 283–298. https://doi.org/10.1093/pa/gsl009

Conway, M., Scrivens, R., & Macnair, L. (2019). *Right-wing extremists' persistent online presence: History and contemporary trends.* International Centre for Counter-terrorism – The Hague. DOI: 10.19165/2019.3.12

De Boer, H., Ferwerda, H., & Kuppens, J. (2022). *Do or don't. Kennissynthese ingroeimechanismen en rekruteringsprocessen van jongeren in de georganiseerde criminaliteit.* Den Haag: WODC.

Decker, S. H., Melde, C., & Pyrooz, D. C. (2013). What do we know about gangs and gang members and where do we go from here? *Justice Quarterly, 30*(3), 369-402. https://doi.org/10.1080/07418825.2012.732101

DeCook, J. R. (2018). Memes and symbolic violence: #Proudboys and the use of memes for propaganda and the construction of collective identity. *Learning, Media and Technology*, *43*(4), 485-504. https://doi.org/10.1080/17439884.2018.1544149

Densley, J. A. (2012). Street gang recruitment: Signaling, screening, and selection. *Social problems, 59*(3), 301-321. https://doi.org/10.1525/sp.2012.59.3.301

Densley, J. A. (2015). Joining the gang: A process of supply and demand. In S.H. Decker and D.C. Pyrooz (eds.), *The handbook of gangs*, 235-256. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118726822.ch13

Devost, M., Houghton, B., & Pollard, N. (1997). Information terrorism: Political violence in the information age. *Terrorism and Political Violence, 9*(1), 72–83. https://doi.org/10.1080/09546559708427387

Djuric, N., Zhou, J., Morris, R., Grbovic, M., Radosavljevic, V., & Bhamidipati, N. (2015). Hate speech detection with comment embeddings. *Proceedings of the 24th International Conference on World Wide Web*. New York, NY: ACM, 29–30. https://doi.org/10.1145/2740908.2742760

Doosje, B., Moghaddam, F. M., Kruglanski, A. W., De Wolf, A., Mann, L., & Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. *Current Opinion in Psychology, 11*, 79-84. doi:https://doi.org/10.1016/j.copsyc.2016.06.008

DSA verordening (Nederlandse samenvatting): https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=LEGISSUM:4625430

Elaluf-Calderwood, S., Kietzmann, J., & Saccol, A. Z. (2005). Methodological approach for mobile studies: empirical research considerations. In *4th European Conference on Research Methodology for Business and Management Studies, Academic Conferences Limited,* 133-140.

EU (2020). *Online gaming in the context of the fight against terrorism.* EU Counter-Terrorism Coordinator, Council of the European Union. https://data.consilium.europa.eu/doc/document/ST-9066-2020-INIT/en/pdf

Europol (2021). *European Union terrorism situation and trend report*. Publications Office of the European Union, Luxembourg

Europol (2023). *European Union terrorism situation and trend report*. Publications Office of the European Union, Luxembourg

Feddes, A. R., Mann, L., & Doosje, B. (2012). From extreme emotions to extreme actions: Explaining nonnormative collective action and reconciliation. *Behavioral and Brain Sciences, 35*(6), 432-433. doi:10.1017/S0140525X12001197

Ferguson, K. (2016). *Countering violent extremism through media and communication strategies. A review of the evidence*. UK: Partnership for Conflict, Crime & Security Research.

Fishman, B. (2019). Crossroads: Counter-Terrorism and the Internet. *Texas National Security Review,* 2(2), 82–100. http://dx.doi.org/10.26153/tsw/1942

Frischlich, L., Schatto-Eckrodt, T., & Völker, J. (2022). *Withdrawal to the shadows: Dark social media as opportunity structures for extremism*. (CoRE-NRW Forschungspapier, 3). Bonn: Bonn International Centre for Conflict Studies (BICC). https://nbn-resolving.org/urn:nbn:de:0168-ssoar-88967-8

Ganesh, B., & Bright, J. (2020). Countering Extremists on Social Media: Challenges for Strategic Communication and Content Moderation. *Policy & Internet, 12*(1), 6-19. https://doi.org/10.1002/poi3.236

Gaikwad, M., Ahirrao, S., Kotecha, K., & Abraham, A. (2022). Multi-ideology multi-class extremism classification using deep learning techniques. *IEEE Access*, *10*, 104829-104843. doi: 10.1109/ACCESS.2022.3205744

Gallacher, J. (2020). Automated detection of terrorist and extremist content. In B. Ganesh & J. Bright (eds.), *Extreme digital speech: Contexts, responses, and solutions,* 54-66. Dublin: VOX-Pol.

Gaudette, T., Scrivens, R., & Venkatesh, V. (2022). The role of the internet in facilitating violent extremism: Insights from former right-wing extremists. *Terrorism and Political Violence*, *34*(7), 1339-1356. https://doi.org/10.1080/09546553.2020.1784147

Gill, P., Corner, E., Thornton, A., & Conway, M. (2015). *What are the roles of the Internet in terrorism? Measuring online behaviours of convicted UK terrorists.* VOX-Pol Network of Excellence.

Golder, S., Ahmed, S., Norman, G., & Booth, A. (2017). *Attitudes toward the ethics of research using social media: A systematic review. Journal of medical internet research, 19*(6), 195-214.

Groenendijk, P. (2023). White Lives Matter-extremisten 'claimen' teksten op Erasmusbrug: 'We gaan verder op grote locaties'. *Het Parool*, 3 januari 2023. https://www.parool.nl/nederland/white-livesmatter-extremisten-claimen-teksten-op-erasmusbrug-we-gaan-verder-op-grote-locaties~b1edd142/

Guadagno, R. E., Lankford, A., Muscanell, N. L., Okdie, B. M., & McCallum, D. M. (2010). Social influence in the online recruitment of terrorists and terrorist sympathizers: Implications for social psychology research. *Revue Internationale de Psychologie Sociale*, *23*(1), 25-56.

Hall, M., Logan, M., Ligon, G. S., & Derrick, D. C. (2020). Do machines replicate humans? Towards a unified understanding of radicalizing content on the open social web. *Policy & Internet, 12*(1), 109–138. https://doi.org/10.1002/poi3.223

Hassan, G., Brouillette-Alarie, S. , Alava, S.,…& Sieckelinck, S. (2018). Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence. *International Journal of Developmental Science, 12*(1-2), 71-88. https://doi.org/10.3233/dev-170233

Hegghammer, T. (2014). Interpersonal trust on Jihadi internet forums. *SocArXiv.* https://doi.org/10.31235/osf.io/vyeuz

Helmus, T. C., & Klein, K. (2018). *Assessing outcomes of online campaigns countering violent extremism: A case study of the redirect method*. Santa Monica, CA: RAND Corporation.

Henschke, A., & Reed, A. (2021). Toward an ethical framework for countering extremist propaganda online. *Studies in Conflict & Terrorism*, 1-18. https://doi.org/10.1080/1057610X.2020.1866744

Herath, C., & Whittaker, J. (2021). Online radicalisation: Moving beyond a simple dichotomy. *Terrorism and Political Violence, 35*(5), 1027-1048. https://doi.org/10.1080/09546553.2021.1998008

Hodwitz, O. (2020). Legal restrictions and challenges for police and law enforcement authorities. In J. R. Vacca (ed.), *Online terrorist propaganda, recruitment and radicalization*, 137-148. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Hudson, J. M., & Bruckman, A. (2005). Using Empirical Data to Reason about Internet Research Ethics. In H. Gellersen, K. Schmidt, M. Beaudouin-Lafon, & W. Mackay (Eds.), ECSCW 2005 (pp. 287–306). Springer-Verlag. https://doi.org/10.1007/1-4020-4023-7_15

Erdemandi, M., Savoia, E., & Williams, M. J. (2024) Assessing the effectiveness of programs to prevent and counter violent extremism. *National Institute of Justice Journal*. https://nij.ojp.gov/topics/articles/assessing-effectiveness-programs-prevent-and-counter-violent-extremism

Hoffman, B. (2006). *Inside terrorism: Revised and expanded edition*. New York, NY: Columbia University Press.

Holt, T. J., Freilich, J. D, & Chermak, S. M. (2020). Legislation specifically targeting the use of the Internet to recruit terrorists. In J. R. Vacca (ed.), *Online terrorist propaganda, recruitment, and radicalization*, 125-136. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Huey, L. (2015). This is not your mother's terrorism: Social media, online radicalization and the practice of political jamming. *Journal of Terrorism Research, 6*(2), 1–16. https://doi.org/10.15664/jtr.1159

Ingram, K. M. (2016). "More than 'jihadi brides' and 'eye candy': How Dabiq appeals to Western women," International Center for Counter-Terrorism,http://icct.nl/publication/more-than-jihadi-brides-and-eye-candy-how-dabiq-appeals-to-western-women

Jensen, M., James, P., LaFree, G., Safer-Lichtenstein, A., & Yates, E. (2018). The use of social media by United States extremists. *National Consortium for the Study of Terrorism and Responses to Terrorism,* Maryland: START

Johnston, M. F., Iqbal, M., & True, J. (2020). The lure of (violent) extremism: Gender constructs in online recruitment and messaging in Indonesia. *Studies in Conflict & Terrorism*, *46*(4), 470–488. https://doi.org/10.1080/1057610X.2020.1759267

Jones, E. (2017). The reception of broadcast terrorism: Recruitment and radicalisation. *International review of psychiatry, 29*(4), 320-326. https://doi.org/10.1080/09540261.2017.1343529

Jung, E. H., & Sundar, S. S. (2018). Status update: Gratifications derived from Facebook affordances by older adults. *New Media & Society*, *20*(11), 4135-4154. https://doi.org/10.1177/1461444818768090

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! the challenges and opportunities of social media. *Business Horizons, 53*(1), 59-68.

Keatley, D. A., Knight, S., & Marono, A. (2021). A crime script analysis of violent and nonviolent extremists. *Studies in Conflict & Terrorism*, *46*(11), 2285-2302. https://doi.org/10.1080/1057610X.2021.1917651

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241-251. https://doi.org/10.1016/j.bushor.2011.01.005

Kim, S., & Lee, A. (2021). Black Lives Matter and its counter-movements on Facebook. Available at SSRN: https://dx.doi.org/10.2139/ssrn.3980259

King, M. & Taylor, D. M. (2011). The radicalization of homegrown jihadists: A review of theoretical models and social psychological evidence. *Terrorism and Political Violence, 23*(4), 602-622. doi:10.1080/09546553.2011.587064.

Klein, A. (2009). *A space for hate: The white power movement's adaption into cyberspace.* Duluth, MN: Litwin Books, LLC.

Kutner, S. (2020). *Swiping right: The allure of hyper masculinity and cryptofascism for men who join the Proud Boys*. International Centre for Counter-Terrorism. DOI: 10.19165/2020.1.03

Lakhani, S. (2021). *Video gaming and (violent) extremism: An exploration of the current landscape, trends, and threats.* Radicalisation Awareness Network. https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

Lakomy, M. (2019). Recruitment and incitement to violence in the Islamic State's online propaganda: Comparative analysis of Dabiq and Rumiyah. *Studies in Conflict & Terrorism*, *44*(7), 565-580. https://doi.org/10.1080/1057610X.2019.1568008

Lawrence, N. & Robertson, B. W. (2023). Extremist organizations and online platforms: a systematic literature review. *Qualitative Research Reports in Communication*, 1–11. https://doi.org/10.1080/17459435.2023.2240808

Lea, B. R., Yu, W. B., Maguluru, N., & Nichols, M. (2006). Enhancing business networks using social network based virtual communities. *Industrial Management & Data Systems, 106*(1), 121-138.

Lennings, C. J., Amon, K. L., Brummert, H., & Lennings, N. J. (2010). Grooming for terror: The Internet and young people. *Psychiatry, Psychology and Law*, *17*(3), 424–437. https://doi.org/10.1080/13218710903566979

Leukfeldt, E. R., & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention: Recruitment, motives and involvement mechanisms. In S. Hufnagel, & A. Moiseienko (eds.), *Criminal networks and law enforcement: Global perspectives on illegal enterprise*, 75-89. New York: Routledge.

Leukfeldt, E. R. & Roks, R. (2020). Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes. *Deviant Behavior, 42*(11), 1458–1469. https://doi.org/10.1080/01639625.2020.1755587

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W. & Roks, R. (2019). Criminal networks in a digitised world: On the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*, *22*, 324–345. https://doi.org/10.1007/s12117-019-09366-7

Logan, M. K., Windisch, S., & Simi, P. (2024). Adverse childhood experiences (ACE), adolescent misconduct, and violent extremism: a comparison of former left-wing and right-wing extremists. *Terrorism and Political Violence*, *36*(1), 55-74.

Lösel, F., King, S., Bender, D., & Nitsch, H. (2018). Protective factors against extremism and violent radicalization: A systematic review of research. *International Journal of Developmental Science, 12*(1-2), 89-102. doi:10.3233/dev-170241

Macdonald, S., & Whittaker, J. (2019). Online radicalization: Contested terms and conceptual clarity. In J. R. Vacca (ed.), *Online terrorist propaganda, recruitment, and radicalization*, 33-46. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Manrique, P., Cao, Z., Gabriel, A.,... & Johnson, N. (2016). Women's connectivity in extreme networks. *Science advances*, *2*(6), e1501742. DOI:10.1126/sciadv.1501742

Maricourt, C. D., & Burrell, S. R. (2022). #MeToo or #MenToo? Expressions of backlash and masculinity politics in the #MeToo era. *The Journal of Men's Studies*, *30*(1), 49-69. https://doi.org/10.1177/10608265211035794

Marwick, A., Clancy, B. & Furl, K. (2022). Far-Right online radicalization: A review of the literature. *The Bulletin of Technology & Public Life.* https://doi. org/10.21428/bfcb0bff.e9492a11

Mattheis, A. A. (2019). Manifesto memes: The radical right's new dangerous visual rhetoric. *CARR Insights. Centre for Analysis of the Radical Right*.

Matusitz, J. (2014). *Symbolism in terrorism: Motivation, communication, and behavior*. Lanham, MD: Rowman & Littlefield Publishers

McCauley, C. & Moskalenko, S. (2008). Mechanisms of political radicalization: Pathways toward terrorism. *Terrorism and Political Violence, 20*(3), 415-433. doi:10.1080/09546550802073367.

McMillan, D. W., & Chavis, D. M. (1986). Sense of community: A definition and theory. Journal of community psychology, 14(1), 6-23.

Mcswiney, J. (2021). Far-Right recruitment and mobilization on Facebook: The case of Australia. In M. Devries, J. Bessant, & R. Watts (eds.), *Rise of the far right: Technologies of recruitment and mobilization*, 23-40. United States: Rowman & Littlefield Publishers.

Mina, A. X. (2018). *Memes to movements: How the world's most viral media is changing social protest and power*. Boston: Beacon Press.

Ministerie van Justitie en Veiligheid (2023). *Contourenbrief Versterkte Aanpak Online inzake extermistische en terorristische content*. Kenmerk: 4968229.

Mitts, T., Phillips, G., & Walter, B. F. (2022). Studying the impact of ISIS propaganda campaigns. *The Journal of Politics, 84*(2), 1220-1225. https://doi.org/10.1086/716281

Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American psychologist, 60*(2), 161-169. https://doi.org/10.1037/0003-066X.60.2.161

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. https://doi.org/10.1080/19434472.2021.1993302

Mutton, R., Lewis, J., & Marsden, S. (2023). *Online radicalisation: A rapid review of the literature.* Centre for Research and Evidence on Security Threats (CREST).

Nagle, A. (2017). *Kill all normies: Online culture wars from 4Cham and Tumblr to Trump and the alt-right*. Zero Books.

Nanninga, P., de Jonge, L., & Valk, F. (2022). *Fenomeenanalyse Extremisme Noord-Nederland, 2014-2022*. Rijksuniversiteit Groningen.

National Research Council (1991). *Computers at risk: Safe computing in the information age.* Washington, DC: National Academy Press

Nationale Contraterrorisme Strategie 2022-2026: Nationale Contraterrorisme Strategie (NCTS) 2022-2026 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

NCTV (2023). DTN58, Dreigingsbeeld Terrorisme Nederland 58. Dreigingsbeeld Terrorisme Nederland 58 | Rapport | Rijksoverheid.nl

NCTV (2023). DTN59, Dreigingsbeeld Terrorisme Nederland 59, NCTV. Dreigingsbeeld Terrorisme Nederland december 2023 | Publicatie | Rijksoverheid.nl

NCTV (2024). DTN60, Dreigingsbeeld Terrorisme Nederland 50, NCTV.

NCTV (2024). Memes als online wapen. Fenomeenanalyse naar het gebruik van memes door extreemrechts.
file:///C:/Users/sc199/Documents/NCTV%20Fenomeenanalyse+'Memes+als+online+wapen'.pdf

NCTV (2024). Definities gebruikt in het Dreigingsbeeld Terrorisme Nederland.
https://www.nctv.nl/onderwerpen/dtn/definities-gebruikt-in-het-dtn#:~:text=Radicalisering%20%E2%80%93%20Een%20proces%20van%20toenemende%20bereidheid%20om,aanvaarden%20en%20die%20in%20daden%20om%20te%20zetten.

Neumann, P. R. (2013). Options and strategies for countering online radicalization in the United States. *Studies in Conflict & Terrorism,* 36(6), 431–59. https://doi.org/10.1080/1057610X.2013.784568

Nguyen, H., & Gokhale, S. S. (2022). Analyzing extremist social media content: A case study of Proud Boys. *Social Network Analysis and Mining*, *12*(115). https://doi.org/10.1007/s13278-022-00940-6

Nickolson, L., Van Bergen, N., Feddes, A., Mann, L., & Doosje, B. (2021). *Extremistisch denken en doen: Een systematische studie van empirische bevindingen over het radicaliseringsproces*. Den Haag: WODC.

NOS (2022). "Tweede grote EU-techwet moet burgers online beter beschermen". https://nos.nl/artikel/2426177-tweede-grote-eu-techwet-moet-burgers-online-beter-beschermen

Rosenblat, M. O., & Barrett, M. (2023*). Gaming the system: How extremists exploit gaming sites and what can be done to counter them.* New York: NYU Center for Business and Human Rights.

Pauwels, L. & Schils, N. (2016). Differential online exposure to extremist content and political violence: Testing the relative strength of social learning and competing perspectives. *Terrorism and Political Violence, 28*(1), 1-29, DOI: 10.1080/09546553.2013.876414

Peeters, T., van Wonderen, R., Burggraaff, D., & de Wit, N. (2022). *Online extreemrechtse radicalisering. Handvatten voor een preventieve aanpak*. Utrecht: Verwey Jonker Instituut.

Peresin, A. (2015). Fatal attraction: Western muslimas and ISIS. *Perspectives on Terrorism*, 9(3), 21–38. http://www.jstor.org/stable/26297379

Pohl, E., & Riesmeyer, C. (2023). See no evil, fear no evil: Adolescents' extremism-related media literacies of Islamist propaganda on Instagram. *Journal for Deradicalization*, (34), 50-84.

RAN (2020). *Extremists' use of video gaming – strategies and narratives*. https://home-affairs.ec.europa.eu/system/files/2020-11/ran_cn_conclusion_paper_videogames_15-17092020_en.pdf

Rapoport, D. C. (1984). Fear and trembling: Terrorism in three religious traditions. *American Political Science Review, 78*(3), 658–677. https://doi.org/10.2307/1961835

Rijksoverheid (2023). 'EU-regelgeving van start: extra verantwoordelijkheden digitale diensten.' https://www.rijksoverheid.nl/actueel/nieuws/2023/02/17/eu-regelgeving-van-start-extra-verantwoordelijkheden-digitale-diensten

Roks, R., Leukfeldt, E. R., & Densley, J. A. 2020. The hybridization of street offending in the Netherlands. *The British Journal of Criminology, 61*(4), 926–45. https://doi.org/10.1093/bjc/azaa091

Roks, R., & Van der Schoot, J. (2019). Het aanpassingsdilemma online: Een verkennend onderzoek naar extreemrechts op social media. *Tijdschrift voor Criminologie*, *61*(3), 225-245. https://doi.org/10.5553/TvC/0165182X2019061003001

Rousis, G. J., Richard, F. D., & Wang, D. Y. D. (2022). The truth is out there: The prevalence of conspiracy theory use by radical violent extremist organizations. *Terrorism and Political Violence, 34*(8), 1739-1757. https://doi.org/10.1080/09546553.2020.1835654

Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century.* Philadelphia: University of Pennsylvania Press. https://doi.org/10.2307/j.ctt3fhbht

Salama, Aarts, Lucassen (mei 2020). Justitieleinterventies.nl: beschrijving DIAMANT Identiteit en Weerbaarheid bij kwetsbaarheid voor radicalisering. Utrecht: Nederlands Jeugdinstituut, Movisie en Trimbos instituut

Schils, N., & Verhage, A. (2017). Understanding how and why young people enter radical or violent extremist groups. *International Journal of Conflict and Violence, 11*(2), 1-17. https://doi.org/10.4119/ijcv-3084.

Schlette, A., van Prooijen, J. W., Blokland, A., & Thijs, F. (2022). The online structure and development of posting behaviour in Dutch anti-vaccination groups on Telegram. *New Media & Society*, 146144482211284.

Schmid, A. P., & De Graaf, J. (1982). *Violence as communication: Insurgent terrorism and the western news media.* London: Sage.

Scrivens, R., & Conway, M. (2019). The roles of 'old' and 'new' media tools and technologies in the facilitation of violent extremism and terrorism. In R., Leukfeldt, & T. J. Holt (eds.) *The human factor of cybercrime* (1st ed.), 286-309. Routledge. https://doi.org/10.4324/9780429460593

Scrivens, R., Davies, G., & Frank, R. (2018). Searching for signs of extremism on the web: An introduction to sentiment-based identification of radical authors. *Behavioral Sciences of Terrorism and Political Aggression, 10*(1), 39–59. https://doi.org/10.1080/19434472.2016.1276612

Scrivens, R. (2022). Examining online indicators of extremism among violent and non-violent right-wing extremists. *Terrorism and Political Violence*, *35*(6), 1389–1409. https://doi.org/10.1080/09546553.2022.2042270

Shifman, L. (2013). *Memes in digital culture*. MIT Press. https://doi.org/10.7551/mitpress/9429.001.0001

Sikkens, E., Sieckelinck, S., van San, M., & de Winter, M. (2017). Parental reaction towards radicalization in young people. *Child & Family Social Work*, *22*(2), 1044-1053. https://doi.org/10.1111/cfs.12324

Simi, P., & Futrell, R. (2006). Cyberculture and the endurance of white power activism. *Journal of Political and Military Sociology, 34*(1), 115-142. http://www.jstor.org/stable/45294188

Smith, J. M., & Alarid, M. (2019). Terrorism recruitment and radicalization into the 21st century. In J. R. Vacca (ed.). *Online terrorist propaganda, recruitment, and radicalization*, 179-195. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Smith, R. G. (2014). Responding to organised crime through intervention in recruitment pathways. *Trends and issues in crime and criminal justice*, (473), 1-9. https://doi.org/10.52922/ti188384

Staring, R., Bisschop, L., Roks, R., Brein, E., & van de Bunt, H. (2023). Drug crime and the port of Rotterdam: About the phenomenon and its approach. In H. Nelen, & D. Siegel (eds.) *Organized crime in the 21st century: Motivations, opportunities, and constraints*, 43-61. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-21576-6_4

Stevens, T., & Neumann, P. R. (2009). *Countering online radicalisation: A strategy for action.* London: International Centre for the Study of Radicalisation and Political Violence (ICSR).

Tajfel, H., & Turner, J. C. (2004). The social identity theory of intergroup behavior. In J. T. Jost, & J. Sidanius (Eds.), Political Psychology: Key readings (key readings in social Psychology) (pp. 276-293). New York, NY: Psychology Press.

Thijs, F., Rodermond, E., Kleemans, E. R., & Van de Weijer, S. (2022). Violent and nonviolent terrorist suspects: A comparative analysis based on data from the Netherlands. *European Journal on Criminal Policy and Research*, 30, 63-83. https://doi.org/10.1007/s10610-022-09523-9

Thijs, F., Rodermond, E., & Kleemans, E. R. (2024). From extreme ideas to violent and nonviolent outcomes: An in-depth analysis of probation files on terrorist suspects in the Netherlands. *Terrorism and Political Violence*, 1–21. https://doi.org/10.1080/09546553.2024.2344552

Thompson, R. (2011). Radicalization and the use of social media. *Journal of Strategic Security, 4*(4), 167-90. http://www.jstor.org/stable/26463917

Todorovic, D., Sieckelinck, S., Manders, W., Timmerman, G., & van der Linden, J. (2023). Developmental Needs of Adolescents in the Online Lifeworld in the Context of Youth Work. *European Social Work Research , 1*(2), 165-182. https://doi.org/10.1332/OXMM1218

Trend, D. (2007). *The myth of media violence: A critical introduction.* Blackwell Publishing.

Ul Rehman, Z., Abbas, S., Khan, M. A.,… & Saeed, M. A. (2021). Understanding the language of ISIS: An empirical approach to detect radical content on Twitter using machine learning. *Computers, Materials & Continua*, *66*(2), 1075-1090. https://doi.org/10.32604/cmc.2020.012770

Vacca, J. R. (ed.) (2019). *Online terrorist propaganda, recruitment, and radicalization*. Boca Raton, FL: CRC Press, Taylor & Francis Group.

Valentini, D., Lorusso, A. M., & Stephan, A. (2020). Onlife extremism: Dynamic integration of digital and physical spaces in radicalization. *Frontiers in psychology*, *11*(524), 1-15. doi: 10.3389/fpsyg.2020.00524

Valkenburg, P.T. (2014). Schermgaande Jeugd: over jeugd en media. Amsterdam: Prometheus.

Van den Berg, J. (2021). 'Het ging niet meer over de avondklok, maar over het plan de Bijenkorf te plunderen'. *De Volkskrant*. https://www.volkskrant.nl/nieuws-achtergrond/het-ging-niet-meer-over-de-avondklok-maar-over-het-plan-de-bijenkorf-te-plunderen~b542335b

Van der Vegt, I., Mozes, M., Kleinberg, B., & Gill, P. (2021). The Grievance Dictionary: Understanding threatening language use. *Behavior Research Methods, 53*, 2105–2119. https://doi.org/10.3758/s13428-021-01536-2

Van Es, K., & Schäfer, M. T. (2017). *The datafied society. Studying culture through data.* Amsterdam University Press.

Van Wonderen, R. & Peeters, M. (2022). *Werken aan weerbaarheid tegen desinformatie en eenzijdige meningsvorming: Evaluatie lesprogramma Under Pressure*. Utrecht: Verwey-Jonker Instituut.

Van Wonderen, R., Burggraaff, D., Ganpat, S., Cauberghs, O., & Beek, G. van (2023). *Rechtsextremisme op sociale mediaplatforms? Ontwikkelingspaden en handelingsperspectieven*. Utrecht: Verwey-Jonker Instituut.

Vidino, L., & Hughes, S. (2015). *ISIS in America: From retweets to Raqqa*. Washington, DC: GW Program on Extremism.

Von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the digital era: The use of the Internet in 15 cases of terrorism and extremism*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR453.html

Walker, C., & Conway, M. (2015). Online terrorism and online laws. *Dynamics of Asymmetric Conflict, 8*(2), 156-175. https://doi.org/10.1080/17467586.2015.1065078

Walther, S., & McCoy, A. (2021). US extremism on Telegram: Fueling disinformation, conspiracy theories, and accelerationism. *Perspectives on Terrorism*, *15*(2), 100-124. https://www.jstor.org/stable/27007298

Weerman, F. (2019). Criminaliteit, digitalisering en de online sociale wereld. Dezelfde processen in een nieuwe sociale context. *Tijdschrift voor Criminologie*, 61(4), 395-404. https://doi.org/10.5553/TvC/0165182X2019061004008

Weerman, F. M., Lovegrove, P. J., & Thornberry, T. (2015). Gang membership transitions and its consequences: Exploring changes related to joining and leaving gangs in two countries. *European Journal of Criminology, 12*(1), 70-91. https://doi.org/10.1177/1477370814539070

Weimann, G. (2010). Terror on Facebook, Twitter, and YouTube. *Brown Journal of World Affairs, 16* (2), 45–54.

Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research, 3*(2), 75–90.

Weimann, G. (2016). The emerging role of social media in the recruitment of foreign fighters. In de Guttry, A., Capone, F., Paulussen, C. (eds.), *Foreign Fighters under International Law and Beyond*, 77-95. The Hague: T.M.C. Asser Press. https://doi.org/10.1007/978-94-6265-099-2_6

Whittaker, J. (2021). The online behaviors of Islamic state terrorists in the United States. *Criminology & Public Policy*, *20*(1), 177-203. https://doi.org/10.1111/1745-9133.12537

Whittaker, J. (2022). Rethinking online radicalization. Perspectives on Terrorism, 16(4), 27-40.

Williams, T. J. V., & Tzani, C. (2022). How does language influence the radicalisation process? A systematic review of research exploring online extremist communication and discussion. *Behavioral Sciences of Terrorism and Political Aggression*, 1-21. https://doi.org/10.1080/19434472.2022.2104910

Williamson, B. (2020). Brenton Tarrant: The processes which brought him to engage in political violence. *CSTPV Short Papers*, https://cstpv.wp.st-andrews.ac.uk/files/2020/08/Williamson-Tarrant.pdf

Windisch, S., Logan, M. K., & Ligon, G. S. (2018). Headhunting among extremist organizations: An empirical assessment of talent spotting. *Perspectives on Terrorism*, *12*(2), 44-62. http://www.jstor.org/stable/26413313

Windisch, S., Wiedlitzka, S., Olaghere, A., & Jenaway, E. (2022). Online interventions for reducing hate speech and cyberhate: A systematic review. *Campbell systematic reviews*, *18*(2), e1243. https://doi.org/10.1002/cl2.1243

Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: Research trends in internet activism, radicalization, and counter-strategies. *International Journal of Conflict and Violence*, 14(2), 1-20. doi:https://doi.org/10.4119/ijcv-3809

Wolfowicz, M., Litmanovitz, Y., Weisburd, D., & Hasisi, B. (2020). A field-wide systematic review and meta-analysis of putative risk and protective factors for radicalization outcomes. *Journal of Quantitative Criminology, 36, 407-447*. https://doi.org/10.1007/s10940-019-09439-4

Wolfowicz, M., Perry, S., Hasisi, B., & Weisburd, D. (2021). Faces of radicalism: Differentiating between violent and non-violent radicals by their social media profiles. *Computers in human behavior*, *116*, 106646, 1-10. https://doi.org/10.1016/j.chb.2020.106646

Yoder, K. J., Ruby, K., Pape, R., & Decety, J. (2020). EEG distinguishes heroic narratives in ISIS online video propaganda. *Scientific reports, 10*(19593), 1-8. https://doi.org/10.1038/s41598-020-76711-0

Zeiger, S. & Gyte, J. (2021). Prevention of radicalization on social media and the Internet. In P. Schmid (ed.) *Handbook of terrorism prevention and preparedness*, 358-395. The Hague: International Centre for Counter-Terrorism. https://www.icct.nl/sites/default/files/2023-01/Handbook_Schmid_2020.pdf

Zelin, A. Y. (2015). Picture or it Didn't Happen: A Snapshot of the Islamic State's Official Media Output. *Perspectives on Terrorism,* 9(4), 85-97. http://www.jstor.org/stable/26297417

Zych, I., & Naseascu, E. (2022). Is radicalization a family issue? A systematic review of family-related risk and protective factors, consequences and interventions against radicalization. *Campbell Systematic Reviews, 18*(3), 1-68. https://doi.org/10.1002/cl2.1266

Bijlage 1. Samenstelling begeleidingscommissie

Voorzitter
Prof. dr. K. (Kees) van den Bos, Universiteit Utrecht

Leden
Dr. P. (Pieter) Nanninga, Rijksuniversiteit Groningen
Dr. S. (Stijn) Sieckelinck, Hogeschool van Amsterdam
Dr. P. (Pien) van de Ven, Wetenschappelijk Onderzoek- en Datacentrum (WODC)
Medewerker Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

Bijlage 2. Topiclijst interviews

Introductie

- Voorstellen
- Informed consent doornemen
- Inhoud functie
- Jaren ervaring en eerdere ervaring
- Wat verstaat u onder 'extremisme', 'rekrutering', 'mobilisatie' en 'online rekrutering/mobilisatie'?
- Wat verstaat u onder extremistische groepen? [Onze definities toelichten indien ze erg afwijken van definities respondent]
- In hoeverre heeft u binnen uw functie te maken met/zicht op online rekrutering voor extremistische groepen?

Aard en mechanismen van online rekrutering

- Hoe denkt u dat rekrutering en mobilisatie voor extremistische groeperingen in het algemeen verloopt?
- Kent u voorbeelden van online rekrutering/mobilisatie? [zo ja: naar toelichting vragen]
    - Bij welke vormen van extremisme vond dit plaats? [Indien respondent aangeeft dat het bij meerdere extremistische groepen/stromingen plaatsvindt:]
        - Ziet u verschillen/ overeenkomsten in de wijze waarop verschillende groeperingen/stromingen gebruik maken van het online domein voor rekrutering en mobilisatie?
- Kent u voorbeelden van offline rekrutering/mobilisatie? [zo ja: naar toelichting vragen]
    - Bij welke vormen van extremisme vond dit plaats? [Indien respondent aangeeft dat het bij meerdere extremistische groepen/stromingen plaatsvindt:]
        - Ziet u verschillen/ overeenkomsten in de wijze waarop verschillende groeperingen/stromingen offline rekruteren/mobiliseren?
- Op wat voor individuen richten de rekruteerders zich? Wat is de doelgroep?
    - Overeenkomsten/verschillen tussen extremistische groepen/stromingen?
    - Verschillen online en offline?
- Wat voor manieren of methoden van rekrutering ziet u voorbij komen?
    - Welke boodschap wordt daarbij gebruikt?
    - Welke komen het vaakst voorbij of lijken het meest aan te slaan?
    - Overeenkomsten/verschillen tussen extremistische groepen/stromingen?
    - Verschillen online en offline?
- Waarvoor wordt er gerekruteerd? In hoeverre wordt dat vermeld?
    - Overeenkomsten/verschillen tussen extremistische groepen/stromingen?
    - Verschillen online en offline?
- Welke online platforms worden er momenteel gebruikt voor rekrutering en mobilisatie? Wat denkt u dat deze platforms aantrekkelijk maakt?
    - In hoeverre heeft u zicht op wat op deze platforms gebeurd (open vs. gesloten groepen)? Hoe krijgt u daar zicht op?
    - Overeenkomsten/verschillen tussen extremistische groepen/stromingen?
- In hoeverre denkt u dat online rekrutering voor extremisme vergelijkbaar is met (online) rekrutering voor andere vormen van criminaliteit? Welke lessen kunnen we hieruit leren?
- [Zelfradicalisering en radicalisering door peers toelichten] Kent u voorbeelden van mensen die a) vanuit zichzelf online zijn geradicaliseerd of b) zelf op zoek zijn gegaan naar extremistische groepen online?

- [om toelichting vragen: wat voor personen, wat voor groepen/acties, hoe verliep dit proces etc.]

Interactie tussen online en offline gedrag

- Hoe vaak komt het voor dat offline extremistische acties hun oorsprong online vinden? Kunt u daar voorbeelden van geven?
  - Bij welke extremistische stromingen/groepen vond dit plaats? Zag u hierbij verschillen/overeenkomsten?
- Kent u ook voorbeelden van online acties die offline ontstonden of voorbeelden waarbij de volgordelijkheid van online en offline extremisme complexer was?
  - Bij welke extremistische stromingen/groepen vond dit plaats? Zag u hierbij verschillen/overeenkomsten?
- Hoe groot denkt u dat de rol van het online domein is in rekrutering/mobilisatie door extremistische groepen? Speelt het internet/sociale media een primaire of secundaire rol?
  - In hoeverre denkt u dat dit verschilt per stroming/groepering?
- Denkt u dat radicalisering/rekrutering ook enkel online kan plaatsvinden? Zo ja, heeft u daar voorbeelden van?
- Wat weet u over de handelswijze van extremistische netwerken die zowel online als offline actief zijn? Welke acties/handelingen vonden online plaats? En welke offline?
- Is de rol van het online domein in rekruterings-/mobilisatieprocessen de afgelopen jaren veranderd volgens u?
  - Wanneer is het ongeveer veranderd? Op wat voor manier? Welke ontwikkelingen ziet u daarin?

Handelingsperspectieven en mogelijke aanpakken

- Welke maatregelen en aanpakken worden er dat u weet gebruikt voor het tegengaan van online rekrutering door extremistische groeperingen? (bv. Op het gebied van online platforms/sites, weerbaarheid kwetsbare personen, online tegengeluiden etc).
- Welke actoren zijn (in de Nederlandse context) betrokken bij de aanpak van online rekrutering door extremistische groepen? Wat is hun rol? Wat zijn hun bevoegdheden?
- Wat is de rol van de platforms zelf, of welke rol zouden zij moeten hebben volgens u?
- Welke maatregelen/aanpakken zijn volgens u effectief en welke niet? Waarom wel/niet?
- Zouden (mogelijke) aanpakken zich volgens u (meer) moeten richten op specifieke extremistische stromingen? Waarom wel/niet?
- Ziet u bepaalde uitdagingen/obstakels m.b.t. het tegengaan van online rekrutering door extremistische groepen en zo ja, welke?
- Hoe zouden huidige aanpakken (verder) verbeterd kunnen worden volgens u? In hoeverre ziet u mogelijkheden voor nieuwe maatregelen/aanpakken? Hoe zou een dergelijke aanpak eruitzien?
- Welke uitdagingen staan ons nog te wachten als het gaat om de aanpak van online extremisme?

Bijlage 3. Codeerschema contentanalyse

Code	Uitleg code
Online strategieën	
Expliciete rekrutering	Worden leden/abonnees/volgers expliciet opgeroepen of aangemoedigd om lid te worden van de groepering, bijvoorbeeld door middel van een link naar een inschrijvingsformulier?
Directe oproep tot actie • Online oproep tot offline actie • Online oproep tot online actie	Worden leden/abonnees/volgers direct opgeroepen om over te gaan tot bepaalde acties of handelingen namens de groepering?
Evenement/bijeenkomst	Blijkt uit de berichtgeving dat de groepering evenementen of bijeenkomsten organiseert?
Contributie	Blijkt uit de berichtgeving dat leden van de groepering (gevraagd worden om) contributie (te) betalen?
Donatie/financiering	Wordt er op het platform opgeroepen tot donatie of financiering van de groepering?
Merchandise	Blijkt uit de berichtgeving dat de groepering merchandise heeft?
Soorten media • Video • Foto • Afbeelding • Spraakopname • Podcast • Document • Overig	Welke vormen van media worden er gedeeld?
Toegankelijkheid digitaal materiaal	Is het digitale materiaal dat gedeeld wordt openbaar of niet?
Verwijzing naar openbaar platform • Sociale mediaplatform • Website • Nieuwsbrief/magazine • Blog • Overig	Wordt er binnen het platform verwezen naar andere openbare platforms van de groepering? Zo ja, welke?
Verwijzing naar besloten platform	Wordt er binnen het platform verwezen naar besloten platforms van de groepering?
Vermelding verdere contactinformatie	Bijvoorbeeld naam, (e-mail)adres, QR-code etc.
Doorlichtingsprocedure	Blijkt uit berichtgeving dat er aan bepaalde eisen moet worden voldaan om lid te worden van de groepering? Denk bijvoorbeeld aan het hebben van een bepaalde visie, bereidheid om over te

	gaan tot actie, zich te identificeren of elkaar fysiek te ontmoeten.
Overige talen • Engels • Arabisch	Wordt er op het platform gecommuniceerd in andere talen dan in het Nederlands?
Rekruteringsnarratief	Worden er bepaalde narratieven ingezet ten behoeve van rekrutering? Denk bijvoorbeeld aan strategische polarisatie, narrowcasting, positieve aspecten van lidmaatschap benadrukken, uitbuiten van grieven etc.
Wisselwerking tussen online en offline context	
Adverteren • Online adverteren tot offline evenement/bijeenkomst • Offline adverteren voor online platform	Wordt er geadverteerd voor offline evenementen/bijeenkomsten, of wordt er offline geadverteerd voor het online platform?
Netwerken	Blijkt uit de berichtgeving dat de groepering communiceert of contact onderhoudt met andere extremistische groeperingen, bijvoorbeeld door online een andere groepering te adverteren, of door offline ontmoetingen?
Mainstream discussie beïnvloeden	Speelt de groepering in op sociaal-politieke gebeurtenissen, bijvoorbeeld door online propaganda te verspreiden gerelateerd aan een dergelijke actuele gebeurtenis?
Overig	
Overige content	Overige berichten op het platform die niet direct met rekrutering te maken lijken te hebben

Het NSCR is onderdeel van de institutenorganisatie van de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)

Bezoekadres:
De Boelelaan 1077
1081 HV Amsterdam

Postadres:
Postbus 71304
1008 BH Amsterdam

T 020 598 5239
E nscr@nscr.nl
W www.nscr.nl

nscr Nederlands Studiecentrum

Criminaliteit en Rechtshandhaving