Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

29 754 **Terrorismebestrijding**

26 643 **Informatie- en communicatietechnologie (ICT)**

Nr. 729 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 september 2024

Extremistische en terroristische groeperingen gebruiken het internet actief voor de verspreiding van gedachtegoed, rekrutering en geweldsvoorbereiding. Zij zoeken via mainstream platformen gelijkgestemden van over de hele wereld en communiceren vervolgens via heimelijke en versleutelde chats over hun plannen. Recente arrestaties laten zien dat vanuit online contact ook daadwerkelijk kan worden overgegaan tot het plannen van aanslagen. Het kabinet is er alles aan gelegen om aanslagen te voorkomen en acht het daarbij van groot belang om inzicht te krijgen in de wijze waarop rekrutering door en voor extremistische en terroristische groepen op het internet plaatsvindt om de aanpak hierop aan te laten sluiten.

Bijgaand bied ik u het onderzoeksrapport «Radicale reclame op sociale media» aan. Het betreft een onderzoek naar online rekrutering door en voor extremistische groepen, uitgevoerd door het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC). Hieronder geef ik de belangrijkste bevindingen van het onderzoek, de door de onderzoekers geschetste aanbevelingen voor vervolgonderzoek alsook de aanbevelingen voor beleid en de praktijk weer en geef ik een reactie op deze bevindingen en aanbevelingen.

Ik dank de onderzoekers voor hun waardevolle onderzoek dat inzicht biedt in processen van online rekrutering en aanbevelingen doet voor hoe dit in de toekomst nog beter in beeld gebracht en aangepakt kan worden.

Onderzoeksbevindingen

Het online domein als een unieke omgeving

Uit de onderzoeksresultaten blijkt dat het online domein over kenmerken beschikt die kunnen bijdragen aan het proces van rekrutering. Zo ligt de drempel om toe te treden tot een bepaalde extremistische groepering

kst-29754-729
ISSN 0921 - 7371
's-Gravenhage 2024

online veel lager dan offline, vooral omdat het internet anonimiteit biedt. Daarnaast gaat het online domein letterlijk over landsgrenzen en is fysieke nabijheid geen vereiste om te rekruteren of gerekruteerd te worden. Ook kan online eenvoudig een vertekend, positiever beeld geschetst worden van een bepaalde extremistische groepering die daarmee aantrekkelijker kan worden voorgesteld voor potentiële rekruten.

Extremistische groepen maken gebruik van een grote diversiteit aan platforms, waaronder mainstream sociale mediaplatforms zoals Facebook en YouTube en low profile platforms zoals Telegram. Telegram is volgens de professionals op dit moment het meest gebruikte platform onder extremistische groepen. Als reden wordt genoemd dat dit platform meer anonimiteit biedt en minder actief is op het gebied van content-moderatie.

Online rekrutering voornamelijk generiek van aard

Een rekruteringsproces vangt volgens de onderzoekers doorgaans aan op openbare platformen waar niet zozeer illegale content, maar veel vaker borderline (of «legal yet harmful») content bijdraagt aan de aantrekkingskracht van en daaropvolgende toetreding tot extremistische groepen. Het betreft dan (legale) online content die geen strikt terroristisch karakter kent en zelfs niet altijd hoeft te leiden tot geweld, maar wel de veiligheid van burgers en instituties ondermijnt, bijvoorbeeld doordat het aanzet tot haat of opruiing of omdat de content extremistisch gedachtengoed normaliseert.
Uit het onderzoek komt tevens naar voren 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. In een trapsgewijs proces dat hierop volgt, kunnen geïnteresseerden dieper in de groepering binnenkomen door vervolgens uitgenodigd te worden voor besloten groepen.

Wisselwerking tussen online rekrutering (en mobilisering) en offline gedrag

De onderzoekers constateren een wisselwerking tussen online rekrutering en de offline wereld. Ten eerste kan iemands offline situatie, bijvoorbeeld een moeilijke thuissituatie, zijn of haar vatbaarheid voor online rekrutering vergroten. Hiervan is vooral sprake onder jongeren. Hoewel dergelijke kwetsbaarheden niet direct leiden tot lidmaatschap van een groepering, 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. Zo constateren de onderzoekers dat alle onderzochte extremistische groepen tevens offline groepsactiviteiten organiseren en wordt er, in verband met een toenemend veiligheidsbewustzijn, met name in latere rekruteringsfasen meer waarde gehecht aan fysiek contact. Overigens is de link tussen online rekrutering en het overgaan tot daadwerkelijke offline (gewelddadige) acties volgens de onderzoekers ingewikkeld vast te stellen. Uitzondering hierop vormden de rekruteringsstrategieën van Al Qaida en IS waarbij online rekrutering een opmaat was naar het plegen van terroristische aanslagen.

Bestaande aanpakken en handelingsperspectieven

De afgelopen jaren zijn diverse maatregelen ter preventie van online rekrutering ontwikkeld. De onderzoekers hebben deze maatregelen onderzocht en hebben daarbij ingezoomd op de aanpak gericht op het vergroten van (1) de online weerbaarheid, (2) online tegengeluiden (3) regulering en moderatie.

1. Maatregelen gericht op online weerbaarheid

De onderzoekers onderstrepen het belang van maatregelen gericht op het vergroten van de online weerbaarheid, zoals de ontwikkeling van vaardigheden om berichtgeving zelfstandig en kritisch te beoordelen (mediawijsheid), om bronnen te kunnen evalueren en te bevragen en om desinformatie te kunnen onderscheiden van betrouwbare berichtgeving. Het vergroten van de online weerbaarheid gebeurt nu vooral via cursussen en programma's gericht op jongeren. Uit de weinige evaluaties die zijn uitgevoerd, blijkt dat deze bewustwordings- en informatieprogramma's zeker op de korte termijn positieve effecten lijken te hebben. Echter, om jongeren langdurig online weerbaar te maken, wordt door de respondenten binnen het onderzoek een meer structurele inzet nodig geacht van preventieve online weerbaarheidsprogramma's. De rol van ouders bij de digitale opvoeding van jongeren wordt bovendien cruciaal geacht, evenals hun belangrijke signalerende functie als het gaat om preventie van online radicalisering en rekrutering.

2. Aanpak gericht op online tegengeluiden

De inzet van online tegengeluiden door overheden en het maatschappelijk middenveld richt zich op verschillende aan extremisme gerelateerde processen, zoals het voorkomen van online radicalisering en de verspreiding van nepnieuws, en niet specifiek op het voorkomen van online rekrutering. Volgens de onderzoekers is nog onvoldoende duidelijk in hoeverre de inzet van online tegengeluiden (het gewenste) effect sorteert. Bovendien is nog weinig bekend over eventuele onbedoelde neveneffecten of zelfs tegengestelde effecten.

3. Aanpak gericht op regulering en contentmoderatie

Sinds de inwerkingtreding van de Digitale dienstenverordening (Digital Services Act) per februari 2024, geldt dat alle platformen binnen de Europese Unie (EU) verplicht zijn om op te treden tegen illegale content. Uit het onderzoek naar online rekrutering blijkt dat extremistische en terroristische content in toenemende mate lijkt te verplaatsen naar besloten groepen op «low profile» (alternatieve-technologische) platformen. Extremistische content heeft bovendien plaatsgemaakt voor borderline (of «legal yet harmful») content, die zich moeilijker laat modereren.

Aanbevelingen

Met betrekking tot vervolgonderzoek bevelen de onderzoekers aan om de in dit onderzoek gebruikte methode van contentanalyse verder uit te breiden. In vervolgonderzoek ook de gamingsplatforms te betrekken, de ervaringen van mensen die zelf zijn of hebben gerekruteerd mee te nemen en in kaart te brengen welke mogelijkheden overheidsinstanties en tech-bedrijven hebben om online content te modereren en platforms te reguleren, alsmede hoe hier in de praktijk gebruik van wordt gemaakt en wat de effecten hiervan zijn. Daarnaast wordt aanbevolen om evaluatieonderzoek te verrichten om de effectiviteit van de bestaande maatregelen, waaronder op weerbaarheid, in kaart te brengen.

Met betrekking tot beleid en de praktijk komen de onderzoekers tot de volgende aanbevelingen:

- Het verder ontwikkelen van evidence-based programma's ter vergroting van de online weerbaarheid en daarbij professionals vanuit instanties buiten het strafrechtelijk domein nadrukkelijk(er) te betrekken, variërend van jeugdwerkers tot leerkrachten.

- Het professionaliseren van (het voorkomen van) online rekrutering en een intensivering van de samenwerking tussen instanties waarbij met name expertise rond offline radicalisering en rekrutering wordt gecombineerd met expertise rond online processen. Meer in het algemeen wordt aanbevolen om kennis over het online domein sterk te vergroten binnen de lokale overheid.
- Om in samenwerking met de tech-bedrijven verbeteringen te blijven doorvoeren met betrekking tot het detecteren van online extremistisch materiaal.
- Een concretere aanpak van borderline content op te stellen en een «taskforce borderline content» op te richten waarin niet alleen professionals vanuit beleid en de praktijk en vertegenwoordigers van de tech-sector plaatsnemen, maar ook een breed palet aan wetenschappers, inclusief extremisme-experts, juristen en ethici.

Beleidsreactie

Om het handelingsperspectief voor het tegengaan van online extremisme en terrorisme te versterken wordt momenteel gewerkt aan de Versterkte Aanpak Online, waarvan de contouren reeds met uw Kamer zijn gedeeld. De bevindingen en aanbevelingen uit dit onderzoek zijn waardevol en zullen ook worden meegenomen in de uitwerking van deze aanpak die in het najaar van 2024 met u gedeeld zal worden. De versterking loopt langs vier lijnen: de dialoog met de internetsector, het wettelijk instrumentarium, de lokale aanpak en de internationale inzet.[1]

Op dit moment geldt dat waar sprake is van terroristische content de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) op basis van de Verordening Terroristische Online Inhoud en de Uitvoeringswet Terroristische Online Inhoud deze content binnen een uur kan laten verwijderen of ontoegankelijk kan laten maken. Steeds vaker is echter sprake van (legale) online content dat de veiligheid van burgers en instituties ondermijnt. Maatregelen met betrekking tot deze borderline (of «legal yet harmful») content zijn ingewikkeld, omdat tevens het recht op de vrijheid van meningsuiting dient te worden beschermd. In de dialoog met de internetsector die momenteel in het kader van de Versterkte Aanpak Online inzake extremistische en terroristische content wordt gevoerd, worden platformen gewezen op de verantwoordelijkheden die zij hebben met betrekking tot de bescherming van hun gebruikers. Het is daarbij, zoals de onderzoekers ook benadrukken, van groot belang dat tech-bedrijven verbeteringen blijven doorvoeren met betrekking tot het detecteren van online extremistisch materiaal. Dit wordt aangekaart en verder aangemoedigd in de eerdergenoemde dialoog met de internetsector.

In dit onderzoek wordt opnieuw het belang van het (eigen) zoekgedrag in radicaliseringsprocessen aangekaart.[2] Het kabinet hecht grote waarde aan het tegengaan van de dreiging van online radicalisering en extremisme, zeker daar waar het jongeren betreft. Mede naar aanleiding van de motie van het lid Kuik waarin wordt verwezen naar de ReDirect-methode (CDA)[3] heeft de NCTV gezocht naar mogelijkheden om barrières op te werpen in dit online zoekproces, om enerzijds te voorkomen dat personen steeds

---

[1] Kamerstukken II 2022.23, 29 754, nr. 708.

[2] Zie ook het onderzoek naar de relatie tussen (rechts) extremistische content en de werking van aanbevelingsalgoritmen dat het Verwey-Jonker Instituut en Textgain in opdracht van het WODC hebben uitgevoerd: «rechts-extremisme op sociale mediaplatforms? Ontwikkelingspaden en handelingsperspectieven» (WODC, oktober 2023). In dit onderzoek wordt gesteld dat het zoekgedrag van de internetgebruiker zelf minstens zo belangrijk is als de rol van algoritmen in mogelijke radicaliseringspaden.

[3] Kamerstukken II 2022/23, 29 754, nr. 658.

verder in een extremistische fuik terechtkomen wanneer zij op zoek gaan naar online extremistische content, en anderzijds om deze personen door te geleiden naar een (online) hulpaanbod.

Hieruit is gebleken dat voor het effectief opzetten en implementeren van dergelijke online interventies, de overheid in hoge mate afhankelijk is van samenwerking met, en de welwillendheid van sociale mediaplatformen. In het kader van de Versterkte Aanpak Online worden momenteel gesprekken met de internetsector gevoerd over het opzetten van een pilot in lijn met de genoemde motie. In de Versterkte Aanpak Online zal ik de voortgang van deze gesprekken met uw Kamer delen.

De komende jaren zal er bijzondere aandacht uitgaan naar het integreren van het online domein in de lokale integrale aanpak van radicalisering en extremisme.
Door diverse gemeenten wordt er al gewerkt met online jongerenwerkers die via sociale mediaplatformen in contact zijn met jongeren en hen zo ondersteunen. Bij zorgelijk online gedrag[4], kunnen jongerenwerkers daarover in gesprek gaan met jongeren en zo nodig interveniëren binnen de primaire preventie dan wel de persoonsgerichte aanpak in de fysieke leefwereld. Tevens wordt op dit moment bezien hoe het online domein kan worden geïncorporeerd binnen bestaande trainingen van het Rijksopleidingsinstituut tegengaan Radicalisering (ROR). Ten slotte heeft het Landelijk Steunpunt Extremisme (LSE) in samenwerking met de NCTV een online chatfunctie ontwikkeld. Hiermee wordt een laagdrempelige manier aangeboden om jongeren actief in het online domein in een vroegtijdig stadium in contact te brengen met het hulpaanbod van het LSE, zodat radicalisering wordt voorkomen of tegengegaan. De online chatfunctie kan een logisch sluitstuk vormen op een online interventie waarover nu gesprekken plaatsvinden met de internetsector, mede naar aanleiding van de motie van het lid Kuik (CDA)[5].

Ook wordt de inzet op het vergroten van online of digitale weerbaarheid via verschillende (lokale) interventies en het ondersteunen van professionals en gemeenten de komende jaren verder versterkt. Onder meer via de Versterkingsgelden worden gemeenten aangemoedigd om de focus op evidence-based programma's in het kader van de aanpak van online radicalisering en extremisme te versterken. Gemeenten spelen immers een cruciale rol in de preventie en aanpak van radicalisering en extremisme. Samen met jongerenwerkers, scholen en andere ketenpartners spannen zij zich in om te signaleren en in te grijpen als individuen radicaliseren maar ook om een rol te vervullen in het bijstaan van individuen die kwetsbaar zijn voor extremistische en onverdraagzame boodschappen. Zij doen dit vanuit hun eigen expertise en hun lokale binding met inwoners. Het Ministerie van Sociale Zaken en Werkgelegenheid (SZW) ondersteunt (jeugd) professionals en gemeenten bij het betrekken van, en het werken in de online leefwereld. Dit gaat om het bieden van kennis, handelingsperspectief en benodigde randvoorwaarden.

In het rapport doen de onderzoekers diverse aanbevelingen voor vervolgonderzoek. Ook deze aanbevelingen zullen onderdeel vormen van de Versterkte Aanpak Online. Naar de mogelijkheden die overheidsinstanties en tech-bedrijven hebben om online content te modereren en platformen te reguleren, is al het nodige onderzoek gedaan. Zo heeft bijvoorbeeld TNO in opdracht van de NCTV in april 2024, het onderzoeks-

[4] Zoals ondermijning, georganiseerde criminaliteit, radicalisering en extremisme.
[5] Kamerstukken II 2022/23, 29 754, nr. 658.

rapport «Online extremisme en radicalisering: Verkenning van nieuwe detectie en interventiemogelijkheden» opgeleverd.
Wat betreft de aanbeveling om te komen tot een concretere aanpak van borderline content door het oprichten van een taskforce waarin niet alleen professionals vanuit beleid en de praktijk en vertegenwoordigers van de tech-sector plaatsnemen, maar ook een breed palet aan wetenschappers, inclusief extremisme-experts, juristen en ethici, kan worden gemeld dat de NCTV het WODC heeft verzocht om onderzoek te doen naar de haalbaarheid van het opstellen van een duidingskader aan de hand waarvan online platformen kunnen bepalen welke content extremistisch is en mogelijk kan leiden tot verdere radicalisering. Naar gelang de uitkomsten van dit onderzoek zal verder bekeken worden welke stappen er kunnen worden gezet om borderline content aan te pakken. Tevens wordt er in Europees verband gewerkt aan richtlijnen voor internetbedrijven om met borderline content om te gaan. Hier zal Nederland ook actief bij betrokken blijven.

Gelet op de populariteit van online games, ben ik met de onderzoekers van mening dat het cruciaal is dat er meer zicht komt op de rol die gamingplatformen spelen in het kader van online radicalisering en rekrutering. Betere bescherming van minderjarigen is daarbij essentieel. Dit is ook nadrukkelijk onderwerp van gesprek in de eerdergenoemde dialoog met de internetsector. Daarnaast is Nederland lid van een internationale werkgroep van het Global Internet Forum to Counter Terrorism (GIFCT) die gericht is op het ondersteunen van professionals in de gamingindustrie met als doel deze omgevingen te beschermen tegen extremistisch en terroristisch misbruik.[6]

Tot slot

De invloed van extremistische en terroristische online content op de nationale veiligheid is de laatste jaren sterk toegenomen; extremisten en terroristen gebruiken het online domein om hun ideologieën te verspreiden en bewegingen te vormen. In nauwe samenwerking met andere departementen en uitvoeringsorganisaties zal het kabinet de inzet op het tegengaan van online rekrutering door extremistische groeperingen blijven intensiveren. De internetsector vervult hierbij een cruciale rol en ik acht het van groot belang om hierin gezamenlijk te blijven optrekken. Tegelijkertijd blijft ons uitgangspunt om te komen tot een ambitieuze inzet op deze thematiek om aanslagen te voorkomen en ons land veilig te houden.

De Minister van Justitie en Veiligheid,
D.M. van Weel

[6] Gaming Community of Practice (GCoP) van het Global Internet Forum to Counter Terrorism