

CYBERWEERBAARHEID

Inzichten van toekomstige professionals

Onderzoeksartikelen geschreven door studenten in samenwerking met [CyberweerbaarNL](#)

2025 -2026



CYBER
WEERBAAR
NL

Voorwoord

Onze samenleving is ingrijpend veranderd onder invloed van digitale criminaliteit. Het expertisenetwerk Cyberweerbaar NL zet zich in voor een mensgerichte aanpak van digitale weerbaarheid. Deze bundel verzameld inzichten van de professionals van de toekomst om ons te ondersteunen bij het effectief verbeteren van onze weerbaarheid.

De geselecteerde artikelen zijn zorgvuldig samengesteld door de redactie van docent-onderzoekers. De studenten studeren aan NHL Stenden Hogeschool, Hogeschool Saxion en Avans Hogeschool. Ze beschrijven invalshoeken over 'digitaal vakmanschap', 'slachtofferschap' en de impact van de digitalisering op de 'democratische rechtstaat'. Wij hopen dat deze collectie niet alleen kennis biedt, maar praktisch toepasbare tips voor de praktijk, argumentatie voor het debat over cyberweerbaarheid en vernieuwende invalshoeken. De bundeling van artikelen vanuit verschillende opleidingen en geografisch verspreid gelegen hogescholen bevordert het gezamenlijk reflecteren op cyberweerbaarheid. Door over de muren van de hogescholen samen te leren, versterken we verantwoorde innovatie.

Deze eerste editie is de start van een serie waarin we binnen het expertisenetwerk Cyberweerbaar NL jaarlijks studenten een podium bieden en we praktijkpartners van ons netwerk informeren over de inzichten die de professionals van de toekomst opdoen in de praktijk. IT-specialisten lezen over praktische toepassingen, professionals in governance vinden evidence-based onderbouwing voor beleid, Hbo docenten vinden inspiratie voor de onderwijspraktijk en onderzoekers ontdekken nieuwe perspectieven. Lees de artikelen op basis van relevantie voor uw praktijk of van voor tot achteren.

Onze dank gaat uit naar alle auteurs – de professionals van de toekomst – die hun inzichten met ons delen, naar de redactie voor de coördinatie en naar de betrokken hogescholen voor de ondersteuning. De bundel is mede tot stand gekomen met steun van Regieorgaan SIA in het SPRONG programma Cyberweerbaar NL. Mocht u na het lezen vragen hebben of contact zoeken voor samenwerking, horen wij dat graag.

Veel leesplezier gewenst.

Het Regieteam Cyberweerbaar NL

Inhoudsopgave

Inleiding	6
Artikelen digitaal vakmanschap.....	8
Cyberbewust, maar niet incidentklaar	8
<i>Iris Brans</i>	8
Datalek in de zorg.....	19
<i>Stan Harmsen</i>	19
Cyberdreigingen rondom satellieten en ruimtevaart.....	34
<i>Jelmer Brouwer</i>	34
Cyberbewustzijn en cyberweerbaarheid als fundament voor veilig hoger onderwijs	39
<i>George Abboud</i>	39
Payroll Pirates en hoe zij HR beïnvloeden	49
<i>Sarah Salih</i>	49
Cyberdreigingen in softwareleveringsketens	57
<i>Karel Rietveld</i>	57
Artikelen slachtofferschap	70
De belofte van liefde, de realiteit van misleiding; Hoe kwetsbare gebruikers digitale signalen van datingfraude missen.....	70
<i>Rhodee Tonnis</i>	70
De hardnekkigheid van phishing: waarom bewustwordingscampagnes burgers onvoldoende beschermen.....	81
<i>Denise Zieleman</i>	81
Artikelen democratische rechtsstaat	94
Van online narratief naar radicale overtuiging	94
<i>Jordy Kortink</i>	94
Deepfakes en democratische veiligheid	107
<i>Reijer Bakker</i>	107
Doxing van politieagenten.....	117

<i>Maïke Berkenpas</i>	117
Het radicaliseren van jongeren in online omgevingen	133
<i>Dieunée Knoll</i>	133

Inleiding

Digitale weerbaarheid vraagt om mensen die vragen stellen, verbanden leggen en nieuwe perspectieven aandragen. Hoe beschermen we burgers tegen digitale misleiding? Hoe bereiden organisaties zich voor op cyberincidenten? En hoe bewaken we publieke waarden in een digitaliserende samenleving? In deze bundel onderzoeken studenten zulke vragen en vertalen zij hun bevindingen naar inzichten en handelingsperspectieven voor de praktijk.

Het initiatief ontstond vanuit de wens om studentenwerk binnen Cyberweerbaar Nederland (CWNL) een breder podium te geven. Door de beste artikelen te selecteren en te bundelen, maken drie hogescholen deze kennis toegankelijk voor het CWNL-netwerk. De publicatie tijdens het CWNL-jaarcongres verbindt zo onderwijs, onderzoek en praktijk.

De bijdragen komen vanuit de minor Digitale Weerbaarheid van Mens en Organisatie (NHL Stenden Hogeschool), de master Veiligheid en Digitalisering (Hogeschool Saxion) en studenten die hun (afstudeer)stage uitvoerden bij het lectoraat Cyberweerbare Organisaties (Avans Hogeschool). Vanaf komend studiejaar sluit ook de derdejaarsmodule Veiligheid & Technologie van de opleiding Integrale Veiligheidskunde bij Avans Hogeschool aan. Daarmee brengt het initiatief verschillende opleidingsniveaus, disciplines en perspectieven samen.

De artikelen behandelen actuele veiligheidsvraagstukken en combineren wetenschappelijke inzichten met een eigen, onderbouwde argumentatie. Studenten worden uitgedaagd om risico's te analyseren én oplossingsrichtingen te formuleren. Bij de selectie is gelet op originaliteit, argumentatie, maatschappelijke relevantie, toepasbaarheid en schrijfstijl; passend bij het opleidingsniveau.

De bijdragen tonen de breedte van digitale weerbaarheid: naast technologie staan gedrag, vertrouwen, samenwerking en verantwoordelijkheid centraal. Ze brengen kennis bij elkaar, bieden nieuwe invalshoeken en roepen vragen op voor verder onderzoek.

Deze bundel is een podium voor studenttalent en een uitnodiging aan het CWNL-netwerk. We nodigen lezers uit om de inzichten te bespreken, de voorgestelde richtingen te onderzoeken en de verbinding met onderwijs en onderzoek te versterken. Zo kan een studieopdracht uitgroeien tot een samenwerking of een concrete bijdrage aan een digitaal weerbaardere samenleving.

NHL Stenden Hogeschool

De artikelen zijn geschreven door derdejaarsstudenten van de minor Digitale Weerbaarheid van Mens en Organisatie. Deze studenten komen van verschillende studies, onder andere Integrale Veiligheidskunde, Bedrijfskunde, Accountancy en International Human Resource Management. Onderdeel van deze keuzemodule is het schrijven van een onderzoeksartikel over een relevant digitaal veiligheidsvraagstuk,

in lijn met de thematiek van CyberweerbaarNL. De studenten werden daarbij begeleid door Kimberly Bluhm, Sander Ebbers en Bowy de Boer.

Hogeschool Saxion

De artikelen zijn geschreven door eerstejaars deeltijdstudenten van de masteropleiding Veiligheid en Digitalisering van Hogeschool Saxion, Universiteit Twente en het Nederlands Instituut Publieke Veiligheid (NIPV). In het kader van de module Veiligheid in een digitaliserende samenleving voerden studenten een probleemanalyse uit van een vraagstuk dat verband houdt met cybercriminaliteit en/of maatschappelijke spanningen, waarbij zij expliciet de relatie met de democratische rechtsstaat onderzochten. De studenten werden daarbij begeleid door Renze Tjoelker en Robin Christiaan van Halderen.

Avans Hogeschool

De artikelen zijn geschreven door een vierdejaarsstudent Integrale Veiligheidskunde en een derdejaarsstudent Bedrijfskunde die hun (afstudeer)stage uitvoerden bij het lectoraat Cyberweerbare Organisaties van het Centre of Expertise Veiligheid & Veerkracht. Met hun onderzoeken dragen zij bij aan de kennisontwikkeling binnen het lectoraat over hoe mensen en organisaties zich kunnen voorbereiden op cyberincidenten, daarop reageren en daarvan herstellen. De studenten werden daarbij begeleid door Roel de Beer en Renske Korenromp.

Deze bundel is het resultaat van een mooie samenwerking tussen studenten, docenten en CyberweerbaarNL. Wij zijn trots op de inzet en de kwaliteit van de bijdragen en bedanken iedereen die hieraan mee heeft gewerkt!

Namens de betrokken hogescholen,

Kimberly Bluhm, *NHL Stenden Hogeschool*

Renze Tjoelker, *Hogeschool Saxion*

Roel de Beer, *Avans Hogeschool*

Noot: De artikelen zijn gepubliceerd in de vorm waarin zij door de studenten zijn ingediend en zijn niet inhoudelijk of redactioneel bewerkt door docenten.

Artikelen digitaal vakmanschap

Cyberbewust, maar niet incidentklaar

Iris Brans

Integrale Veiligheidskunde (jaar 4), Avans Hogeschool

1. Inleiding

Digitalisering is niet meer weg te denken uit het Nederlandse midden- en kleinbedrijf. Ondernemers gebruiken digitale systemen voor administratie, betalingen, klantgegevens, communicatie en primaire bedrijfsprocessen. Die digitalisering biedt kansen, maar vergroot ook de afhankelijkheid van de beschikbaarheid en betrouwbaarheid van digitale voorzieningen. Wanneer e-mail, boekhouding, een webshop, kassasysteem of klantomgeving uitvalt, is dat daarom al snel meer dan een IT-probleem: de bedrijfsvoering kan direct worden geraakt. Nationale veiligheidsanalyses laten bovendien zien dat cyberincidenten en verstoringen bij leveranciers kunnen leiden tot financiële schade, reputatieverlies en uitval van processen (NCTV, 2025).

Tegelijkertijd zijn organisaties niet in dezelfde mate voorbereid op digitale dreigingen. De Cyber Security Raad (2024) spreekt van een cyberweerbaarheidskloof tussen organisaties die digitale veiligheid structureel organiseren en organisaties die daarin achterblijven. Die kloof is niet uitsluitend een probleem van individuele bedrijven. Mkb-organisaties functioneren in digitaal verweven ketens en zijn afhankelijk van onder meer IT-dienstverleners, cloudleveranciers, boekhoudsystemen, softwareleveranciers en andere zakelijke partners. Een cyberincident bij één schakel kan daardoor processen bij meerdere organisaties verstoren. Onvoldoende cyberweerbaarheid raakt daarmee ook ketenveiligheid, klantvertrouwen, economische veerkracht en maatschappelijke continuïteit (Nederveen et al., 2026).

Voor al kleinere ondernemingen bevinden zich in een kwetsbare positie. Hun digitale afhankelijkheid neemt toe, terwijl tijd, gespecialiseerde kennis, capaciteit en financiële ruimte vaak beperkt zijn. Toch is het te eenvoudig om hun achterstand uitsluitend te verklaren vanuit een gebrek aan bewustzijn. Het TNO onderzoek Veilig digitaal ondernemen onderscheidt vijf typen ondernemers: voorlopers, uitbesteders, overmoedigen, machtelozen en onverschilligen (TNO, 2024). Dit artikel richt zich op de zogenoemde machteloze ondernemers. Zij erkennen cyberrisico's en onderschatten de mogelijke gevolgen niet per definitie, maar ervaren onvoldoende kennis, vaardigheden, middelen of handelingsperspectief om concrete maatregelen te nemen.

Daarmee verschuift het veiligheidsvraagstuk van weten naar doen. In het praktijkonderzoek achter IncidentKlaar kwamen steeds dezelfde drempels terug: beperkte kennis, weinig tijd en middelen, lage prioriteit, ervaren complexiteit,

onzekerheid over de juiste aanpak, afhankelijkheid van IT-dienstverleners en een risico dat abstract blijft. Ondernemers weten vaak wel dat digitale veiligheid belangrijk is, maar niet waar zij moeten beginnen of welke eerste stap voor hun organisatie haalbaar is (Brans, 2026a). Juist dat verschil is relevant, omdat gedrag niet vanzelf volgt uit bewustzijn. Gedragswetenschappelijke modellen laten zien dat mensen niet alleen kennis en motivatie nodig hebben, maar ook vaardigheden, gelegenheid, middelen en vertrouwen om een handeling daadwerkelijk uit te voeren (Ajzen, 1991; Michie, Van Stralen, & West, 2011).

Vanuit deze maatschappelijke en gedragsmatige problematiek is binnen het lectoraat Cyberweerbare Organisaties van Avans Hogeschool het afstudeeronderzoek Van machteloos naar IncidentKlaar uitgevoerd. Centraal stond de vraag hoe een gedragsgerichte interventie kan worden ontwikkeld en getoetst die machteloze mkb-ondernemers met beperkte kennis, tijd en middelen aanzet tot een eerste concrete stap richting basis-herstelvermogen bij cyberincidenten. Onder basis-herstelvermogen wordt in dit onderzoek verstaan: minimale organisatorische voorbereiding om bij een cyberincident doelgericht te kunnen handelen, bijvoorbeeld door verantwoordelijkheden, noodcontacten, eerste acties, communicatie en vervolgstappen vooraf vast te leggen (Brans, 2026a).

Dit artikel betoogt dat het verkleinen van de cyberweerbaarheidskloof voor deze doelgroep daarom méér vraagt dan bewustwording. Zolang ondernemers wel weten dat zij iets moeten doen, maar niet ervaren dat zij kúnnen beginnen, blijft de afstand tussen kennis en gedrag bestaan. De centrale stelling is dan ook: de cyberweerbaarheidskloof in het mkb is óók een handelingskloof. Een effectieve interventie moet die afstand verkleinen door de eerste stap klein, concreet, begrijpelijk en uitvoerbaar te maken.

Dit artikel is gebaseerd op het afstudeeronderzoek “Van machteloos naar IncidentKlaar”, dat door de auteur is uitgevoerd binnen het lectoraat Cyberweerbare Organisaties van Avans Hogeschool. Binnen dit onderzoek is de gedragsgerichte interventie IncidentKlaar ontwikkeld en getoetst.

2. Betogende analyse

2.1 De cyberweerbaarheidskloof is ook een handelingskloof

In discussies over digitale veiligheid ligt de nadruk vaak op kennis: ondernemers zouden onvoldoende weten over phishing, ransomware, updates, multifactorauthenticatie of back-ups. Kennis is belangrijk, maar verklaart niet waarom ondernemers die het risico wél erkennen alsnog weinig maatregelen nemen. Bij machteloze ondernemers ligt het probleem juist in de vertaling van bewustzijn naar uitvoering.

Het praktijkonderzoek laat zien dat meerdere drempels tegelijk optreden. Ondernemers gaven aan niet goed te weten waar zij moesten beginnen, cybersecurity technisch en ingewikkeld te vinden en beperkte tijd, budget en capaciteit te ervaren. Ook afhankelijkheid van IT-dienstverleners speelde een rol.

Ondernemers gaan er geregeld vanuit dat digitale veiligheid door de IT-partij is geregeld, terwijl zij niet altijd zicht hebben op verantwoordelijkheden, herstelafspraken of communicatie tijdens incidenten. Daarnaast bleek digitale veiligheid bij veel ondernemers geen structureel gespreksonderwerp en concurreert het met direct zichtbare prioriteiten in de dagelijkse bedrijfsvoering (Brans, 2026a).

Dat patroon sluit aan bij recent onderzoek naar cybersecurityondersteuning voor kleine en middelgrote ondernemingen. Khan et al. (2025) beschrijven dat kleine organisaties vaak worden geremd door beperkte kennis, begrip, capaciteit en middelen en dat zij niet vanzelf proactief ondersteuning zoeken. Daarmee ontstaat een paradox: juist organisaties die ondersteuning het hardst nodig hebben, beschikken vaak over de minste ruimte om complexe ondersteuning te vinden, beoordelen en implementeren.

Voor de praktijk betekent dit dat algemene adviezen al snel tekortschieten. Een lijst met tien maatregelen kan inhoudelijk juist zijn, maar voor een ondernemer die niet weet welke maatregel eerst moet, kan diezelfde lijst de omvang van het probleem benadrukken. De ondernemer krijgt dan meer informatie, maar nog geen handelingsperspectief. De cyberweerbaarheidskloof wordt daarmee mede in stand gehouden door de manier waarop ondersteuning is ingericht: veel aandacht voor wat organisaties idealiter moeten regelen, maar minder voor hoe een ondernemer met beperkte tijd en kennis daadwerkelijk kan beginnen.

Ook de afhankelijkheid van externe IT-partijen verdient aandacht. Technische dienstverlening kan veel risico's verkleinen, maar technische uitbesteding neemt organisatorische verantwoordelijkheid niet weg. Een IT-leverancier kan accounts beveiligen of back-ups beheren, maar de ondernemer moet nog steeds weten wie tijdens een incident beslist, wie klanten informeert, welke bedrijfsprocessen prioriteit hebben en wat er gebeurt wanneer de leverancier zelf wordt geraakt. Wanneer die afspraken ontbreken, kan vertrouwen in de IT-partij omslaan in schijnzekerheid. De kern is daarom niet dat ondernemers alles zelf moeten doen, maar dat zij voldoende overzicht en eigenaarschap nodig hebben om passende hulp te organiseren.

2.2 *Waarom bewustwording alleen niet genoeg is*

Gedragswetenschap biedt een bruikbaar kader om te verklaren waarom bewustzijn niet automatisch tot actie leidt. Volgens het COM-B-model ontstaat gedrag wanneer drie voorwaarden samen aanwezig zijn: capability, opportunity en motivation (Michie, Van Stralen, & West, 2011). Iemand moet beschikken over de kennis en vaardigheden om een handeling uit te voeren, de praktische gelegenheid en middelen hebben én voldoende motivatie ervaren om daadwerkelijk te handelen. Het Theoretical Domains Framework verfijnt dit verder met factoren als kennis, vaardigheden, overtuiging in eigen kunnen, doelen, sociale invloeden, emoties en beschikbare middelen (Cane, O'Connor, & Michie, 2012).

Die samenhang was duidelijk zichtbaar in het onderzoek. Beperkte capability kwam terug in onvoldoende kennis, overzicht en vertrouwen in eigen kunnen.

Beperkte opportunity werd zichtbaar in tijdsdruk, budget, capaciteit en afhankelijkheid van externe partijen. Motivation werd beïnvloed door lage prioriteit, een abstracte risicobeleving en het idee dat het eigen bedrijf te klein of niet interessant genoeg is. Deze factoren versterken elkaar. Wie niet weet waar te beginnen, schat een taak sneller als groot en ingewikkeld in. Wie weinig tijd heeft, stelt zo'n taak eerder uit. En wanneer het risico abstract blijft, ontbreekt de urgentie om op een drukke werkdag toch tijd vrij te maken.

Ajzen (1991) beschrijft in de Theory of Planned Behavior eveneens dat een positieve houding niet voldoende is voor gedrag. Ook sociale normen en ervaren gedragscontrole beïnvloeden de intentie en uitvoering. Dat is relevant voor cyberweerbaarheid in het mkb. Een ondernemer kan digitale veiligheid belangrijk vinden en zelfs voornemens zijn maatregelen te nemen, maar alsnog niet handelen wanneer de uitvoering buiten de eigen controle lijkt te liggen.

Dit vraagt ook om een andere kijk op de mens in cybersecurity. Zimmermann et al. (2024) pleiten voor een human-centered benadering waarin gebruikers niet primair als 'zwakste schakel' worden behandeld, maar als partners in cybersecurity. Voor het mkb betekent dit dat niet-handelen niet automatisch moet worden geïnterpreteerd als desinteresse of nalatigheid. Een interventie kan technisch correct zijn en toch slecht aansluiten op de tijd, kennis, context of beslisruimte van de gebruiker.

De consequentie is scherp: wanneer niet-handelen voortkomt uit een combinatie van capability, opportunity en motivation, kan een interventie die alleen informatie toevoegt het probleem niet oplossen. Voor machteloze ondernemers moet de uitvoering zelf eenvoudiger worden. Dat vraagt om prioritering, praktische hulpmiddelen, zichtbare vervolgstappen en ondersteuning die beschikbaar is zodra zelfstandig handelen niet lukt. De vraag is dus niet alleen hoe ondernemers bewuster kunnen worden, maar vooral hoe de omgeving zo kan worden ingericht dat de eerste veilige handeling waarschijnlijker wordt.

2.3 Basis-herstelvermogen als haalbaar startpunt

Cybersecuritycommunicatie richt zich terecht sterk op preventie. Sterke authenticatie, updates, back-ups en veilig gedrag verkleinen de kans en impact van incidenten. Tegelijkertijd kan geen enkele organisatie alle cyberincidenten voorkomen. Voorbereiding op respons en herstel is daarom een essentieel onderdeel van digitale weerbaarheid. Het NCSC benoemt incidentvoorbereiding expliciet als basisprincipe en adviseert organisaties vooraf na te denken over continuïteit, incidentrespons en herstel (NCSC, z.d.).

Voor kleinere ondernemers ontstaat hier echter opnieuw een risico op overvraging. Een volledig incidentresponsprogramma, business-continuitymanagementsysteem of informatiebeveiligingsmanagementsysteem is voor een onderneming die nog nauwelijks iets heeft vastgelegd een grote stap. Daarom is in het onderzoek bewust gekozen voor het begrip basis herstelvermogen:

niet het eindniveau van cyberweerbaarheid, maar een minimale organisatorische basis waarmee tijdens een incident doelgericht kan worden gehandeld. Die basis bestaat uit eenvoudige maar cruciale vragen. Wie is verantwoordelijk? Wie moet worden gebeld? Welke systemen, gegevens en leveranciers zijn essentieel? Welke eerste acties zijn nodig? Hoe wordt intern en extern gecommuniceerd? De kracht van deze benadering zit juist in de beperking. Het doel is niet om te suggereren dat een noodcontactenlijst of eenvoudig incidentplan voldoende bescherming biedt. Het doel is om te voorkomen dat een ondernemer pas tijdens een incident voor het eerst over deze vragen nadenkt.

Vanuit veiligheidskundig perspectief is dat relevant omdat weerbaarheid niet hetzelfde is als het voorkomen van alle verstoringen. Weerbaarheid gaat ook over het vermogen om de impact van een incident te beperken, keuzes te maken en herstel te organiseren. Voor de doelgroep van dit onderzoek is een minimale herstelbasis daarom een logische eerste stap: concreet genoeg om uitvoerbaar te zijn en betekenisvol genoeg om tijdens een incident verschil te kunnen maken.

Bovendien reikt die waarde verder dan één onderneming. Kleine bedrijven zijn onderdeel van ketens en verwerken gegevens of ondersteunen processen van klanten en leveranciers. Wanneer zij bij een incident geen duidelijkheid hebben over verantwoordelijkheden, escalatie of communicatie, kan onzekerheid zich door de keten verspreiden. Basis-herstelvermogen is daarmee geen volledige oplossing voor ketenweerbaarheid, maar wel een praktische bouwsteen ervan.

2.4 Van gedragsanalyse naar ontwerpprincipes

Wanneer de kern van het probleem een handelingskloof is, moet een interventie anders worden ontworpen. De Behavior Change Wheel koppelt gedragsproblemen aan interventiefuncties zoals education, training, enablement, persuasion, modelling en environmental restructuring (Michie, Van Stralen, & West, 2011). De Behavior Change Technique Taxonomy biedt vervolgens concrete technieken, waaronder actieplanning, doelen stellen, instructie, feedback en het opdelen van gedrag in haalbare stappen (Michie et al., 2013).

Voor IncidentKlaar zijn deze inzichten vertaald naar vijf ontwerpprincipes. Ten eerste moet een ondernemer snel inzicht krijgen in de eigen situatie. Zonder overzicht blijft digitale weerbaarheid een abstract verzamelbegrip. Ten tweede moet het gewenste gedrag worden vertaald naar kleine stappen met een duidelijk resultaat. Ten derde moeten praktische hulpmiddelen beschikbaar zijn, zodat ondernemers niet telkens vanaf een leeg document hoeven te beginnen. Ten vierde moet ondersteuning bereikbaar zijn voor wie niet zelfstandig verder kan. Ten vijfde moet urgentie herkenbaar worden gemaakt met voorbeelden die aansluiten op de bedrijfsvoering van de ondernemer.

Deze uitgangspunten veranderen de logica van ondersteuning. De interventie begint niet met een normenkader of een volledige lijst van mogelijke maatregelen, maar met drie vragen: waar sta je, wat is nu de eerstvolgende haalbare stap en

hoeveel ondersteuning heb je daarbij nodig? Dat maakt keuzeondersteuning onderdeel van cyberweerbaarheid.

'Klein beginnen' betekent daarbij niet dat de ambitie klein moet blijven. Een ondernemer die alleen een belijst en een eerste incidentprocedure opstelt, heeft nog geen volwassen herstelorganisatie. Maar een eerste uitvoerbare stap kan wel de drempel verlagen naar vervolgacties. Juist voor een doelgroep die door complexiteit en onzekerheid geneigd is uit te stellen, kan de omvang van de eerste opdracht bepalend zijn voor de vraag of er überhaupt beweging ontstaat.

2.5 IncidentKlaar: van inzicht naar een passende vervolgstap

Op basis van de gedragsanalyse is IncidentKlaar ontwikkeld: een laagdrempelige, gedragsgerichte interventie die ondernemers stapsgewijs van inzicht naar actie leidt. Het prototype bestaat uit vier samenhangende onderdelen: een cyberscan, een herstelkit, een workshoproute en een expertcatalogus (Brans, 2026a).

Het tijdens het afstudeeronderzoek ontwikkelde prototype is te bekijken via <https://incidentklaar.lovable.app/>. Het betreft een testbaar prototype dat is ontwikkeld voor demonstratie en evaluatie en nog niet als definitieve uitvoeringsomgeving moet worden beschouwd.

De cyberscan vormt het instapmoment. De ondernemer beantwoordt korte vragen over de eigen digitale afhankelijkheid en voorbereiding. De waarde van de scan zit niet alleen in een score, maar vooral in het creëren van een startpunt. De ondernemer krijgt zicht op aandachtspunten en wordt vervolgens naar een passende route geleid.

De herstelkit is bedoeld voor ondernemers die zelfstandig een eerste basis kunnen opbouwen. Deze bevat onder meer hulpmiddelen voor verantwoordelijkheden, noodcontacten, eerste acties, communicatie, incidentregistratie en evaluatie. Daarmee wordt herstelvoorbereiding tastbaar. De ondernemer hoeft niet zelf te bedenken welke onderdelen minimaal nodig zijn en hoeft niet vanaf een leeg document te beginnen.

Voor ondernemers die de stap niet volledig zelfstandig kunnen of willen zetten, is een workshoproute ontwikkeld. De workshop is geen aanvullende awarenesssessie, maar een werkvorm waarin ondernemers daadwerkelijk onderdelen van hun herstelbasis invullen. Die opzet vergroot de opportunity: er is begeleiding beschikbaar en er wordt bewust tijd gereserveerd. Tegelijkertijd kan de groepssetting motivation ondersteunen doordat ondernemers herkennen dat anderen tegen vergelijkbare problemen aanlopen.

De expertcatalogus vormt de route voor situaties waarin specialistische ondersteuning nodig is. Voor machteloze ondernemers kan ook het vinden en beoordelen van passende hulp een drempel zijn. Door ondersteuning beter vindbaar te maken, wordt de vraag 'wie kan mij hiermee helpen?' onderdeel van het handelingsperspectief.

De vier onderdelen zijn daarmee niet los ontworpen. Zij reageren op verschillende gedragsproblemen. De scan biedt capability door inzicht en overzicht. De herstelkit vergroot capability en opportunity met concrete hulpmiddelen. De workshop voegt begeleiding en een concreet uitvoeringsmoment toe. De expertcatalogus verlaagt de drempel naar specialistische ondersteuning. Motivation wordt ondersteund doordat de ondernemer niet blijft hangen bij algemene risico-informatie, maar direct een haalbare vervolgstap ziet. IncidentKlaar is dus geen volledig cybersecurity- of complianceplatform. Het is bewust ontworpen als eerste route uit handelingsverlegenheid.

2.6 Wat de evaluatie laat zien én waar de grens ligt

Een interventie kan theoretisch overtuigend zijn en toch niet aansluiten op de praktijk. Daarom is het prototype geëvalueerd met ondernemers en cybersecurity-experts. Zestien respondenten vulden een vragenlijst in: twaalf ondernemers en vier experts. Daarnaast zijn vijf walkthroughs verdiepend uitgewerkt. De evaluatie was gebaseerd op het EAST-framework - Easy, Attractive, Social en Timely - en richtte zich op ervaren begripelijkheid, bruikbaarheid, toepasbaarheid, laagdrempeligheid en activerende werking (Brans, 2026a).

De eerste resultaten zijn positief. De gemiddelde score over de gesloten stellingen bedroeg 4,40 op een vijfpuntsschaal. De cyberscan werd het hoogst beoordeeld met 4,63. De startpagina scoorde 4,55 en de uitslag 4,50. Respondenten beschreven het prototype als professioneel, duidelijk, laagdrempelig en praktisch. Vooral de korte scan en de directe vervolgstap werden gewaardeerd, omdat zij het abstracte onderwerp vertalen naar de eigen situatie.

De meest waardevolle uitkomst is echter niet de hoogste score, maar het onderdeel dat lager scoorde. De herstelkit behaalde gemiddeld 3,95. Respondenten vonden de inhoud waardevol, maar twijfelden of kleinere ondernemers de volledige kit zelfstandig kunnen toepassen. Daarmee werd precies het centrale spanningsveld van het onderzoek zichtbaar: wat inhoudelijk nodig is om een minimale herstelbasis te vormen, kan gedragsmatig alsnog te groot voelen voor iemand die vanaf nul begint.

Dat resultaat voorkomt een te gemakkelijke conclusie. Meer hulpmiddelen betekenen niet automatisch meer handelingsperspectief. Wanneer de hoeveelheid informatie te groot wordt, kan handelingsperspectief opnieuw omslaan in handelingsverlegenheid. De oplossing is daarom niet simpelweg alles inkorten, maar de inhoud gefaseerd aanbieden. Een ondernemer moet eerst een minimale start kunnen maken en daarna kunnen verdiepen. Ook moet duidelijk zijn welke onderdelen zelfstandig kunnen worden uitgevoerd en wanneer input van een IT-dienstverlener of andere expert nodig is.

De resultaten hebben bovendien duidelijke beperkingen. De steekproef was doelgericht en beperkt en is niet representatief voor het gehele Nederlandse mkb. De evaluatie onderzocht ervaren bruikbaarheid en activerende werking, maar niet of

ondernemers maanden later daadwerkelijk herstelmaatregelen hebben geïmplementeerd of onderhouden. Enkele technische functies van het prototype waren tijdens de testfase nog niet volledig operationeel. De uitkomsten bewijzen daarom niet dat IncidentKlaar duurzame gedragsverandering veroorzaakt.

Juist die beperking is belangrijk voor een interventie die gedragsverandering beoogt. Een hoge waardering is niet hetzelfde als effect. De logische vervolgstap is daarom een pilot waarin werkelijk gedrag centraal staat: vullen ondernemers daadwerkelijk een minimale herstelbasis in, maken zij afspraken met leveranciers, schakelen zij hulp in wanneer dat nodig is en actualiseren zij de voorbereiding na verloop van tijd? Pas wanneer die vragen positief kunnen worden beantwoord, kan worden gesproken over aantoonbare bijdrage aan duurzame cyberweerbaarheid.

2.7 Van prototype naar bredere impact

De cyberweerbaarheidskloof is niet door één ondernemer of één interventie op te lossen. Kleine bedrijven bewegen zich in een netwerk van IT-dienstverleners, accountants, brancheorganisaties, gemeenten, onderwijsinstellingen, verzekeraars en andere partners. Wanneer ondersteuning alleen beschikbaar is voor ondernemers die zelf actief zoeken, precies weten wat zij nodig hebben en voldoende tijd en budget hebben, blijft juist de machteloze doelgroep moeilijk bereikbaar.

Daarom is de manier waarop ondersteuning wordt aangeboden minstens zo belangrijk als de inhoud. Vertrouwde kanalen kunnen de afstand verkleinen. Ondernemersnetwerken en brancheorganisaties kunnen herkenbare praktijkvoorbeelden bieden. Gemeenten kunnen bereik en lokale aansluiting organiseren. IT-dienstverleners kunnen technische en organisatorische voorbereiding beter verbinden. Onderwijs kan onder begeleiding bijdragen aan praktijkgerichte doorontwikkeling. Khan et al. (2025) wijzen eveneens op de waarde van samenwerkings- en communityvormen bij cybersecurityondersteuning voor kleinere ondernemingen.

Het afstudeeronderzoek zelf had al een beperkte maar concrete praktijkimpact. Meer dan zestig ondernemers, experts en stakeholders waren betrokken via interviews, interactieve sessies, een mkb cyberevent, een kennissessie en walkthroughs. Daarmee werd niet alleen data verzameld; deelnemers werden ook aangezet om na te denken over hun digitale afhankelijkheid en herstelvoorbereiding (Brans, 2026a). IncidentKlaar won in 2026 de Impactprijs Nieuw Ondernemerschap van Avans Hogeschool. Die erkenning bewijst niet dat de interventie op lange termijn effectief is, maar bevestigt wel dat het vraagstuk en de gekozen oplossingsrichting maatschappelijke en ondernemende relevantie hebben.

Voor brede toepassing is opschaling echter niet de eerste stap. Het huidige prototype is ontwikkeld om het interventieconcept zichtbaar en testbaar te maken. Verdere toepassing vraagt om eigenaarschap, veilige technische inrichting, privacyborging, inhoudelijk beheer en duidelijke kwaliteitscriteria. Ook de routes,

branchespecifieke voorbeelden en gefaseerde opbouw van de herstelkit moeten verder worden aangescherpt (Brans, 2026b).

Daaruit volgt een bredere les voor cyberweerbaarheidsinterventies: succes moet niet primair worden gemeten in bereik, downloads of tevredenheid, maar in concrete gedragingen en borging. Een interventie heeft pas werkelijk impact wanneer ondernemers na gebruik niet alleen beter begrijpen waarom cyberweerbaarheid belangrijk is, maar daadwerkelijk een eerste herstelactie uitvoeren en die voorbereiding blijven onderhouden.

3. Conclusie en aanbevelingen

De cyberweerbaarheidskloof binnen het mkb is niet alleen een verschil in beveiligingsniveau, maar ook in handelingsvermogen. Machteloze ondernemers erkennen cyberrisico's, maar lopen vast op beperkte kennis, tijd en middelen, ervaren complexiteit en onzekerheid over waar zij moeten beginnen. De gedragswetenschappelijke analyse bevestigt dat informatie alleen onvoldoende is: gedrag ontstaat pas wanneer capability, opportunity en motivation gezamenlijk voldoende aanwezig zijn (Ajzen, 1991; Cane et al., 2012; Michie, Van Stralen, & West, 2011).

Voor deze doelgroep is basis-herstelvermogen daarom een passend startpunt. Het vormt geen eindniveau van digitale weerbaarheid, maar een minimale organisatorische voorbereiding waarmee een ondernemer tijdens een cyberincident niet volledig vanaf nul hoeft te handelen. IncidentKlaar vertaalt dit uitgangspunt naar een cyberscan, herstelkit, workshop en expertcatalogus. De eerste evaluatie laat zien dat vooral de laagdrempelige scan, directe terugkoppeling en concrete vervolgstappen positief worden ervaren. Tegelijkertijd laat de herstelkit zien dat ondersteuning haar doel kan missen wanneer te veel informatie tegelijk wordt aangeboden. Fasering en passende begeleiding blijven daarom essentieel.

Voor de praktijk volgen vier aanbevelingen. Ten eerste moet herstelvoorbereiding naast preventie een vanzelfsprekend onderdeel van digitale weerbaarheid worden. Ten tweede moet ondersteuning aansluiten op verschillen tussen ondernemers: zelfstandig waar mogelijk, begeleid waar nodig en specialistisch wanneer de situatie daarom vraagt. Ten derde moet de eerste stap herkenbaar en praktisch worden gemaakt, bijvoorbeeld vanuit concrete continuïteitsvragen zoals wat er gebeurt wanneer e-mail, kassa, webshop of klantdata uitvalt. Ten vierde moeten interventies uiteindelijk worden beoordeeld op daadwerkelijk gedrag: leggen ondernemers verantwoordelijkheden en noodcontacten vast, bereiden zij eerste acties voor en houden zij deze afspraken actueel?

Voor IncidentKlaar betekent dit dat een volgende pilot zich vooral moet richten op de daadwerkelijke toepassing en borging. Daarbij kan worden onderzocht welke onderdelen ondernemers uitvoeren, waar zij alsnog afhaken, welke vorm van ondersteuning zij kiezen en of de voorbereiding na verloop van tijd behouden blijft.

Pas daarna kan worden vastgesteld in hoeverre de interventie leidt tot duurzame gedragsverandering en bredere toepassing verantwoord is.

De kern is daarmee dat meer bewustzijn alleen de cyberweerbaarheidskloof niet verkleint. Voor machteloze ondernemers ontstaat digitale weerbaarheid pas wanneer risico-inzicht wordt vertaald naar een eerste concrete en haalbare handeling. Niet perfect voorbereid zijn is het beginpunt; beginnen met voorbereiden wel.

Literatuurlijst

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. [https://doi.org/10.1016/0749-5978\(91\)90020-T](https://doi.org/10.1016/0749-5978(91)90020-T)

Brans, I. J. A. (2026a). Van machteloos naar IncidentKlaar: Een praktische interventie voor het verkleinen van de cyberweerbaarheidskloof binnen het mkb [Afstudeeronderzoek HBO Integratie Veiligheidskunde]. Avans Hogeschool, Lectoraat Cyberweerbare Organisaties.

Brans, I. J. A. (2026b). Van machteloos naar IncidentKlaar: Implementatie- en doorontwikkelplan. Avans Hogeschool, Lectoraat Cyberweerbare Organisaties.

Cane, J., O'Connor, D., & Michie, S. (2012). Validation of the theoretical domains framework for use in behaviour change and implementation research. *Implementation Science*, 7, 37. <https://doi.org/10.1186/1748-5908-7-37>

Cyber Security Raad. (2024). Verkleinen van de cyberweerbaarheidskloof. Cyber Security Raad.

Khan, N., Furnell, S., Bada, M., Rand, M., & Nurse, J. R. C. (2025). Investigating the experiences of providing cyber security support to small- and medium-sized enterprises. *Computers & Security*, 154, 104448. <https://doi.org/10.1016/j.cose.2025.104448>

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 6, 42. <https://doi.org/10.1186/1748-5908-6-42>

Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., Eccles, M. P., Cane, J., & Wood, C. E. (2013). The Behavior Change Technique Taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. *Annals of Behavioral Medicine*, 46(1), 81-95. <https://doi.org/10.1007/s12160-013-9486-6>

Nationaal Cyber Security Centrum. (z.d.). Basisprincipe 5: Bereid je voor op incidenten. Ministerie van Justitie en Veiligheid.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2025). Cybersecuritybeeld Nederland 2025: Riskante mix in een onvoorspelbare wereld. Ministerie van Justitie en Veiligheid.

Nederveen, F., Silferversten, E., Aquilio, M. C., & Warnier, S. (2026). Digitale weerbaarheid van Nederlandse organisaties. RAND Corporation.

TNO. (2024). Veilig digitaal ondernemen (TNO 2024 R10701). TNO.

Zimmermann, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M., & Ebert, N. (2024). Human-Centered Cybersecurity Revisited: From Enemies to Partners. *Communications of the ACM*, 67(11), 72-81. <https://doi.org/10.1145/3665665>

Noot: praktijkresultaten en evaluatiescores zijn ontleend aan het afstudeeronderzoek en implementatie- en doorontwikkelplan van Brans (2026a, 2026b).

Datalek in de zorg

Stan Harmsen

Master Veiligheid en Digitalisering, Hogeschool Saxion

1. Aanleiding

Begin juli 2025 is Clinical Diagnostics Nederland – medisch laboratorium dat in opdracht van Bevolkingsonderzoek Nederland (hierna: Bevolkingsonderzoek) uitstrijkjes van onder andere baarmoederhalskanker onderzoekt – getroffen door een cyberaanval (Clinical Diagnostics Nederland, z.d.). Daarbij heeft de hacker zich toegang verschaft tot medische gegevens van 941.000 betrokken vrouwen die zich hebben laten testen op baarmoederhalskanker (Bevolkingsonderzoek Nederland, 2025b; NOS, 2025). Naar aanleiding van de hack informeerde de Minister van Volksgezondheid, Welzijn en Sport (*Kamerstukken II, 32761, nr. 327, 2025*) de Tweede Kamer over het datalek dat heeft plaatsgevonden en dat de samenwerking tussen Bevolkingsonderzoek Nederland en het laboratorium tijdelijk wordt opgeschort in het kader van het lopende onderzoek.

Als gevolg van het datalek liggen bijzondere persoonsgegevens van veel vrouwen digitaal op straat. In een artikel van de Erasmus University Rotterdam (2025) wordt de ernst hiervan benadrukt. Vooralsnog heeft het datalek nog niet geleid – in ieder geval niet aantoonbaar – tot directe financiële schade voor de betrokkenen. Wel heeft er een diepe schending van de privacy plaatsgevonden. Om die reden hebben veel vrouwen zich aangesloten bij een gezamenlijke schadeclaim die loopt tegen Bevolkingsonderzoek (Nu.nl, 2025) én heeft een aantal gedupeerden aangifte gedaan bij de politie (NOS, 2026b).

Hoewel Bevolkingsonderzoek in 2024 nog een stijging zag in de deelname van het onderzoek naar baarmoederhalskanker (RIVM, 2025), zegt het RIVM zelf ook niet te weten wat de gevolgen van de hack kunnen zijn voor de deelname aan het onderzoek in de komende jaren. In de eerder aangehaalde kamerbrief onderschrijft de Minister van VWS het belang van deelname aan het bevolkingsonderzoek:

Ik benadruk nog eens dat deelname aan het bevolkingsonderzoek van groot belang is. Doel van het bevolkingsonderzoek baarmoederhalskanker is verlaging van de sterfte door baarmoederhalskanker of de voorstadia daarvan in een vroeg stadium op te sporen. Door vroege opsporing kan voorkomen worden dat baarmoederhalskanker zich ontwikkelt of kan baarmoederhalskanker beter behandeld worden. Daardoor sterven minder mensen aan baarmoederhalskanker (*Kamerstukken II, 32761, nr. 327, 2025*).

Cyberaanvallen gericht op zorgorganisaties of hun leveranciers zijn echter geen nieuw fenomeen. Onlangs is Chipsoft, leverancier van het elektronisch patiëntendossier van 70 procent van de Nederlandse ziekenhuizen, nog slachtoffer

geworden van een cyberaanval (NOS, 2026a). Naar schatting van Shackleford (2015, geciteerd in Schmidt et al., 2021, p.1) ontstaat 80% van de cyberinbreuken in de toeleveringsketen. Ook bij Bevolkingsonderzoek lag de oorzaak in de leveranciersketen. Het Z-CERT (2023; 2024a; 2025; 2026) onderschrijft de urgentie van deze dreiging in haar dreigingsanalyse. Hierin komt niet alleen aan bod dat de dreiging 'Ransomware of afpersen met datalekken bij leverancier' één van de grootste actuele dreigingen is (Z-CERT, 2026, p. 7), maar eveneens dat het effectief managen van informatiebeveiliging in leveranciersrelaties één van de meest aangetroffen tekortkomingen is van organisaties die NEN 7510 gecertificeerd zijn (Z-CERT, 2026, pp. 74-75).

De casus rond Bevolkingsonderzoek laat zien dat een datalek in de zorgsector een grote impact kan hebben op betrokkenen waarbij de gevolgen vermoedelijk kunnen variëren per persoon. Daarnaast, omdat het bevolkingsonderzoek wordt georganiseerd vanuit een publiek gezondheidsprogramma, kan een datalek gevolgen hebben die verder reiken dan alleen de schending van privacy. In dit literatuuronderzoek staat daarom centraal welke factoren potentieel bijdragen aan het ontstaan van datalekken bij toeleveranciers, en welke invloed een dergelijk datalek kan hebben op het vertrouwen van betrokkenen. De maatschappelijke en normatieve betekenis hiervan, in relatie tot publieke waarden, de democratische rechtsstaat en de rol van de overheid, wordt in de kritische beschouwing verder uitgewerkt.

In dit literatuuronderzoek staan onderstaande hoofd- en deelvragen centraal: *Welke factoren dragen potentieel bij aan het ontstaan van datalekken in de toeleveringsketen en welke gevolgen kan een dergelijk datalek in de zorgsector hebben op het vertrouwen en de participatie van patiënten?*

Deelvragen

1. Welke factoren dragen potentieel bij aan het ontstaan van datalekken in de toeleveringsketen?
2. Welke invloed kan een datalek in de zorgsector hebben op het vertrouwen en de participatie van patiënten?

2. Onderzoeksmethoden

2.1 Dataverzameling

Relevante data zijn verzameld door middel van literatuuronderzoek en deskresearch. Onderstaand wordt dieper ingegaan op de gebruikte werkwijze voor het verzamelen van relevante data en documenten.

Literatuur. Voor de literatuurstudie zijn studies en vakliteratuur geselecteerd op basis van een aantal inclusie- en exclusiecriteria: 1) documenten zijn uitsluitend meegenomen die inhoudelijk relevant zijn voor het onderwerp of kunnen bijdragen aan de definiëring van centrale begrippen; 2) documenten moesten wetenschappelijke of peer-reviewed literatuur, of relevante vakliteratuur zijn; en 3)

de documenten moesten publiek beschikbaar en Nederlands- of Engelstalig zijn. Data is verzameld door het toepassen van de bibliografische methode en de sneeuwbalmethode. Ook zijn publicaties meegenomen die al voor andere doeleinden waren verzameld.

Deskresearch. Naast literatuur zijn ook (beleids)documenten van publieke organisaties geraadpleegd en opgenomen. Hierbij gaat het om beleidsdocumenten van de bij de casus betrokken organisaties of beleidsdocumenten en wet- en regelgeving van Nederlandse of Europese overheidsinstanties (ook: kamerbrieven en beleidsagenda's). Hierbij gaat het om documenten die publiek beschikbaar zijn.

2.2 Afbakening

In deze literatuurstudie is gekozen voor een interdisciplinaire benadering om antwoord te geven op de hoofd- en deelvragen. De geselecteerde disciplines zijn: 1) het recht vanwege de geldende normenkaders waarop inbreuk is gedaan, 2) informatica, specifiek gericht op informatiebeveiliging en cybersecurity en 3) psychologie vanwege de mogelijke reactie van een individu op een datalek in relatie tot het ontvangen van zorg.

2.3 Gebruik van GenAI

In dit verslag is GenAI uitsluitend als hulpmiddel gebruikt als aanvullende controle op spelling, taal en grammatica. Hierbij is gebruikgemaakt van ChatGPT (OpenAI, 2026).

3. Probleemanalyse

De resultaten zijn in dit hoofdstuk onderverdeeld per deelvraag.

3.1 Welke factoren dragen potentieel bij aan het ontstaan van datalekken in de toeleveringsketen?

Zoals aangegeven in de aanleiding ontstaat 80% van de cyberinbreuken in de toeleveringsketen (Shackleford, 2015, geciteerd in Schmidt et al., 2021, p.1) waarbij het Z-CERT (2023; 2024a; 2025; 2026) hier een aantal jaren op rij aandacht voor vraagt in haar jaarlijkse dreigingsanalyse. Een grote uitdaging die eveneens werd aangekaart was het effectief managen van informatiebeveiliging in leveranciersrelaties (Z-CERT, 2026, pp. 74-75). In deze paragraaf wordt dieper ingegaan op de huidige manier van leveranciersmanagement en de gevonden tekortkomingen daarvan.

Uitdagingen. Een van de mogelijke redenen van het ontstaan van 80% van de cyberinbreuken in de toeleveringsketen is het feit dat veel organisaties in een hoog tempo zijn gaan digitaliseren tijdens de COVID-19 pandemie waarbij informatietechnologie (IT) meer bij externe partijen is belegd (Latsiou & Lambrinoudakis, 2026). Hiermee zijn organisaties in toenemende mate afhankelijk geworden van toeleveranciers. Deze afhankelijkheid is echter niet lineair, maar ook

steeds vaker onderling en wederzijds (Latsiou & Lambrinoudakis, 2026; Mares, 2010, geciteerd in Seid et al., 2025). Hierdoor is de toeleveringsketen groter en complexer geworden, maar ook kwetsbaarder aangezien één cyberinbreuk consequenties kan hebben voor meerdere partijen (Latsiou & Lambrinoudakis, 2026; Seid et al., 2025). Daarbij wordt door beide onderzoeken aangehaald dat derde partijen en het beperkte zicht op wat zij doen ook één van de verklarende factoren kan zijn van het ontstaan van cyberinbreuken in de keten. Latsiou en Lambrinoudakis (2026) voegen daaraan toe dat aanvallers steeds vaker aanvallen uitvoeren in de keten omdat directe aanvallen op goed beveiligde organisaties duurder of moeilijker worden. Als laatste noemen Latsiou en Lambrinoudakis (2026) dat beheersmaatregelen zoals het opstellen van vragenlijsten voor leveranciers niet langer afdoende zijn. Tegelijkertijd concluderen zij dat er weinig methodieken beschikbaar zijn met betrekking tot risico's in de toeleveringsketen.

De rol van wet- en regelgeving. Bovenstaande schetst dat cyberinbreuken in de toeleveringsketen diverse oorzaken kunnen hebben. Tegelijkertijd zijn organisaties op grond van wet- en regelgeving verplicht om informatiebeveiliging in te richten. Hierbij kan worden gedacht aan de Algemene Verordening Gegevensbescherming (hierna: AVG) op het moment dat er persoonsgegevens worden verwerkt of de NIS2-richtlijn voor essentiële en belangrijke organisaties.

AVG. Sinds mei 2018 is de AVG van toepassing vanuit de Europese Unie. De essentie van de verordening is niet nieuw: bedrijven, overheden en andere organisaties mogen niet zomaar persoonsgegevens verwerken van burgers die binnen de Europese Unie wonen. Indien er persoonsgegevens worden verwerkt, dan behoort deze verwerking voldoende vertrouwelijkheid plaatsvinden en moet de integriteit van de gegevens worden gewaarborgd. Verdere invulling aan deze eis is te vinden in de AVG (2016, Artikel 32) waar organisaties die persoonsgegevens verwerken verplicht worden om passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. De AVG schrijft niet voor hoe organisaties dit moeten bereiken.

Netwerk- en informatiesystemen (NIS2-richtlijn). De Europese Unie is momenteel bezig met het beleidsprogramma 'het digitale decennium' (Europese Commissie, 2025). Dit beleidsprogramma is door de Europese Unie opgezet om zowel de talloze kansen van een digitale wereld te grijpen als de belangrijke uitdagingen aan te gaan.

Om richting te geven aan het decennium zijn er vier hoofddoelen geformuleerd: 1) Een digitaal geschoolde bevolking en hoogopgeleide digitale professionals, 2) Veilige en duurzame digitale infrastructuur, 3) Digitale transformatie van bedrijven en 4) Digitalisering van overheidsdiensten. Aanvullend op deze hoofdpunten heeft de Europese Commissie (2025) verschillende subdoelstellingen geformuleerd om te waarborgen dat Europese waarden worden gerespecteerd, waaronder 'Bouwen aan een veilige digitale wereld' en 'Ervoor zorgen dat alle organisaties cyberbeveiligingsmaatregelen nemen'. Om invulling te geven aan de

twee laatstgenoemde doelstellingen heeft de Europese Commissie de NIS2-richtlijn opgesteld, wat een opvolger is van de NIS1 (Europese Commissie, 2026). Met de komst van de NIS2-richtlijn beoogt de Europese Commissie het gemeenschappelijke ambitieniveau op het gebied van cyberbeveiliging te verhogen door kritieke sectoren aan te wijzen die onder de richtlijn vallen. Waar de gezondheidszorg al onder de NIS1 viel, zijn overheidsdiensten onlangs toegevoegd met de komst van de NIS2 (Europese Commissie, 2026). Waar de AVG niet expliciet voorschrijft welke maatregelen er geïmplementeerd moeten worden, geeft de *NIS2-richtlijn* (2022, Artikel 21, lid 2) wel tien minimale maatregelen aan om netwerk- en informatiesystemen te beveiligen. Onder andere de beveiliging van de toeleveringsketen wordt hierin genoemd. Een belangrijk, maar tegelijkertijd ook een complex aspect van informatiebeveiliging (Fernando et al., 2023; Schmidt et al., 2021).

Manier van leveranciersmanagement: normenkader. Om organisaties te helpen voldoen aan de wettelijke eisen omtrent informatiebeveiliging bestaan er normenkaders voor informatiebeveiliging, zoals de ISO 27001 (Clements & Milton, 2018) of, ook relevant voor Bevolkingsonderzoek, de NEN 7510 – Nederlandse norm voor informatiebeveiliging in de zorg gebaseerd op de ISO 27799 (Wirken, 2012). Vanwege de aard en essentie van de ISO 27001 waarin best-practice richtlijnen worden aangeboden voor informatiebeveiliging kan dit organisaties helpen te voldoen aan de eis vanuit de AVG voor persoonsgegevensbeveiliging (Clements & Milton, 2018; Lopes et al., 2019). Indien organisaties zich laten certificeren aan een normenkader brengt dit verscheidene voordelen met zich mee. Hulshof en Daneva (2021) omschrijven daarbij dat het wekken van onderling vertrouwen (lees: tussen stakeholders) een algemeen onderschreven positief effect is. In dezelfde literatuurstudie van Hulshof en Daneva (2021) wordt eveneens gekeken naar kwesties en uitdagingen die verband houden met het certificeren voor informatiebeveiliging: ‘De meest genoemde uitdaging is ontoereikende beveiligingsgarantie ...’ (p. 161). Opvallend is dat het grootste voordeel en het grootste nadeel tegenstrijdig zijn. Waar certificeringen enerzijds veel worden gebruikt om vertrouwen onder stakeholders op te bouwen is het maar de vraag of dit vertrouwen gerechtvaardigd is. Ahmed et al. (2025) onderschrijven deze bevinding in een onderzoek naar de effectiviteit van kaders voor datagovernance bij het waarborgen van de veiligheid en privacy van gezondheidsgegevens: deelnemers waren ontevreden over de mate van bescherming, vertrouwen en beveiliging die normenkaders bieden. Bevindingen uit het onderzoek doen echter geen afbreuk aan de meerwaarde van normenkaders, maar tonen volgens Hulshof en Daneva (2021, p. 165) aan dat een IT-controleproces expertise vergt van de auditor en dat informatiebeveiliging van nature complex is wat het moeilijk maakt om deze goed te beschrijven in een eenduidig sectorspecifiek controlekader (Ahmed et al., 2025).

Om deze risico's in de toeleveringsketen effectief te mitigeren erkent het Z-CERT (2024b) het belang om leveranciers te selecteren die voldoen aan bepaalde

normenkaders (zoals de ISO 27001 of NEN 7510). Z-CERT (2024b, p. 12) benadrukt daarbij het belang om goed te toetsen op de effectiviteit van de geïmplementeerde beheersmaatregelen. Daarnaast stelt het Z-CERT dat een certificaat de opzet en het bestaan aantoont van beheersmaatregelen, maar niet de effectiviteit daarvan.

Op basis van bovenstaande literatuur kan daarmee worden gesteld dat cyberinbreuken in de toeleveringsketen potentieel verschillende oorzaken kennen. Hoewel organisaties vanuit diverse wet- en regelgeving verplicht zijn om passende beveiligingsmaatregelen te treffen, laat de literatuur zien dat certificeringen op normenkaders onvoldoende zekerheid bieden voor effectieve informatiebeveiliging in de toeleveringsketen terwijl ze hier wel ten dele voor worden gebruikt. Winst lijkt daarbij te kunnen worden behaald in de wijze waarop informatiebeveiliging binnen leveranciersrelaties wordt getoetst en gecontroleerd.

3.2 Welke invloed kan een datalek in de zorgsector hebben op het vertrouwen en de participatie?

In een studie van Pool et al. (2024) wordt op basis van bestaande literatuur een integraal model samengesteld dat enerzijds de factoren toont die datalekken in de hand werken, maar ook wat de impact is van een datalek op patiënten in de zorg. Hieruit kwamen vier thema's naar boven die gericht waren op gedrag van de patiënt: 1) bezorgdheid over privacy, 2) achterhouden van gezondheidsinformatie, 3) minder gebruik van het systeem en 4) aangetast vertrouwen. Daarnaast werden er twee overige thema's gevonden die invloed hebben op de bedrijfswaarde. Deze zijn: 5) kwaliteit van zorg en 6) kosten voor het herstellen van vertrouwen. Hieronder wordt dieper ingegaan op deze thema's.

Impact van datalekken in de zorg. Park en Lim (2025) onderschrijven het derde punt van Pool et al. (2024). In hun onderzoek staat de vraag centraal of datalekken bij een ziekenhuis invloed hebben op het terugkeren van patiënten naar ziekenhuizen en welke factoren meespelen in die overweging. Deze vragen trachten Park en Lim te beantwoorden door de Technology Threat Avoidance Theory (TTAT) van Liang en Xue (2009) centraal te stellen. In de TTAT staan twee belangrijke processen centraal die mensen doorlopen nadat ze een dreiging hebben ervaren: 1) dreigingsbeoordeling: de dreiging wordt beoordeeld op basis van de door hun waargenomen kwetsbaarheden voor mogelijke negatieve gevolgen. En 2) coping beoordeling: wanneer er naar aanleiding van het incident een dreiging wordt waargenomen, start het evalueren van eventueel te nemen maatregelen (coping opties) en zullen beschermingsmaatregelen worden getroffen om de dreiging te vermijden. Park en Lim (2025) voegen echter nog een element toe aan het proces van coping beoordeling. Waar eerdere literatuur zich met name heeft gericht op het eerste aspect, zeggen Park en Lim (2025) dat de effectiviteit van de te nemen maatregel net zo belangrijk is. In relatie tot een datalek bij een ziekenhuis kan een patiënt ervoor kiezen om niet meer naar het ziekenhuis te gaan, maar kan dat immers ook sterk negatieve invloed hebben op de gezondheid van de patiënt. De mate van

afhankelijkheid van het ontvangen van zorg kan daarmee impact hebben op het wel of niet nemen van zelfbeschermende maatregelen tegen het datalek. Park en Lim (2025, p. 1295) zien een daling in het aantal ziekenhuisbezoeken als gevolg van een datalek. Gemiddeld 4,65% van de patiënten gaat minder vaak naar het ziekenhuis. Dit effect is echter zwakker naarmate een patiënt afhankelijker is van de te ontvangen zorg. Bovenstaand onderzoek vindt empirische steun in de casus rond Bevolkingsonderzoek. In een kamerbrief (*Kamerstukken II*, 32761, nr. 334, 2026) over de huidige stand van zaken van het datalek wordt aangegeven dat het aantal ingestuurde testen 11% lager was dan in diezelfde maanden van 2024. De daling trok daarna enigszins bij. Daarnaast heeft Bevolkingsonderzoek zelf een meting laten uitvoeren op het vertrouwen in de instantie. Van de 1000 respondenten heeft 13% aangegeven niet (meer) te willen deelnemen als gevolg van de hack.

In lijn met wat Pool et al. (2024) stellen blijft de schade aan vertrouwen niet beperkt tot het minder bezoeken van de zorginstelling waar het datalek is gebeurd. Cyberinbreuken kunnen ook invloed hebben op de informatie die patiënten aan zorgverleners toevertrouwen (Agaku et al., 2013; Shenoy & Appel, 2017, in Coventry & Branley, 2018, p. 50). In de studie van Agaku et al. (2013, p. 375) gaf 12,3% van de respondenten aan ooit informatie achtergehouden te hebben voor een zorgverlener uit bezorgdheid over de veiligheid en privacy van hun gezondheidsgegevens. Lott et al. (2020) onderschrijven deze bevinding door het tegenovergestelde vast te stellen. Zij stellen namelijk dat vertrouwen sterk samenhangt met een lagere kans dat er ooit informatie wordt achtergehouden.

Esmaeilzadeh en Sambasivan (2017) onderschrijven daarnaast het wantrouwen ten aanzien van informatie-uitwisseling van gezondheidsgegevens als gevolg van een datalek (Bos & Verheij, 2024). Ook hier bevestigen Lott et al. (2020) dit door omgekeerde redenering. Patiënten met een groter vertrouwen in de deskundigheid van artsen zijn eerder bereid om belangrijke medische gegevens te delen met andere zorgverleners. Naast bovenstaande impact en zorgen over privacy stellen Choi et al. (2019) dat ook de kwaliteit van zorg wordt geraakt door een beveiligingsinbreuk (zoals een datalek). Zo gaan de maatregelen die een datalek moeten verhelpen gepaard met een verslechtering van de tijdigheid van de zorg en de behandelresultaten.

Een datalek kan volgens bovenstaande literatuur negatieve invloed hebben op de bereidheid om terug te keren naar de zorginstelling waar de gezondheidsinformatie is gelekt. Dit beperkt zich echter niet hiertoe. Datalekken schaden ook het vertrouwen in het delen van medische informatie met de zorgverlener én de steun voor de informatie-uitwisseling tussen verschillende zorgpartijen. Naast het geschaad vertrouwen, lijkt ook de kwaliteit van zorg te worden geraakt door maatregelen die de inbreuk moeten tegengaan.

4. Oplossingsrichtingen

Eigenaarschap van kritieke processen

Het verlenen van gezondheidszorg is een kritisch proces. Dit wordt niet alleen onderschreven door de NIS2-richtlijn, maar kan eveneens worden gesuggereerd vanwege het sociale grondrecht op gezondheidszorg. In de presentatie van Rolf van Wegberg (persoonlijke communicatie, 5 maart 2026) bij het studium generale van Saxion wordt aangegeven dat de overheid eigenaarschap moet nemen van data (lees: persoonsgegevens) die worden verwerkt in kritische processen. Verantwoordelijkheden van organisaties in de keten dienen daarbij duidelijk belegd te zijn, onder andere voor informatiebeveiliging. In het verlengde daarvan dient het controleren op certificeringen voor informatiebeveiliging niet als eindpunt te worden gezien, maar als een middel om het gesprek aan te gaan met kritieke leveranciers en/of leveranciers die gevoelige informatie verwerken waarbij het van belang is om de effectiviteit van geïmplementeerde beheersmaatregelen te toetsen (Z-CERT, 2024b, p. 12).

IT auditen. Zoals in paragraaf 3.1 beschreven vraagt het auditen van IT om expertise van auditors (Ahmed et al., 2025; Hulshof en Daneva, 2021, p. 165). Aan deze expertise wordt ook gewerkt vanuit het digitaal decennium, een beleidsprogramma vanuit Europa (Europese Commissie, 2025). Eén van de vier hoofddoelstellingen is om per 2030 over 20 miljoen meer hoogopgeleide digitale professionals te beschikken om onder andere te kunnen bouwen aan een veilige digitale wereld en ervoor te zorgen dat organisaties cyberbeveiligingsmaatregelen nemen. Goed opgeleide professionals bieden daarbij twee oplossingen: enerzijds voor een betere beveiliging bij organisaties en hun toeleveranciers, anderzijds het beter kunnen auditen van normenkaders waardoor deze als betrouwbaarder kunnen worden gezien. Het controleren daarop blijft echter van belang.

Wetgeving en normenkaders. Voor informatiebeveiliging bestaan er diverse wetten en normenkaders om organisaties te helpen aan wetgeving te voldoen (bijvoorbeeld AVG, NIS2-richtlijn en ISO-standaarden). Specifiek voor informatiebeveiliging in de toeleveringsketen verwijst ENISA (EU-Agentschap voor cyberbeveiliging; 2023, pp. 21-22) naar de ISO 31000. Dit is een norm voor risicomanagement. Ook in een studie van Seid et al. (2025) is gekeken naar normenkaders zoals de ISO, NIST en NIS2-richtlijn als hulpmiddel bij het invullen van cyberrisico's bij derde partijen. Eén van de bevindingen uit het onderzoek van Seid et al. (2025) is dat bovenstaande normenkaders positief bijdragen aan het beperken van risico's in de toeleveringsketen, maar dat de toepassing ervan in de praktijk vaak lastig blijkt. Gezien het (steeds groter wordende) belang van informatiebeveiliging in de toeleveringsketen lijkt er een voor de hand liggende keuze: het ontwerpen van een richtlijn op basis van best-practices die organisaties helpt om digitale risico's in de toeleveringsketen te mitigeren.

Herstel van vertrouwen als onderdeel van incidentrespons. Gezien de impact op vertrouwen als gevolg van een datalek in de zorg is het belangrijk om eveneens

aandacht te hebben voor het herstellen van dit vertrouwen. In een door een Bevolkingsonderzoek zelf uitgevoerd onderzoek (*Kamerstukken II*, 32761, nr. 334, 2026) wordt genoemd dat vertrouwen kan worden hersteld door (1) betere en strengere informatiebeveiliging, (2) transparantie en heldere communicatie over wat er fout ging en wat er nu anders gaat en (3) gegevens te anonimiseren en minder lang te bewaren.

Bovenstaande geeft een eerste indicatie hoe vertrouwen hersteld kan worden. Dit onderzoek heeft zich echter niet beziggehouden met het herstellen van vertrouwen na een datalek in de zorgsector. Aanvullend onderzoek is nodig naar manieren om vertrouwen na een datalek in de zorgsector te herstellen.

5. Kritische beschouwing

In deze kritische beschouwing zal de casus van Bevolkingsonderzoek verder centraal staan. Dit omdat het datalek bij Bevolkingsonderzoek bijzonder is te noemen vanwege de schaal waarop medische gegevens zijn gelect en om de publieke samenwerking waarbij verschillende overheidsinstanties betrokken zijn. Voor de leesbaarheid van de kritische beschouwing wordt er eerst stilgestaan bij de definiëring van centrale begrippen.

Definiëring. Nederland is volgens het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK; 2024, p. 20) een democratische rechtsstaat. Dit vormt het fundament voor de Nederlandse samenleving. Onder de begrippen democratie, rechtsstaat en democratische rechtsstaat wordt verstaan:

1. Democratie is een staatsvorm waarbij het mandaat voor de macht bij het volk ligt (BZK, 2024, p. 20).
2. Een rechtsstaat is een staat die gegrond is in en gebonden aan het recht (Van den Berg, 2024). Een rechtsstaat kenmerkt zich door de aanvaarding van grondrechten, de scheiding der machten, de gebondenheid van de overheid aan het recht en de onafhankelijke rechtspraak (BZK, 2024, p. 20; Van den Berg, 2024; Witteveen et al., 2002, p. 9).
3. Democratische rechtsstaat is een combinatie van bovenstaande: 1) de bron van macht ligt bij de burgers én 2) de overheid is gebonden aan het recht (BZK, 2024, p. 20).

Nederland is daarnaast ook een verzorgingsstaat, waarin de overheid (semi-)collectieve regelingen op onder andere de gezondheidszorg organiseert (Wetenschappelijke raad voor het regeringsbeleid, 2006, pp. 23-24). Deze taakstellingen, zoals Kortmann (1994, p. 366) dit verwoordt, zijn opgenomen in de *Grondwet* (2023, Artikelen 19-23) als sociale grondrechten en kunnen worden gezien als onderdeel van de sociale rechtsstaat (Van de Sande, 2019). Nederland kent daarbij niet alleen klassieke grondrechten, maar ook sociale grondrechten.

Spanningsveld en de invloed van het datalek daarop. De samenwerking rond bevolkingsonderzoeken vindt haar vertrekpunt in de *Grondwet* (2023, Artikel 22, lid 1). Daarin krijgt de overheid de taak om maatregelen te treffen ter bevordering van

de volksgezondheid. Kortmann (1994) noemt dat ondanks het feit dat sociale grondrechten een taak opleggen aan de overheid, deze taak altijd onder het voorbehoud van klassieke grondrechten uitgevoerd dient te worden; zoals het klassieke grondrecht op de privacy uit artikel 10, lid 2 en 3.

Het ontvangen van zorg is (bijna) inherent aan het moeten inleveren op de eigen privacy, in casu de informationele privacy. Als gevolg van het datalek komt het reeds bestaande spanningsveld tussen de publieke waarden van privacy en goede zorg sterker naar voren en onder grotere spanning terecht. Een datalek kan het verschil maken in de risico-overweging van de patiënt om bijvoorbeeld benodigde zorg te gaan mijden of essentiële informatie achter te houden wat de gezondheid van de patiënt direct kan raken.

Vertrouwen. In paragraaf 3.2 is te lezen wat de impact van een datalek kan zijn op het vertrouwen van patiënten. Dit blijft niet beperkt tot het eventueel niet meer willen deelnemen aan de bevolkingsonderzoeken, maar kan voor degenen die wel deelnemen ook betekenen dat ze vanuit wantrouwen essentiële (medische) informatie achterhouden. Juist omdat meerdere overheidsinstanties betrokken zijn, mag worden verwacht dat verantwoordelijkheden in de keten duidelijk zijn belegd en dat naleving van normenkaders aantoonbaar wordt gecontroleerd. Het IGJ-rapport roept hieromtrent vragen op, omdat Clinical Diagnostics ten tijde van het incident niet voldeed aan NEN 7510 en niet beschikte over een CISO (Inspectie Gezondheidszorg en Jeugd, 2026, p. 4).

Literatuurlijst

Agaku, I. T., Odisa, A. O., Ayo-Yusuf, O. A., & Conolly, G. N. (2013). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association*, 21(2), 374-378. [doi:10.1136/amiajnl-2013-002079](https://doi.org/10.1136/amiajnl-2013-002079)

Ahmed, A., Shahzad, A., Naseem, A., Ali, S., & Ahmad, I. (2025). Evaluating the effectiveness of data governance frameworks in ensuring security and privacy of healthcare data: A quantitative analysis of ISO standards, GDPR, and HIPAA in blockchain technology. *PLoS One*, 20(5). <https://doi.org/10.1371/journal.pone.0324285>

Algemene verordening gegevensbescherming (AVG). (2016, 4 mei). EUR-Lex. Geraadpleegd op 4 juni 2026, van <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=nl>

Bevolkingsonderzoek Nederland. (2025a, 12 augustus). *Datalek persoonsgegevens deelnemers bevolkingsonderzoek baarmoederhalskanker*. https://www.bevolkingsonderzoeknederland.nl/media/nqkh2hr1/20250811_conceptbrief-cli%C3%ABnten-incident-bmhk_def.pdf

Bevolkingsonderzoek Nederland. (2025b, 29 augustus). *Datalek veel groter dan eerder vermeld*. <https://www.bevolkingsonderzoeknederland.nl/nieuws/datalek-veel-groter-dan-eerder-vermeld/>

Bos, I., & Verheij, R. (2024). *Literatuurscan naar vertrouwen in uitwisseling en hergebruik van gezondheidsgegevens onder burgers en zorgprofessionals*. <https://www.nivel.nl/sites/default/files/bestanden/1004548.pdf>

Choi, S. J., Johnson, M. E., & Lehmann, C. U. (2019). Data breach remediation efforts and their implications for hospital quality. *Health Services research*, 54(5), 971-980. [doi: 10.1111/1475-6773.13203](https://doi.org/10.1111/1475-6773.13203)

Clements, T., & Milton, S. (2018). *Maintaining Data Protection and Privacy Beyond GDPR Implementation* [Whitepaper]. ISACA. https://www.isaca.org/-/media/files/isacadp/feature/downloads/m/maintaining-data-protection-and-privacy-beyond-gdpr-implementation_res_eng_0218.pdf

Clinical Diagnostics Nederland. (z.d.). *Onderzoek via Bevolkingsonderzoek Nederland*. <https://clinicaldiagnostics.nl/nl/onderzoek-via-bevolkingsonderzoek-nederland/>

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48-52. <https://doi.org/10.1016/j.maturitas.2018.04.008>

Erasmus University Rotterdam (2025, 11 september). *Massaclaims na datalek bevolkingsonderzoek, samen sterk door de WAMCA?*. <https://www.eur.nl/nieuws/massaclaims-na-datalek-bevolkingsonderzoek-samen-sterk-door-de-wamca>

Esmailzadeh, P., & Sambasivan, M. (2017). Patients' support for health information exchange: a literature review and classification of key factors. *BMC Medical Informatics and Decision Making*, 17(33). <https://doi.org/10.1186/s12911-017-0436-2>

ENISA. (2023). *Good practices for supply chain cybersecurity*. [doi:10.2824/805268](https://doi.org/10.2824/805268)

Europese Commissie. (2025, 17 juni). *Digitaal decennium – Beleidsprogramma*. <https://digital-strategy.ec.europa.eu/nl/policies/digital-decade-policy-programme>

Europese Commissie. (2026, 20 januari). *NIS2-richtlijn: beveiliging van netwerk- en informatiesystemen*. <https://digital-strategy.ec.europa.eu/nl/policies/nis2-directive>

Fernando, Y., Tseng, M. L., Wahyuni-Td, I. S., de Sousa Jabbour, A. B. L., Chiappetta Jabbour, C. J., & Foropon, C. (2023). Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia. *Journal of Industrial & Production Engineering*, 40(2), 102–116. <https://doi.org/10.1080/21681015.2022.2116495>

Grondwet. (2023, 22 februari). Overheid.nl. <https://wetten.overheid.nl/BWBR0001840/2023-02-22/0>

Hulshof, M., Daneva, M. (2021). Benefits and challenges in information security certification – A systematic literature review. *Business Modeling and Software Design*, 422, 154-169. https://doi.org/10.1007/978-3-030-79976-2_9

Inspectie Gezondheidszorg en Jeugd. (2026, 13 mei). *Clinical Diagnostics NMDL B.V. en LCPL B.V. Rijswijk december 2025; Incidententoezicht*. <https://toezichtdocumenten.igj.nl/link/publicatie?publ=01df6ff4-53d9-4a74-a474-aca3b8f531db>

Kamerstukken II, 32761, nr. 327. (2025, 11 augustus). Overheid.nl. Geraadpleegd op 28 mei 2026, van <https://zoek.officielebekendmakingen.nl/kst-32761-327.html>

Kamerstukken II, 32761, nr. 334. (2026, 9 februari). Overheid.nl. Geraadpleegd op 28 mei 2026, van <https://zoek.officielebekendmakingen.nl/kst-32761-334.html>

Kortmann, C. A. J. M. (1994). Grondwetsinterpretatie. *Rechtsgeleerd Magazijn Themis*, 8, 363-370. <https://bib.kuleuven.be/rbib/collectie/archieven/rmt/1994-8.pdf>

Latsiou, A., & Lambrinoudakis, C. (2026). Cyber supply chain risk management: From threats to treatment. *International Journal of Information Security*, 25(40). <https://doi.org/10.1007/s10207-025-01207-9>

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90. <https://doi.org/10.2307/20650279>

Lopes, I. M., Guarda, T. and Oliveira, P. (2019). Implementation of ISO 27001 standards as

GDPR compliance facilitator. *Journal of Information Systems Engineering & Management*, 4(2). <https://doi.org/10.29333/jisem/5888>

Lott, B. E., Campos-Castillo, C., & Anthony, D. (2020). Trust and privacy: How patient trust in providers is related to privacy behaviors and attitudes. *MIA Annual Symposium Proceedings*, 487–493. <https://pmc.ncbi.nlm.nih.gov/articles/PMC7153104/>

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2024). *Staat van het Bestuur*; 2024. <https://www.kennisopenbaarbestuur.nl/site/binaries/site-content/collections/documents/2025/03/17/staat-van-het-bestuur-2024/bzk-brochure-staat-van-bestuur-2024.pdf>

NIS 2-richtlijn. (2022, 27 december). EUR-Lex. <https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555>

NOS. (2025, 29 augustus). *Datalek bevolkingsonderzoek blijkt nog groter: zeker 700.000 vrouwen getroffen*. <https://nos.nl/artikel/2580325-datalek-bevolkingsonderzoek-blijkt-nog-groter-zeker-700-000-vrouwen-getroffen>

NOS. (2026a, 7 april). *Bedrijf dat software levert voor patiëntendossiers aangevallen door hackers*. <https://nos.nl/artikel/2609548-bedrijf-dat-software-levert-voor-patientendossiers-aangevallen-door-hackers>

NOS. (2026b, 17 februari). *OM: 118 aangiften na datalek bij laboratorium achter bevolkingsonderzoek*. <https://nos.nl/artikel/2602822-om-118-aangiften-na-datalek-bij-laboratorium-achter-bevolkingsonderzoek>

Nu.nl. (2025, 27 augustus). *Al bijna 70.000 aanmeldingen voor massaclaim na lek bij bevolkingsonderzoek*. <https://www.nu.nl/binnenland/6366955/al-bijna-70000-aanmeldingen-voor-massaclaim-na-lek-bij-bevolkingsonderzoek.html>

OpenAI. (2026). *ChatGPT (Versie 5.5) [Generatieve AI]*. <https://chatgpt.com>

Park, E., & Lim, J. H. (2025). The impact of healthcare data breaches on patient hospital visit behaviour. *International Journal of Research in Marketing*, 42(4), 1285-1304. <https://doi.org/10.1016/j.ijresmar.2025.01.004>

Pool, J., Akhlaghpour, S., Fatehi, F., & Burton-Jones, A. (2024). A systematic analysis of failures in protecting personal health data: A scoping review. *International Journal of Information Management*, 74. <https://doi.org/10.1016/j.ijinfomgt.2023.102719>

RIVM. (2025, 27 november). *Wisselend beeld deelname bevolkingsonderzoeken naar kanker*. <https://www.rivm.nl/nieuws/wisselend-beeld-deelname-bevolkingsonderzoeken-naar-kanker>

Seid, E., Ilter, D., Blix, F., & Popov, O. (2025). Cyber supply chain resilience: Analyzing ISO, NIST, and NIS2 frameworks for mitigating third-party risks. *Procedia Computer Science*, 263, 591-599. <https://doi.org/10.1016/j.procs.2025.07.071>

Schmidt, A., Albert, L. A., & Zheng, K. (2021). Risk management for cyber-infrastructure protection: A bi-objective integer programming approach. *Reliability Engineering & System Safety*, 205. <https://doi.org/10.1016/j.ress.2020.107093>

Van den berg, J. Th. T. (2024). Sociale rechtsstaat en economische risicogemeenschap. In M. A. V. Klein-Meijer, B. A. M. Van Stokkom, & P. B. A. Ter Veer (Reds.). *Sociale grondrechten na de verzorgingsstaat* (pp. 8-18). WODC en Uitgeverij Gouda Quint BV. https://repository.wodc.nl/bitstream/handle/20.500.12832/642/jv9802-volledige-tekst_tcm28-76512.pdf?sequence=2&isAllowed=y

Van de Sande, S. A. L. (2019). *Overheidsaansprakelijkheid voor het verstrekken van onjuiste informatie*. https://www.inview.nl/document/ida8d731375742409693d1af19e3130310/overheidsaansprakelijkheid-voor-het-verstrekken-van-onjuiste-informatie-staat-en-recht-nr-45-1-inleiding?ctx=WKNL_CSL_2727&tab=tekst

Van Wegberg, R. (2026, 5 maart). *Oeps.. uw persoonsgegevens zijn gehackt* [Gastcollege]. Studium Generale Saxion, Apeldoorn.

Vrije Universiteit Amsterdam. (2024, 10 december). *Pre-University College – Bètapartners: Websites beoordelen*. Geraadpleegd op 4 april 2026, van <https://libguides.vu.nl/c.php?g=566702&p=3903180>

Wetenschappelijke raad voor het regeringsbeleid. (2006). *De verzorgingsstaat herwogen. Over verzorgen, verzekeren, verheffen en verbinden*. Amsterdam University Press. <https://www.wrr.nl/site/binaries/site-content/collections/documents/2006/10/05/de-verzorgingsstaat-herwogen/R076-Verzorgingsstaat-herwogen.pdf>

Wirken, G. P. J. W. F. (2012). *Information security in Dutch hospitals* [Master thesis]. Utrecht University.

Witteveen, W., Van Klink, B., De Been, W., & Blok, P. (2002). *De sociale rechtsstaat voorbij. Twee ontwerpen voor het huis van de rechtsstaat*. Sdu Uitgevers.

Z-CERT. (2023). *Cybersecurity Dreigingsbeeld Zorg; 2022*. https://z-cert.nl/assets/downloads/Z-CERT_RapportDreigingsbeeld2022.pdf

Z-CERT. (2024a). *Cybersecurity Dreigingsbeeld voor de zorg; 2023*. https://z-cert.nl/assets/downloads/DEF-Z-CERT_RapportDreigingsbeeld2023-2.pdf

Z-CERT. (2024b, 29 januari). *Whitepaper Leveranciersmanagement*. <https://z-cert.nl/assets/downloads/Leveranciersmanagement-whitepaper.pdf>

Z-CERT. (2025). *Cybersecurity Dreigingsbeeld voor de zorg; 2024*. https://z-cert.nl/assets/uploads/Actueel/DEF_Z-CERT_CyberDreigingsbeeldvoordezorg-LR.pdf

Z-CERT. (2026). *Cybersecuritybeeld Zorg; 2025*. https://z-cert.nl/assets/uploads/Actueel/Z-CERT_Cybersecuritybeeld-Zorg-2025.pdf

Cyberdreigingen rondom satellieten en ruimtevaart

Jelmer Brouwer

Minor Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool

1. Inleiding

De ruimtevaartsector is de afgelopen jaren sterk veranderd. Waar ruimtevaart vroeger vooral werd uitgevoerd door nationale overheden en grote internationale organisaties, spelen commerciële bedrijven tegenwoordig een steeds grotere rol. Deze ontwikkeling staat bekend als New Space. Bedrijven zoals SpaceX, OneWeb en Amazon investeren op grote schaal in satellietconstellaties die digitale diensten mogelijk maken, zoals communicatie, navigatie en internettoegang. Deze satellieten worden niet alleen gebruikt voor commerciële doeleinden, maar zijn ook van groot belang voor overheden, bedrijven en burgers. (Manulis et al., 2020; ENISA, 2025).

Door deze ontwikkelingen is de samenleving steeds afhankelijker geworden van satellietsystemen. Satellieten vormen inmiddels een essentieel onderdeel van de digitale infrastructuur waarop vitale processen steunen, zoals lucht- en scheepvaart, noodcommunicatie, financiële systemen en defensie. Tegelijkertijd zijn deze systemen sterk gedigitaliseerd en verbonden met netwerken op aarde, waardoor ze kwetsbaar zijn voor cyberdreigingen (Peled et al., 2023). Cyberaanvallen op satellietsystemen kunnen leiden tot verstoringen met grote maatschappelijke, economische en geopolitieke gevolgen.

De toenemende commercialisering van satellietsystemen roept daarom vragen op over digitale weerbaarheid. Commerciële partijen opereren vaak in een internationale en competitieve markt, waarin kostenbesparing en snelle innovatie centraal staan. Dit kan spanning opleveren met het garanderen van cybersecurity en sterke beveiligingsmaatregelen (Abdrabou et al., 2024).

Dit onderzoeksartikel richt zich op de vraag hoe de toenemende afhankelijkheid van commerciële satellietsystemen nieuwe kwetsbaarheden creëert op het gebied van digitale weerbaarheid. Aan de hand van wetenschappelijke literatuur en praktijkvoorbeelden wordt onderzocht welke beveiligingsmaatregelen nodig zijn om deze risico's te verminderen.

2. New Space en digitale afhankelijkheid

De term New Space verwijst naar een nieuwe manier van werken binnen de ruimtevaartsector. Waar traditionele ruimtevaartprogramma's vaak langdurig, kostbaar en sterk gereguleerd waren, ligt binnen New Space de nadruk op commerciële innovatie, kostenreductie en snelle ontwikkeling (Manulis et al., 2020). Satellieten worden steeds vaker ontworpen en gebouwd met kortere ontwikkelcycli en met behulp van commerciële standaardcomponenten. Dit maakt ruimtevaart

toegankelijker voor private bedrijven, maar heeft ook geleid tot een sterke toename van het aantal satellieten, met name in een lage baan om de aarde.

Deze ontwikkeling heeft grote gevolgen voor de digitale afhankelijkheid van de samenleving. Satellietsystemen vervullen een essentiële rol in moderne samenlevingen en ondersteunen uiteenlopende digitale diensten. Denk hierbij aan wereldwijde communicatie, navigatiesystemen zoals GPS-navigatie en internettoegang in afgelegen of slecht bereikbare gebieden. Overheden, bedrijven en burgers maken dagelijks gebruik van deze diensten, vaak zonder zich bewust te zijn van de onderliggende satellietinfrastructuur. Door deze toenemende afhankelijkheid neemt ook de impact van mogelijke verstoringen toe. Een cyberincident binnen een satellietsysteem kan daardoor gevolgen hebben die verder reiken dan de ruimtevaartsector alleen.

Mijn eigen kijk hierop is dat hoewel het idee van snellere innovatie aantrekkelijk klinkt, snelheid vaak boven veiligheid kan gaan. Als bedrijven te veel focussen op kosten en tempo, kunnen kritieke kwetsbaarheden onopgemerkt blijven. Dit laat zien waarom cybersecurity vanaf het begin in het ontwerp van satellieten geïntegreerd moet worden en niet pas achteraf.

3. Cyberdreigingen binnen commerciële satellietsystemen

Commerciële satellietsystemen worden blootgesteld aan verschillende vormen van cyberdreigingen. Een belangrijke kwetsbaarheid bevindt zich in het grondsegment, zoals grondstations en controlecentra. Deze systemen zijn vaak verbonden met gewone IT-netwerken en Cloud omgevingen (Peled et al., 2023), waardoor zij vergelijkbare risico's kennen als andere digitale infrastructuren. Een cyberaanval op deze systemen kan leiden tot verlies van controle over satellieten of tot verstoring van communicatiediensten.

Naast aanvallen op grondstations vormen ook specifieke satelliet gerelateerde dreigingen een risico. GPS-spoofing en jamming zijn hier bekende voorbeelden van. Bij spoofing worden valse navigatiesignalen uitgezonden, waardoor ontvangers verkeerde positie- of tijdsinformatie krijgen. Jamming richt zich op het verstoren of blokkeren van signalen, waardoor diensten tijdelijk onbruikbaar worden. Daarnaast vormen supply chain-aanvallen een groeiend probleem. Hardware- en softwarecomponenten voor satellieten worden wereldwijd ontwikkeld en geïntegreerd, wat het lastig maakt om volledige controle te houden over de beveiliging van alle onderdelen (ENISA, 2025).

4. Praktijkvoorbeelden

De uitdagingen van digitale weerbaarheid in commerciële satellietsystemen worden duidelijk zichtbaar in recente incidenten en ontwikkelingen binnen het veld. Grootschalige netwerken en het gebruik van commerciële constellaties vergroten het aanvalsoppervlak, waardoor verstoringen snel grensoverschrijdende gevolgen kunnen hebben. Twee voorbeelden illustreren deze kwetsbaarheden: de cyberaanval

op Viasat in 2022 en de snelle uitbreiding van het Starlink-netwerk. Deze gevallen laten zien hoe technische, operationele en maatschappelijke aspecten samenkomen en waarom monitoring, detectie en risicobeheer cruciaal zijn.

Een duidelijk voorbeeld van de kwetsbaarheid van commerciële satellietssystemen is de cyberaanval op satellietoperator Viasat in 2022. Tijdens deze aanval werd het KA-SAT netwerk getroffen, waardoor tienduizenden vaste satellietmodems in Oekraïne en delen van Europa tijdelijk geen verbinding konden maken met het netwerk (KA-SAT Network Cyber Attack Overview, 2022). Dit leidde tot grootschalige verstoring van internetdiensten, met directe gevolgen voor zowel burgerlijke als militaire communicatie. Volgens Viasat zelf vond de aanval plaats via een misconfiguratie in een VPN-apparaat op het grondnetwerk, waardoor aanvallers toegang kregen tot het managementsysteem, zonder dat de satelliet hardware zelf werd beschadigd.

Het incident laat duidelijk zien dat de commerciële satellietdiensten strategische doelen kunnen vormen binnen geopolitieke conflicten en dat de impact van dergelijke aanvallen grensoverschrijdend kan zijn, omdat digitale diensten in meerdere landen tegelijkertijd werden verstoord. Daarnaast laat het zien hoe snel de gevolgen van een aanval zich kunnen verspreiden in een wereldwijd netwerk en benadrukt het dat een enkel incident niet alleen technische maar ook maatschappelijke en economische effecten kan hebben.

Daarnaast toont de snelle uitbreiding van satellietnetwerken zoals Starlink hoe schaalvergroting nieuwe uitdagingen met zich meebrengt. In het afgelopen jaar heeft Starlink meer dan 2.300 extra satellieten aan zijn constellatie toegevoegd en is het netwerk uitgebreid naar tientallen nieuwe landen, met miljoenen actieve klanten wereldwijd (Starlink Network Update, 2025). Het inzetten van duizenden satellieten vergroot het aanvalsoppervlak enorm. Het beveiligen van deze systemen vraagt om continue monitoring, snelle detectie van incidenten en een hoge mate van automatisering om juist te kunnen reageren op nieuwe dreigingen.

5. Beveiligingsmaatregelen en strategieën

De praktijkvoorbeelden van Viasat en Starlink laten zien dat commerciële satellietssystemen kwetsbaar zijn voor zowel cyberaanvallen als operationele risico's door schaalvergroting. Om deze risico's te beperken zijn er verschillende maatregelen en strategieën mogelijk.

Continue monitoring en incidentdetectie is erg belangrijk voor grootschalige satellietnetwerken zoals Starlink. Geautomatiseerde systemen kunnen afwijkingen in satelliet- en grondstationgedrag onmiddellijk detecteren, zodat aanvallen of storingen sneller worden opgemerkt en beperkt (ENISA, 2025). Hierbij worden vaak intrusion detection systems (IDS) ingezet die netwerkverkeer analyseren en verdachte activiteiten direct melden. Persoonlijk denk ik dat geautomatiseerde systemen cruciaal zijn, omdat mensen simpelweg de hoeveelheid data en de snelheid van incidenten niet bij kunnen houden.

Een andere belangrijke maatregel is supply-chain-beveiliging. Veel onderdelen van satellieten en grondstations worden wereldwijd ontwikkeld en geïntegreerd, wat risico's introduceert. Door leveranciers regelmatig te controleren, software op een veilige manier te ontwikkelen en blockchain te gebruiken om de supply chain te volgen, kunnen kwetsbaarheden in de keten beter worden opgespoord en beperkt (Abdrabou et al., 2024; Peled et al., 2023).

Daarnaast spelen redundantie en veerkracht van systemen een grote rol. Door het inzetten van redundante satellieten, back-ups van grondstations en alternatieve communicatieroutes kunnen diensten sneller worden hersteld bij incidenten (Joyce, 2025). Ook end-to-end encryptie van communicatiedata wordt toegepast om te voorkomen dat gevoelige informatie tijdens een aanval kan worden onderschept of gemanipuleerd.

Naast technische maatregelen is ook samenwerking tussen landen en organisaties steeds belangrijker geworden. Satellietoperators vallen wel onder nationale wet- en regelgeving, maar omdat satellietnetwerken grensoverschrijdend werken, is er behoefte aan gezamenlijke afspraken over cybersecurity. Binnen de Europese Unie is hierop ingespeeld met de EU Space Strategy for Security and Defence, die in 2023 is aangenomen.

Als onderdeel van deze strategie is in 2024 het EU Space Information Sharing and Analysis Centre (EU Space ISAC) opgericht. Dit platform is bedoeld om samenwerking en informatie-uitwisseling tussen overheden, satellietoperators en andere betrokken partijen te verbeteren. Door dreigingsinformatie en ervaringen te delen, kunnen cyberincidenten sneller worden herkend en kan er effectiever worden gereageerd. (ENISA, 2025).

6. Conclusie en aanbevelingen

De opkomst van New Space en de groei van commerciële satellietnetwerken hebben de ruimtevaart sterk veranderd. Satellieten zijn belangrijk voor communicatie, navigatie en internet, maar deze afhankelijkheid brengt ook nieuwe risico's. Cyberaanvallen op commerciële netwerken kunnen grote gevolgen hebben voor de samenleving, economie en veiligheid.

Voorbeelden zoals de aanval op Viasat en de snelle uitbreiding van Starlink laten dit duidelijk zien. Bij Viasat werd het netwerk tijdelijk uitgeschakeld door een aanval op het grondstation, terwijl Starlink laat zien dat hoe groter een netwerk wordt, hoe kwetsbaarder het kan zijn. Deze voorbeelden tonen dat cybersecurity een belangrijk onderdeel is van betrouwbare satellietdiensten.

Om de digitale weerbaarheid te verbeteren, zijn zowel technische als organisatorische maatregelen nodig. Automatische monitoring en detectie van incidenten, veilige software en onderdelen, redundantie en encryptie helpen om aanvallen sneller te stoppen en de impact te verkleinen. Ook samenwerking tussen landen en bedrijven is essentieel. In Europa zorgen initiatieven zoals de EU Space

Strategy for Security and Defence en het EU Space ISAC dat informatie gedeeld wordt en dat iedereen beter voorbereid is op cyberdreigingen.

Ten slotte blijft de spanning tussen snelle innovatie en veiligheid een aandachtspunt. Snelheid en kostenbesparing zijn aantrekkelijk, maar mogen niet ten koste gaan van veiligheid. Cybersecurity moet vanaf het begin worden meegenomen in het ontwerp en beheer van satellietsystemen. Door samenwerking, slimme technologie en bewustwording te combineren, kunnen we satellietsystemen veiliger maken en zorgen dat de diensten waarop we allemaal vertrouwen betrouwbaar blijven zowel vandaag als in de toekomst.

Literatuurlijst

Abdrabou, M., Gebali, F., Shawky, M. A., Alluhaidan, A. S., Mansour, A. E., El-Rahman, S. A., Al-Ahwal, A., & Shamseldin, T. (2024). Advanced security framework for low Earth orbit satellites in space information network. EURASIP Journal On Wireless Communications And Networking, 2024(1). <https://doi.org/10.1186/s13638-024-02417-w>

From Cyber to Outer Space: A Guide to Securing Commercial Satellite Operations | ENISA. (2025, 6 november). <https://www.enisa.europa.eu/news/from-cyber-to-outer-space-a-guide-to-securing-commercial-satellite-operations>

Institute of Positioning, Navigation, and Timing. (2025, 17 september). Efforts against Cybersecurity Attack of Space Systems. <https://www.jpnt.org/efforts-against-cybersecurity-attack-of-space-systems/>

Joyce, S. (2025, 13 oktober). Satellite cybersecurity: Safeguarding the final frontier. PwC. <https://www.pwc.com/gx/en/issues/cybersecurity/satellite-cybersecurity.html>

KA-SAT Network cyber attack overview. (2022, 30 maart). Viasat.com. <https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/>

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2020). Cyber security in New Space. International Journal Of Information Security, 20(3), 287–311. <https://doi.org/10.1007/s10207-020-00503-w>

Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023, 3 december). Evaluating the Security of Satellite Systems. arXiv.org. <https://arxiv.org/abs/2312.01330>

Starlink-Netwerupdate. (2025, 14 juli). Starlink. <https://starlink.com/updates/network-update>

Cyberbewustzijn en cyberweerbaarheid als fundament voor veilig hoger onderwijs

George Abboud

Bedrijfskunde (jaar 3), Avans Hogeschool

1. Inleiding

De digitale wereld binnen het hoger onderwijs is de afgelopen jaren sterk gegroeid. Studeren, communiceren, samenwerken, toetsen en informatie delen verlopen steeds vaker via digitale systemen. Studenten gebruiken dagelijks online leeromgevingen, e-mail, cloudopslag, roosterapps, digitale toetsplatforms en in toenemende mate AI-tools. Deze ontwikkeling maakt het onderwijs sneller, flexibeler en toegankelijker, maar vergroot tegelijkertijd de afhankelijkheid van technologie.

Door deze digitalisering nemen ook digitale risico's toe. Studenten kunnen te maken krijgen met phishing, accountmisbruik, datalekken, nepberichten, onveilige links, identiteitsfraude en onzorgvuldig gebruik van persoonsgegevens. Cyberveiligheid is daarom niet alleen een technisch vraagstuk voor ICT-afdelingen, maar ook een gedrag en organisatievraagstuk waarin studenten een belangrijke rol spelen.

Het versterken van cyberweerbaarheid en cyberbewustzijn van studenten is om die reden essentieel. Cyberbewustzijn betekent dat studenten digitale risico's herkennen en begrijpen. Cyberweerbaarheid gaat een stap verder: studenten moeten ook veilig, kritisch en verantwoordelijk kunnen handelen. Een student die weet dat phishing bestaat, is nog niet automatisch cyberweerbaar. Pas wanneer die student verdachte signalen serieus neemt, de juiste vervolgstap kent en veilig gedrag vertoont, ontstaat daadwerkelijke weerbaarheid.

Centrale vraag: Wat is het belang van het versterken van cyberweerbaarheid en cyberbewustzijn van studenten in het hoger onderwijs?

Dit artikel betoogt dat het versterken van cyberweerbaarheid en cyberbewustzijn noodzakelijk is omdat studenten steeds intensiever digitaal werken, terwijl veilig digitaal gedrag niet vanzelf ontstaat. Cyberweerbaarheid vraagt om samenhang tussen mens, proces, technologie en organisatiecultuur.

De mens bepaalt of risico's worden herkend en serieus genomen. Processen bepalen of studenten weten welke stappen zij moeten zetten. Technologie moet veilig gedrag ondersteunen. De organisatiecultuur bepaalt of cyberveilig gedrag normaal, haalbaar en bespreekbaar wordt.

2. Literatuuronderzoek

2.1 Cyberweerbaarheid als breed vraagstuk

Cyberweerbaarheid is breder dan cybersecurity. Cybersecurity richt zich vooral op het beschermen van systemen, het voorkomen van digitale aanvallen en het beperken van technische kwetsbaarheden. Cyberweerbaarheid gaat verder: het gaat om het

vermogen om voorbereid te zijn, adequaat te reageren, te herstellen en te leren van digitale risico's en verstoringen.

Van der Kleij (2025) beschrijft cyberweerbaarheid als een samenhangend vermogen waarin voorbereiden, reageren, aanpassen en herstellen centraal staan. Daarbij benadrukt hij dat cyberweerbaarheid niet alleen technisch is, maar juist ontstaat door de samenhang tussen mensen, processen en technologie.

Voor het hoger onderwijs betekent dit dat cyberweerbaarheid niet uitsluitend afhankelijk is van firewalls, wachtwoordbeleid of technische beveiliging. Studenten moeten ook weten hoe zij veilig moeten handelen. Onderwijsinstellingen kunnen beschikken over sterke technische beveiliging, maar blijven kwetsbaar wanneer studenten risico's onderschatten, verdachte situaties niet herkennen of niet weten welke actie nodig is. Cyberweerbaarheid is daarmee geen losse ICT-maatregel, maar een breed veiligheidsvraagstuk waarin studentgedrag centraal staat.

2.2 Cyberbewustzijn en securitygedrag van studenten

Studenten worden vaak gezien als digitaal vaardig, omdat zij dagelijks technologie gebruiken. Toch betekent intensief digitaal gebruik niet automatisch dat studenten ook cyberveilig handelen. Cyberbewustzijn en securitygedrag zijn daarom belangrijke onderdelen van cyberweerbaarheid.

Gwenhure (2025) laat zien dat technische maatregelen alleen onvoldoende zijn, omdat cyber risico's vaak samenhangen met menselijke kwetsbaarheden, zoals onoplettendheid, gemakzucht, overschatting van eigen kunnen en het omzeilen van veiligheidsregels. Studenten gebruiken veel digitale communicatiekanalen, maar beschikken niet altijd over voldoende formele cybersecuritytraining. Daardoor kan er een verschil ontstaan tussen wat studenten denken te kunnen en hoe veilig zij daadwerkelijk handelen.

Ook gegevens van het Centraal Bureau voor de Statistiek laten zien dat digitale ervaring niet automatisch leidt tot cyberveilig gedrag. Jongeren gebruiken veel digitale communicatiemiddelen, maar nemen beveiligingsmaatregelen niet altijd consequent. Zo installeren zij updates niet altijd direct en controleren zij links minder vaak vooraf dan oudere groepen (Centraal Bureau voor de Statistiek [CBS], 2025b).

Het belang van cyberbewustzijn ligt dus niet alleen in kennis, maar vooral in gedrag. Studenten moeten risico's herkennen en begrijpen waarom hun eigen handelen ertoe doet. Zij moeten niet alleen weten wat phishing is, maar ook wanneer zij kritisch moeten zijn, welke signalen belangrijk zijn en welke vervolgstap nodig is.

2.3 Cyberbewustzijn in het hbo

De sectorrapportage van SURF laat zien dat het cyberbewustzijn in het hoger onderwijs nog niet op het gewenste niveau ligt. Volgens SURF (2023) heeft het hbo een redelijke basis op het gebied van security- en privacybewustzijn, maar ligt het niveau nog onder het gewenste streefniveau. Er is dus bewustzijn aanwezig, maar deze basis is nog onvoldoende om structureel veilig digitaal gedrag te garanderen.

Dit is relevant omdat studenten steeds meer digitale handelingen uitvoeren binnen hun studie. Zij loggen in op verschillende platforms, delen bestanden, gebruiken externe tools en ontvangen veel digitale berichten. Wanneer cyberbewustzijn achterblijft bij digitaal gebruik, ontstaat een kwetsbare situatie.

Cyberbewustzijn moet daarom niet worden gezien als eindpunt, maar als voorwaarde voor cyberweerbaarheid. Bewustzijn betekent dat studenten weten dat digitale risico's bestaan. Cyberweerbaarheid betekent dat zij vervolgens ook veilig handelen. De stap van weten naar doen is bepalend voor de digitale veiligheid van studenten en onderwijsinstellingen.

2.4 Communicatie en handelingsperspectief

Het versterken van cyberweerbaarheid vraagt ook om duidelijke communicatie. Literatuur over cyber- en risicocommunicatie benadrukt dat informatie duidelijk, consistent, betrouwbaar, toegankelijk en tijdig moet zijn. Het National Cyber Security Centre (NCSC, 2024) stelt dat communicatie bij cybergerelateerde situaties niet alleen feitelijk juist moet zijn, maar ook handelingsperspectief moet bieden. Mensen moeten weten wat zij moeten doen, wat zij juist niet moeten doen en waar zij betrouwbare informatie kunnen vinden.

Voor studenten is dit extra belangrijk. Algemene waarschuwingen zoals “wees voorzichtig online” zijn onvoldoende. Studenten hebben concrete en toepasbare informatie nodig: hoe herken ik digitale risico's, welke stappen moet ik nemen, waar kan ik terecht en waarom is mijn gedrag belangrijk?

De cyberaanval op de Technische Universiteit Eindhoven laat zien dat digitale verstoringen direct gevolgen kunnen hebben voor de onderwijscontinuïteit. Lessen, tentamens en toegang tot studiemateriaal kwamen onder druk te staan, waardoor studenten behoefte hadden aan duidelijke communicatie en praktische informatie (COT Instituut voor Veiligheids- en Crisismanagement, 2025). Dit voorbeeld onderstreept dat cyberweerbaarheid niet alleen draait om techniek, maar ook om duidelijkheid, vertrouwen en handelingsperspectief.

Communicatie is daarmee een belangrijk instrument om cyberbewustzijn om te zetten in cyberweerbaar gedrag. Zonder duidelijke informatie blijven studenten afhankelijk van eigen interpretatie, medestudenten of informele bronnen.

2.5 Psychologie en organisatiecultuur

Cyberweerbaarheid hangt sterk samen met psychologie en organisatiecultuur. Sutton en Thompson (2025) benadrukken dat cyberveilig gedrag niet alleen afhankelijk is van techniek of training, maar ook van gedeelde normen, steun vanuit de organisatie en de praktische uitvoerbaarheid van regels. Als veiligheidsmaatregelen onduidelijk, omslachtig of onhandig zijn, volgen mensen ze minder goed.

Voor studenten betekent dit dat cyberveiligheid zichtbaar en normaal moet worden binnen de onderwijsomgeving. Wanneer studenten cyberveiligheid zien als

iets van ICT alleen, voelen zij zich minder verantwoordelijk. Wanneer veilig digitaal gedrag onderdeel wordt van studeren, samenwerken en professioneel handelen, ontstaat meer eigenaarschap.

Organisatiecultuur bepaalt dus of studenten zich gedragen als passieve gebruikers of als actieve schakels in digitale veiligheid. Een cyberweerbare cultuur verlaagt de drempel om vragen te stellen, risico's serieus te nemen en veilig gedrag te vertonen.

2.6 Praktijkinzichten uit de enquête binnen Avans

Om de inzichten uit het theoretisch onderzoek te toetsen binnen de eigen onderwijscontext is een enquête afgenomen onder studenten van Avans Hogeschool. De enquête is dus alleen binnen Avans uitgevoerd en is bedoeld om te bekijken of de theorie over cyberbewustzijn, meldgedrag, communicatie en handelingsperspectief ook herkenbaar is bij Avans-studenten. De enquête had een betrouwbaarheidsniveau van 95% en een foutmarge van minder dan 7%. Op basis van de berekening waren minimaal 195 respondenten nodig; uiteindelijk zijn 200 volledig ingevulde enquêtes verzameld. Daardoor kunnen de uitkomsten worden gebruikt als onderbouwing voor de situatie binnen Avans, maar niet automatisch als algemene uitspraak over alle hbo-studenten in Nederland.

De resultaten bevestigen wat het theoretisch onderzoek laat zien: digitale vaardigheid betekent niet automatisch cyberweerbaar gedrag. Uit de bijlage blijkt dat 49% van de studenten aangeeft voldoende te weten wat een cyberincident is, 21% goed en 12% zeer goed. Tegelijk voelt 44% zich zeker en 18% zich heel zeker in het herkennen van verdachte situaties, zoals phishing of verdachte berichten. Toch betekent herkennen niet automatisch dat studenten ook melden: 51% gaf aan een eerder meegemaakt incident niet te hebben gemeld, terwijl 10% dit wel deed en 39% niet van toepassing invulde.

De enquête laat vooral zien waar de handelingskloof zit tussen weten en doen. Bij redenen om niet te melden kwamen vooral onduidelijkheid over waar en hoe melden, twijfel of het wel echt een cyberincident was en onzekerheid over de ernst van het incident naar voren. Dat ondersteunt de theorie dat studenten in staat zijn om het juiste cyberveilige gedrag te tonen wanneer de vervolgstappen eenvoudig, duidelijk en laagdrempelig zijn. Ook blijkt uit de resultaten dat studenten vooral een docent of coach (29%) en de servicedesk van school (28%) als eerste aanspreekpunt zien. Voor alternatieve communicatie tijdens een cyberincident noemen zij vooral docent/coach (30%), privé-e-mail (26%) en WhatsApp (19%). Dit sluit aan bij het COM-B-model: veilig gedrag ontstaat eerder wanneer studenten weten wat zij moeten doen, de omgeving dit gedrag makkelijk maakt en de communicatie aansluit bij hun dagelijkse praktijk.

3. Gedragsanalyse

3.1 Van cyberbewustzijn naar cyberweerbaar gedrag

Het versterken van cyberweerbaarheid begint bij cyberbewustzijn, maar eindigt daar niet. Studenten moeten niet alleen weten dat digitale risico's bestaan, maar ook begrijpen hoe zij veilig moeten handelen. Juist daar ontstaat vaak een handelingskloof: studenten kunnen technologie gebruiken en herkennen soms risico's, maar weten niet altijd welke vervolgstap nodig is.

Deze handelingskloof maakt het versterken van cyberweerbaarheid belangrijk. Cyberbewustzijn zonder handelingsvermogen blijft passief. Cyberweerbaarheid ontstaat pas wanneer studenten risico's herkennen, de ernst begrijpen, verantwoordelijkheid nemen en veilig gedrag uitvoeren.

Om dit gedrag te verklaren, worden twee gedragsmodellen gebruikt: het COM-B-model en het Health Belief Model.

3.2 COM-B-model: cyberweerbaar gedrag vraagt om capaciteit, gelegenheid en motivatie

Volgens het COM-B-model van Michie et al. (2011) ontstaat gedrag pas wanneer drie voorwaarden aanwezig zijn: capability, opportunity en motivation. Dit model is relevant omdat cyberweerbaar gedrag niet alleen afhankelijk is van kennis, maar ook van de omgeving en motivatie.

Capability: kunnen studenten cyberweerbaar handelen? Capability gaat over het vermogen om gedrag uit te voeren. Bij studenten gaat dit niet alleen om digitale vaardigheid, maar vooral om handelingsbekwaamheid. Studenten moeten digitale systemen kunnen gebruiken, maar ook weten hoe zij risico's herkennen, beoordelen en veilig handelen.

Een student kan bijvoorbeeld goed omgaan met online leeromgevingen en digitale tools, maar toch onvoldoende weten hoe een phishingbericht wordt herkend, wanneer een link verdacht is of wat de juiste vervolgstap is. Cyberweerbaarheid vraagt daarom om meer dan functionele digitale vaardigheid. Het vraagt om concrete handelingskennis.

Het versterken van cyberweerbaarheid betekent dus dat studenten niet alleen informatie krijgen over risico's, maar ook leren wat zij praktisch moeten doen. Zonder die handelingskennis blijft cyberbewustzijn beperkt.

Opportunity: maakt de omgeving veilig gedrag mogelijk? Opportunity gaat over de fysieke en sociale omgeving die gedrag mogelijk maakt of belemmert. Studenten kunnen alleen cyberweerbaar handelen wanneer de onderwijsomgeving veilig gedrag ondersteunt. Als processen, instructies of meldroutes onduidelijk zijn, wordt veilig gedrag moeilijker.

Wanneer studenten niet weten waar zij terechtkunnen, welke informatie betrouwbaar is of welke stap logisch is, ontstaat twijfel. Dan zoeken zij eerst hulp bij medestudenten, docenten of coaches, of wachten zij af. Cyberweerbaar gedrag wordt dan afhankelijk van toeval in plaats van een duidelijk proces.

Het versterken van cyberweerbaarheid vraagt daarom om een omgeving waarin veilig gedrag logisch, toegankelijk en uitvoerbaar is. Processen moeten studenten ondersteunen in plaats van belemmeren.

Motivation: willen studenten cyberweerbaar handelen? Motivation gaat over de bereidheid om gedrag uit te voeren. Studenten kunnen weten wat veilig gedrag is, maar toch niet handelen wanneer zij de urgentie niet voelen.

Motivatie bestaat uit reflectieve en automatische motivatie. Reflectieve motivatie gaat over bewuste overtuigingen, bijvoorbeeld dat cyberveiligheid belangrijk is. Automatische motivatie gaat over gewoonten, emoties en impulsen, zoals gemakzucht, haast, schaamte of onzekerheid.

Studenten handelen eerder cyberweerbaar wanneer cyberveiligheid persoonlijk relevant wordt. Dat gebeurt wanneer zij begrijpen dat hun gedrag invloed heeft op hun eigen gegevens, accounts, privacy, studievoortgang en medestudenten. Zolang cyberveiligheid abstract blijft, blijft gedrag vaak passief.

Het COM-B-model laat daarmee zien dat cyberweerbaarheid pas ontstaat wanneer studenten de capaciteit, gelegenheid en motivatie hebben om veilig digitaal gedrag te vertonen.

3.3 Health Belief Model: risico's moeten persoonlijk, ernstig en handelbaar voelen

Het Health Belief Model verdiept vooral de motivatie achter cyberweerbaar gedrag. Dit model verklaart waarom mensen preventief gedrag wel of niet vertonen. Toegepast op studenten laat het model zien dat cyberveilig gedrag afhankelijk is van risicobeleving, vertrouwen in eigen kunnen en concrete prikkels tot actie (Gwenhure, 2025).

Waargenomen vatbaarheid. Waargenomen vatbaarheid gaat over de vraag of studenten denken dat digitale risico's hen kunnen overkomen. Studenten die zichzelf digitaal vaardig vinden, kunnen hun kwetsbaarheid onderschatten. Zij denken sneller dat cyberrisico's vooral anderen treffen. Daardoor voelen zij minder noodzaak om kritisch te handelen. Het versterken van cyberbewustzijn is daarom belangrijk om studenten te laten zien dat digitale risico's ook henzelf kunnen raken.

Waargenomen ernst. Waargenomen ernst gaat over de mate waarin studenten de gevolgen van digitaal onveilig gedrag serieus nemen. Een verdachte link of een zwak wachtwoord lijkt soms onschuldig, totdat de gevolgen concreet worden: accountmisbruik, identiteitsfraude, verlies van persoonsgegevens of problemen met studievoortgang. Cyberweerbaarheid groeit wanneer studenten begrijpen dat digitale risico's niet abstract zijn, maar direct invloed kunnen hebben op hun studie, privacy en digitale identiteit.

Waargenomen voordelen. Waargenomen voordelen verwijzen naar het geloof dat veilig gedrag zinvol is. Studenten moeten begrijpen dat hun gedrag verschil maakt. Een melding, een controle of het vermijden van een verdachte link kan schade beperken. Wanneer studenten hun eigen rol als nuttig ervaren, neemt de kans toe

dat zij cyberweerbaar handelen. Dit maakt cyberweerbaarheid een gedeelde verantwoordelijkheid in plaats van alleen een taak van ICT.

Waargenomen drempels. Waargenomen drempels zijn factoren die veilig gedrag tegenhouden. Bij studenten kunnen dit twijfel, schaamte, gemakzucht, onduidelijke processen of angst zijn om overdreven te reageren. Deze barrières verklaren waarom studenten soms niets doen, zelfs wanneer zij een risico herkennen. Het versterken van cyberweerbaarheid vraagt daarom niet alleen om meer kennis, maar ook om het verlagen van praktische en psychologische drempels.

Self-efficacy. Self-efficacy gaat over vertrouwen in eigen kunnen. Studenten kunnen vertrouwen hebben in hun algemene digitale vaardigheden, maar toch onzeker zijn over cyberveilig handelen. Zij weten dan wel hoe technologie werkt, maar twijfelen of zij een risico goed beoordelen of de juiste vervolgstap zetten. Cyberweerbaarheid vraagt daarom om handelingsvertrouwen: studenten moeten het gevoel hebben dat zij in staat zijn om veilig te handelen.

Cues to action. Cues to action zijn prikkels die studenten aanzetten tot gedrag. Dit kunnen waarschuwingen, voorbeelden, korte instructies, lessen, meldknoppen of signalen vanuit docenten zijn. Algemene boodschappen zoals “let op online veiligheid” zijn vaak te zwak. Concrete boodschappen zoals “controleer de afzender”, “klik niet op onbekende links” of “neem twijfel serieus” zetten sneller aan tot handelen. Het Health Belief Model maakt duidelijk dat studenten pas cyberweerbaar handelen wanneer zij risico’s persoonlijk relevant vinden, gevolgen serieus nemen, voordelen zien, barrières kunnen overwinnen en vertrouwen hebben in hun eigen handelen.

4. Samenhang tussen mens, proces, technologie en organisatiecultuur

Het belang van cyberweerbaarheid en cyberbewustzijn wordt duidelijk wanneer mens, proces, technologie en organisatiecultuur samen worden bekeken. Cyberweerbaarheid ontstaat niet door één maatregel, maar door de samenhang tussen deze vier onderdelen.

De mens staat centraal, omdat studenten dagelijks digitale keuzes maken. Zij klikken, delen, controleren, negeren of melden. Hun gedrag bepaalt mede de digitale veiligheid van de onderwijsomgeving.

Het proces bepaalt of veilig gedrag uitvoerbaar is. Wanneer processen onduidelijk zijn, blijven studenten twijfelen. Heldere processen verkleinen de handelingskloof tussen bewustzijn en gedrag.

De technologie moet veilig gedrag ondersteunen. Systemen, communicatiekanalen, meldmogelijkheden en beveiligingsmiddelen moeten aansluiten bij de manier waarop studenten daadwerkelijk studeren en communiceren.

De organisatiecultuur bepaalt of cyberveilig gedrag normaal voelt. Wanneer cyberveiligheid zichtbaar, bespreekbaar en praktisch wordt gemaakt, gaan studenten zichzelf eerder zien als onderdeel van de digitale veiligheidsketen.

Daarom is het versterken van cyberweerbaarheid en cyberbewustzijn noodzakelijk. Studenten kunnen digitaal vaardig zijn, maar zijn pas cyberweerbaar wanneer zij technologie kritisch, veilig en verantwoordelijk gebruiken binnen een omgeving die dat gedrag ondersteunt.

De enquête binnen Avans bevestigt dat deze samenhang tussen mens, proces, technologie en organisatiecultuur belangrijk is. Studenten willen meestal wel verantwoord handelen, maar hun gedrag wordt sterk beïnvloed door de vraag of de omgeving dat gedrag makkelijk maakt. De resultaten laten zien dat 61% van de respondenten aangeeft helemaal niet door school te zijn geïnformeerd over hoe zij een cyberincident kunnen melden en 25% niet duidelijk. Wanneer informatie of meldroutes onduidelijk zijn, ontstaat twijfel en kunnen studenten eerst informele bronnen raadplegen, wachten of helemaal niets melden.

Vooraf het proces en de communicatie blijken bepalend. Studenten hebben behoefte aan korte, concrete en betrouwbare informatie: wat is er aan de hand, wat moet ik doen, waar kan ik terecht en welk kanaal is officieel? De genoemde voorkeuren voor docent/coach, servicedesk, privé-e-mail en WhatsApp laten zien dat studenten vooral kiezen voor kanalen en personen die dichtbij, bekend en laagdrempelig zijn. De enquête laat daarmee zien dat cyberbewustzijn pas waarde krijgt wanneer studenten ook een helder handelingsperspectief krijgen. Dit bevestigt de theorie dat bewustzijn alleen onvoldoende is om cyberweerbaar gedrag te laten ontstaan.

Ook de organisatiecultuur speelt hierin mee. Als melden normaal, eenvoudig en veilig voelt, worden studenten eerder actieve schakels in digitale veiligheid. Als zij bang zijn om onrust te veroorzaken, niet weten of iets ernstig genoeg is of geen duidelijke terugkoppeling verwachten, wordt melden uitgesteld. De enquête ondersteunt daarom het theoretische uitgangspunt dat cyberweerbaarheid vraagt om een omgeving waarin veilig gedrag logisch, praktisch uitvoerbaar en bespreekbaar is.

5. Conclusie

Het versterken van cyberweerbaarheid en cyberbewustzijn van studenten in het hoger onderwijs is noodzakelijk door de toenemende digitalisering van het onderwijs en de groeiende digitale risico's die daarmee samenhangen. Studenten gebruiken dagelijks digitale systemen, maar digitaal gebruik betekent niet automatisch veilig digitaal gedrag.

Het literatuuronderzoek laat zien dat cyberweerbaarheid breder is dan technische beveiliging. Het gaat om gedrag, processen, technologie en organisatiecultuur. Securitygedrag van studenten wordt beïnvloed door risicoperceptie, gemak, onzekerheid, handelingskennis en de mate waarin veilig gedrag wordt ondersteund door de omgeving.

De gedragsanalyse met het COM-B-model laat zien dat studenten cyberweerbaar handelen wanneer zij de capaciteit, gelegenheid en motivatie hebben

om dat te doen. Het Health Belief Model laat aanvullend zien dat studenten vooral handelen wanneer risico's persoonlijk, ernstig en beïnvloedbaar voelen.

Daarom moet het hoger onderwijs cyberweerbaarheid en cyberbewustzijn structureel versterken. Studenten moeten niet alleen technologie kunnen gebruiken, maar ook leren hoe zij digitale risico's herkennen, beoordelen en veilig handelen. De kern ligt niet in digitale vaardigheid alleen, maar in cyberweerbaar gedrag.

De enquête binnen Avans ondersteunt deze conclusie. De resultaten laten zien dat studenten cyberincidenten vaak wel kunnen herkennen, maar dat zij vooral behoefte hebben aan eenvoudige meldroutes, duidelijke instructies, betrouwbare updates en bekende communicatiekanalen. Studenten zijn dus beter in staat om het juiste gedrag te tonen wanneer duidelijk is wat zij moeten doen, waar zij terecht kunnen en waarom hun handelen belangrijk is. Omdat de enquête alleen binnen Avans is afgenomen, met 200 volledig ingevulde reacties, een betrouwbaarheidsniveau van 95% en een foutmarge van minder dan 7%, moeten de uitkomsten worden gelezen als praktijkonderbouwing binnen Avans. De cijfers versterken vooral de theoretische conclusie dat cyberbewustzijn pas effectief wordt wanneer het wordt omgezet in eenvoudig uitvoerbaar cyberweerbaar gedrag.

De student is dus niet de zwakke schakel omdat hij digitaal onvaardig is. De werkelijke kwetsbaarheid ontstaat wanneer cyberbewustzijn niet wordt omgezet in cyberweerbaar handelen.

Literatuurlijst

Centraal Bureau voor de Statistiek. (2025a). Online veiligheid en criminaliteit 2024. CBS.

Centraal Bureau voor de Statistiek. (2025b). Online beveiligingsmaatregelen.

COT Instituut voor Veiligheids- en Crisismanagement. (2025). Leerevaluatie cyberaanval TU Eindhoven op 11 januari 2025: Naar nog meer (cyber)weerbaarheids-DNA.

Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: Insights from the health belief model. *Journal of Cybersecurity*, 11(1), Article tyaf034. <https://doi.org/10.1093/cybsec/tyaf034>

Michie, S., van Stralen, M. M., & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 6, Article 42. <https://doi.org/10.1186/1748-5908-6-42>

National Cyber Security Centre. (2024). Guidance on effective communications in a cyber incident.

SURF. (2023). Sectorrapportage 2023: Over security en privacy awareness in onderwijs en onderzoek.

Sutton, A., & Thompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security*, 148, Article 104110. <https://doi.org/10.1016/j.cose.2024.104110>

Van der Kleij, R. (2025). Nu veiligheid er niet meer is: Naar een aanpak van cyberrisico's die wél werkt.

Payroll Pirates en hoe zij HR beïnvloeden

Sarah Salih

Minor Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool

Dit onderzoeksartikel onderzoekt de opkomst en werkwijze van de hackersgroep Payroll Pirates (ook bekend als Storm-2657) en wat hun succes zegt over de digitale weerbaarheid van organisaties op het gebied van HR. Het onderzoek is uitgevoerd aan de hand van deskresearch, waarbij bestaande literatuur en online bronnen zijn geanalyseerd. Bronnen zijn geselecteerd op relevantie, betrouwbaarheid en actualiteit en met elkaar vergeleken om een zo volledig mogelijk beeld te verkrijgen. Uit de analyse blijkt dat Payroll Pirates misbruik maken van een combinatie van factoren van kwetsbaarheden binnen HR- en payrollsystemen. Door middel van phishing, nepwebsites en misleidende zoekadvertenties krijgen ze toegang tot bedrijfsplatformen, waar ze salarisgegevens manipuleren en financiële schade veroorzaken. De activiteiten van de groep kunnen worden verklaard aan de hand van de Routine Activity Theory, waarbij gemotiveerde daders, aantrekkelijke doelwitten en het ontbreken van bescherming samenkomen. Daarnaast toont het onderzoek aan dat kwetsbaarheden binnen HR niet alleen in die afdeling lijft, maar zich kunnen verspreiden naar andere afdelingen door systeemintegraties en identiteitsmisbruik. De bevindingen laten zien dat de digitale weerbaarheid van HR-afdelingen vaak tekortschiet en dat betere technische beveiliging, bewustwording en samenwerking tussen HR en andere afdelingen noodzakelijk zijn om aanvallen te voorkomen.

1. Inleiding

De digitalisering van HR-processen heeft organisaties efficiënter gemaakt, maar brengt tegelijkertijd nieuwe risico's met zich mee. Payroll- en HR-systemen bevatten grote hoeveelheden gevoelige persoonsgegevens en financiële informatie, waardoor zij een aantrekkelijk doelwit vormen voor cybercriminelen. Een recent en opvallend voorbeeld hiervan is de opkomst van de hackersgroep Payroll Pirates, ook bekend onder de naam Storm-2657.

Payroll Pirates hebben internationale aandacht gekregen door hun aanvallen op payrollsystemen binnen organisaties in de Verenigde Staten, voornamelijk bij hoger onderwijs. Volgens een artikel van Microsoft (2025) maakt deze groep gebruik van phishing, misleidende advertenties en zwakke beveiligingsmaatregelen binnen bedrijfssystemen om toegang te krijgen tot salarisgegevens. Door deze werkwijze slagen zij erin om salarissen om te leiden en gevoelige gegevens te misbruiken, vaak zonder dat organisaties dit opmerken. Dit roept de vraag op in hoeverre organisaties voldoende digitaal weerbaar zijn, met name binnen HR.

Dit onderzoeksartikel richt zich daarom op de opkomst en werkwijze van Payroll Pirates en onderzoekt wat hun succes zegt over de digitale weerbaarheid van organisaties op het gebied van HR. Aan de hand van deskresearch en bestaande

literatuur wordt geanalyseerd welke factoren bijdragen aan het succes van deze hackersgroep, welke digitale kwetsbaarheden er binnen HR zijn, en hoe deze kwetsbaarheden kunnen doorwerken naar andere delen van de organisatie.

2. Methoden

Dit onderzoeksartikel is samengekomen door deskresearch. Bestaande informatie en bronnen zijn gebruikt in plaats van zelf onderzoeken uit te voeren.

De informatie is vooral verzameld via Google, door te zoeken op verschillende termen die te maken hebben met Payroll Pirates, maar ook de alternatieve naam, Storm-2657. Daarnaast is Perplexity AI gebruikt om extra bronnen te vinden en om een overzicht te krijgen van relevante informatie over het onderwerp. De prompt die hiervoor was gegeven vroeg om wetenschappelijke artikelen gerelateerd aan Payroll Pirates en andere situaties van payroll fraude.

Alle gevonden bronnen zijn daarna beoordeeld op relevantie en betrouwbaarheid. Er is gekeken of de informatie goed aansloot bij het onderwerp van het onderzoeksartikel en bij het vraagstuk. Ook is gelet op wie de bron heeft geschreven, hoe actueel de informatie is en of de informatie wordt ondersteund door andere betrouwbare bronnen.

Door meerdere bronnen met elkaar te vergelijken, is geprobeerd een zo duidelijk en eerlijk mogelijk beeld te krijgen over het onderwerp van Payroll Pirates. Een nadeel van deze methode is dat het onderzoek volledig afhankelijk is van bestaande online-informatie, die soms onvolledig kan zijn. Ook zijn de Payroll Pirates een specifieke groep waar pas kort informatie over is gedeeld online. Echter was er toch genoeg informatie te vinden om het onderzoeksartikel te onderbouwen.

3 Analyse

3.1 Literatuuronderzoek

Payroll Pirates, ook wel Storm-2657 genoemd, is een hackersnetwerk die payrollsystemen door de VS hackt om geld te verdienen (Fenster, 2025). Ze maken gebruik van cyberaanvallen om toegang te krijgen tot interne systemen van bedrijven en de salarisadministratie van werknemers te manipuleren. Door directe toegang tot payrollsystemen kunnen de hackers geld overmaken naar hun eigen rekeningen of het systeem zodanig verstoren dat bedrijven financieel schade lijden. Microsoft publiceerde op 9 oktober 2025 een rapport over deze Payroll Pirates, met uitleg over wat ze doen en hoe ze te werk gaan. Een aanval op Workday, een HR-platform, zorgde voor de aandacht rondom deze hackergroep. Door het platform binnen te dringen kregen de hackers toegang tot gevoelige persoonlijke en financiële gegevens van werknemers bij diverse grote organisaties. Omdat de groep zulke impact maakte en zich verder bleef uitbreiden, voerde Microsoft een onderzoek uit om bedrijven in te lichten over dit payroll gevaar.

De activiteiten van Payroll Pirates kunnen worden geanalyseerd met de Routine Activity Theory van Cohen & Felson (1979). Hoewel de theorie oorspronkelijk

is ontwikkeld om traditionele criminaliteit te verklaren, is het ook goed toepasbaar op cybercriminaliteit, zoals de activiteiten van Payroll Pirates. Hoewel de theorie oorspronkelijk is ontwikkeld om traditionele criminaliteit te verklaren, is het ook goed toepasbaar op cybercriminaliteit, zoals de activiteiten van Payroll Pirates. Deze theorie stelt dat criminaliteit ontstaat wanneer drie voorwaarden samenkomen: een gemotiveerde dader, een geschikt doelwit en het ontbreken van een capabele beschermer. Payroll Pirates vertegenwoordigen de gemotiveerde daders, waarbij financiële winst de drijfveer is. Payrollsystemen vormen geschikte doelwitten vanwege hun financiële waarde, en de concentratie van persoonsgegevens en het vaak beperkte toezicht binnen organisaties is de afwezigheid van een beschermende kracht (Abdulsalam, Farounbi & Ibrahim, 2021).

De Payroll Pirates gaan doelgericht te werk door werknemers te misleiden met nepwebsites die eruitzien als echte HR- en payrollportalen. Ze maken honderden phishingwebsites die sterk lijken op legitieme platforms zoals Workday en adverteren deze via betaalde zoekadvertenties, zodat ze bovenaan in Google verschijnen wanneer werknemers zoeken naar hun salaris- of HR-omgeving. Wanneer een slachtoffer op zo'n advertentie klikt en zijn inloggegevens invoert, worden deze direct gemeld aan de aanvallers. Met deze gestolen gegevens krijgen de criminelen toegang tot het echte HR-systeem van de organisatie. Daar passen ze vervolgens de bankgegevens voor salarisuitbetaling aan, waardoor het loon van de werknemer ongemerkt wordt overgemaakt naar een rekening die door de aanvallers wordt beheerd. Door steeds nieuwe domeinen en advertenties te gebruiken, weten de Payroll Pirates hun activiteiten lange tijd voort te zetten zonder snel ontdekt te worden (Silent Push, 2024).

Aan de hand van het volgende vraagstuk wordt onderzoek gedaan naar de opkomst en werkwijze van Payroll Pirates: *wat zegt het succes van Payroll Pirates over de digitale weerbaarheid van organisaties op het gebied van HR?*

Op basis van deze hoofdvraag zijn drie deelvragen opgesteld:

1. Welke factoren dragen bij aan het succes van Payroll Pirates?
2. Wat voor digitale risico's komen voor bij HR die te misbruiken zijn door Payroll Pirates?
3. Hoe kunnen kwetsbaarheden binnen HR doorwerken naar de rest van de organisatie?

3.2. Welke factoren dragen bij aan het succes van Payroll Pirates?

De publieke sector schijnt zwak te zijn in het reguleren en onderhouden van payroll systemen (Abdulsalam, Farounbi & Ibrahim, 2021). De studie toont aan dat veel payrollsystemen worden gekenmerkt door beperkte controles en weinig technologische bewustwording. Hierdoor ontstaan kansen voor kwaadwillenden om het systeem te manipuleren, bijvoorbeeld door het creëren van fictieve werknemers (ghost workers), het ongeautoriseerd aanpassen van salarissen of het omleiden van betalingen naar persoonlijke rekeningen, precies hetgene waarmee Payroll Pirates te

werk gaan. Daarnaast blijkt het onderhoud van deze systemen vaak inconsistent, waardoor er verouderde software en zwakke toegangsbeveiliging is. Ook regelgeving en handhaving rondom beveiliging worden niet altijd nageleefd. Ook al bestaan er concrete regels, ontbreekt er vaak effectieve naleving en sancties.

Kennis is ook een factor die Payroll Pirates kan helpen. Bedrijven delen bijvoorbeeld online van welke platformen zij gebruik maken, zoals via hun website, vacatures of LinkedIn. Hierin kan naar voren komen welke payroll systeem zij gebruiken en die informatie is ook beschikbaar voor hackers.

3.3. Wat voor digitale risico's komen voor bij HR die te misbruiken zijn door Payroll Pirates?

Payroll Pirates maken onder anderen gebruik van multi-factor authenticatie (MFA). Als deze volledig afwezig is of makkelijk te overschrijden is, kunnen ze systemen binnenkomen. Dit doen ze bijvoorbeeld door phishing mails te versturen waarin gevraagd wordt om MFA codes door te geven. Deze zien er dan uit als legitiem, vaak is de verzender vermomd als betrouwd bedrijf of collega. Ook worden de e-mails persoonlijk gemaakt door ze te richten op de organisatie die wordt aangevallen, waarbij logo's of industrie-situaties worden gebruikt om de ontvanger te overtuigen. Zodra de aanvaller eenmaal binnen is, kan deze zich voordoen als iemand binnen de organisatie, en vanuit die positie verder handelen. Zo worden er aanpassingen gemaakt waardoor er geen meldingen over aanpassingen binnen het systeem worden verstuurd, en worden personeelsgegevens aangepast waardoor de payroll naar accounts van aanvallers gaan (Microsoft, 2025).

Ook kunnen ze aan de nodige informatie komen door middel van een andere methode: namelijk het plaatsen van neppe advertenties van platformen op zoekmachines, waardoor werknemers op een verkeerde website terecht komen en hier gevoelige informatie invullen (MHR, g.d.).

3.4. Hoe kunnen kwetsbaarheden binnen HR doorwerken naar de rest van de organisatie?

Kwetsbaarheden binnen HR-afdelingen kunnen zich eenvoudig verspreiden naar de rest van de organisatie, omdat HR een centrale positie inneemt binnen bedrijfsprocessen en informatiestromen. HR-systemen bevatten niet alleen salarisgegevens, maar ook uitgebreide persoonsgegevens, toegangsrechten en koppelingen met andere interne systemen. Als aanvallers via phishing of zwakke MFA toegang krijgen tot HR-accounts, zijn er uiteindelijk niet alleen risico's voor de payroll, maar ook andere systemen. Aangezien deze ook vaak gelinkt zijn aan andere systemen in het bedrijf, kunnen Payroll Pirates op veel verschillende plekken komen en daardoor veel schade verrichten.

Daarnaast kan een inbreuk binnen HR leiden tot identiteitsmisbruik. Met toegang tot personeelsgegevens (bijvoorbeeld namen, functies, en e-mailadressen) kunnen aanvallers geloofwaardige phishingmails sturen naar andere afdelingen,

zoals finance of IT, maar ook de informatie buiten het bedrijf gebruiken. Omdat deze communicatie afkomstig lijkt van HR of een bekende collega, is de kans groot dat medewerkers deze berichten vertrouwen en opvolgen, waardoor de aanval zich verder verspreidt.

Ten slotte kan een HR-incident leiden tot juridische gevolgen voor de organisatie. Datalekken van personeelsinformatie raken aan privacywetgeving zoals de AVG (2024), waardoor niet alleen HR maar de volledige organisatie aansprakelijk kan worden gesteld. Dit kan resulteren in boetes, verplichte meldingen en strengere maatregelen. Ook komt hier reputatieschade bij kijken. Personeel en klanten kunnen vertrouwen in het bedrijf verliezen, waardoor er bijvoorbeeld extra overeenkomsten worden aangegaan of er zelfs mensen bij het bedrijf weggaan (Vliet, 2025).

4. Conclusie

Dit onderzoek richtte zich op de opkomst en werkwijze van Payroll Pirates en wat hun succes zegt over de digitale weerbaarheid van organisaties op het gebied van HR. Uit de literatuur en de analyse van de deelvragen lijkt dat het succes van deze groep bestaat uit een combinatie van technische, organisatorische en menselijke kwetsbaarheden binnen organisaties. Veel payroll- en HR-systemen zijn onvoldoende beveiligd en worden slecht onderhouden. Daarnaast worden bestaande regels niet altijd nageleefd, waardoor de consequenties voor cybercriminelen beperkt blijven.

4.1. Deelvraag 1: Welke factoren dragen bij aan het succes van Payroll Pirates?

Het succes van Payroll Pirates kan worden verklaard door een combinatie van factoren. Uit de literatuur blijkt een belangrijke factor is de zwakke inrichting en het beperkte onderhoud van systemen binnen organisaties. Dit sluit ook weer aan bij de Routine Activity Theory: payrollsystemen vormen een aantrekkelijk doelwit en bescherming ontbreekt vaak. Daarnaast speelt informatie een grote rol. Organisaties delen onbedoeld veel informatie over hun gebruikte software. Deze transparantie maakt het voor Payroll Pirates mogelijk om gerichte aanvallen op te zetten. Zij kunnen met de informatie bijvoorbeeld bedrijfsgerichte advertenties maken om hiermee personeelsgegevens te achterhalen. Ten slotte draagt het gebrek aan effectieve naleving van regelgeving en toezicht bij aan het succes van de hackers. Hoewel er regels bestaan rondom beveiliging en gegevensbescherming, blijkt de handhaving vaak zwak, waardoor het risico voor aanvallers beperkt blijft. Hierdoor ontstaat een kwetsbaarheid die niet alleen HR treft, maar uiteindelijk de gehele organisatie.

4.2 Deelvraag 2: Wat voor digitale risico's komen voor bij HR die te misbruiken zijn door Payroll Pirates?

De digitale risico's binnen HR liggen vooral op het vlak van technologie en menselijk gedrag. Payroll Pirates maken effectief gebruik van phishing, social engineering en zwakke of afwezige MFA's. Wanneer dit ontbreekt of medewerkers worden misleid

om codes door te geven, vervalt een cruciale beveiligingslaag. Dit risico hangt direct samen met het succes van de aanvallers; hoe minder concreet de beveiliging en bewustwording, hoe groter de kans op misbruik. Daarnaast vormen nepadvertenties en valse inlogportalen een gevaarlijk risico. Werknemers zoeken zelf actief naar HR-omgevingen en vertrouwen op zoekmachines, waardoor zij buiten de beveiligingsgrenzen van de organisatie kunnen worden misleid. Beide situaties zijn vanuit een bedrijf moeilijk te reguleren. Omdat de methodes sterk afhangen van het gedrag van personeel en hoe zij omgaan met verdachte links en contacten in plaats van een directe aanval, is het niet genoeg voor een bedrijf om simpele, technische maatregelen te nemen.

4.3 Deelvraag 3: Hoe kunnen kwetsbaarheden binnen HR doorwerken naar de rest van de organisatie?

De eerdergenoemde kwetsbaarheden beperken zich niet tot alleen HR. HR-systemen bevatten gevoelige persoonsgegevens en zijn vaak gekoppeld aan andere interne systemen, zoals finance en IT. Wanneer Payroll Pirates via HR toegang verkrijgen, kunnen zij deze positie misbruiken om zich verder door de organisatie te bewegen en extra schade aan te richten. Bovendien maakt toegang tot personeelsgegevens het mogelijk om zeer geloofwaardige vervolgh phishing uit te voeren. Met kennis van functies, namen en relaties met ander personeel kunnen aanvallers andere afdelingen benaderen onder het front van HR-verzoeken, waardoor het risico zich organisatiebreed verspreidt. Ook hebben HR-incidenten juridische en reputatiegevolgen die de hele organisatie raken. Datalekken kunnen leiden tot boetes, meldplicht en verlies van vertrouwen bij medewerkers en externe partijen.

4.4 Hoofdvraag: Wat zegt het succes van Payroll Pirates over de digitale weerbaarheid van organisaties op het gebied van HR?

Het succes van Payroll Pirates laat daarmee zien dat de digitale weerbaarheid van organisaties op het gebied van HR toch nog in veel gevallen tekortschiet. HR en onderliggende systemen vormen een aantrekkelijk en waardevol doelwit voor cybercriminelen. Voor het werkveld betekent dit dat organisaties HR beter moeten worden betrokken in de cybersecurity. Dit vraagt om betere technische beveiliging, zoals goed ingerichte MFA en strengere toegangscontroles, maar ook om structurele training en bewustwording van medewerkers. Daarnaast is nauwere samenwerking tussen HR, IT en security noodzakelijk om risico's tijdig te herkennen en aan te pakken.

5. Discussie

Door gebruik te maken van meerdere bronnen, waaronder wetenschappelijke artikelen en blogposts van bedrijven en hun research naar het onderwerp, is geprobeerd om de betrouwbaarheid van de bevindingen te vergroten. Het vergelijken van verschillende bronnen draagt bij aan een consistent beeld van de werkwijze en impact van Payroll Pirates. Tegelijkertijd heeft deze aanpak beperkingen voor de

validiteit van het onderzoek. Er was maar beperkte informatie bekend omdat dit nog een redelijk recent actieve groep is, en veel bronnen hetzelfde toelichtten. De resultaten geven vooral inzicht in algemene patronen en risico's, maar minder over de precieze statistieken van payrollfraude.

Deze beperkingen bieden tegelijkertijd wel de mogelijkheid voor vervolgonderzoeken. Toekomstig onderzoek zou zich kunnen richten op specifiekere data, bijvoorbeeld door het veld in te gaan door middel van interviews en enquêtes. Hiermee kan beter worden onderzocht hoe organisaties omgaan met systeembeveiliging en in hoeverre medewerkers zich bewust zijn van de risico's. Daarnaast is verder onderzoek naar de menselijke factor binnen HR-processen relevant, aangezien phishing en manipulatie een grote rol spelen in de werkwijze van Payroll Pirates. Ook kan vergelijkend onderzoek tussen sectoren of landen waardevolle inzichten opleveren over de invloed van regelgeving en digitale volwassenheid op de weerbaarheid van HR-systemen.

Ondanks de beperkingen laat dit onderzoek zien dat HR-afdelingen een kwetsbare maar belangrijke schakel vormen binnen de cybersecurity van organisaties.

Literatuurlijst

Abdulsalam, R., Farounbi, B.O., Ibrahim, A.K. (2021, 30 juni). Financial Governance and Fraud Detection in Public Sector Payroll Systems: A Model for Global Application. <https://gisrrj.com/paper/GISRRJ1213322.pdf>

Autoriteit Persoonsgegevens. (2024, 23 december). De AVG in het Kort. <https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/avg-algemeen/de-avg-in-het-kort>

Cohen, L.E., Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. University of Illinois. https://www.researchgate.net/publication/238322365_Social_Change_and_Crime_Rate_Trends_A_Routine_Activity_Approach

Fenster, D. (2025, 12 november). Payroll Pirates: One Network, Hundreds of Targets. Check Point. <https://blog.checkpoint.com/email-security/payroll-pirates-one-network-hundreds-of-targets/> MHR. (g.d.)

The Payroll Pirates: Are your staff salaries safe? <https://mhrglobal.com/sites/default/files/2025-02/MHR-1671-Payroll-Pirates-Whitewater.pdf> Microsoft Threat Intelligence. (2025, 9 oktober). Investigating targeted “payroll pirate” attacks affecting US universities. Microsoft.

<https://www.microsoft.com/en-us/security/blog/2025/10/09/investigating-targeted-payroll-pirate-attacks-affecting-us-universities/>

Silent Push. (2024, 3 december). Hunting Payroll Pirates: Silent Push Tracks HR Redirect Phishing Scam. <https://www.silentpush.com/blog/payroll-pirates/>

Van Vliet, M. (2025, 28 oktober). Reputatieschade: de best verborgen gevolgschade van cybercrime. ABN Amro. https://www.abnamroverzekeringen.nl/artikelen/reputatieschade-door-cybercrime?utm_source=chatgpt.com

Cyberdreigingen in softwareleveringsketens

Karel Rietveld

Master Veiligheid en Digitalisering, Hogeschool Saxion

1. Inleiding

Open Source Software (OSS) vormt een essentieel onderdeel van de digitale infrastructuur van de Rijksoverheid.

De urgentie van dit vraagstuk neemt toe naarmate de digitale infrastructuur complexer wordt en de afhankelijkheid van software-ecosystemen verder groeit. Deze ontwikkeling verschuift de aandacht van individuele systemen naar de gehele software-leveringsketen waaruit de gebruikte componenten afkomstig zijn.

Cyberdreigingen die voortkomen uit afhankelijkheden binnen softwareleveringsketens worden steeds beter in technische en beleidsmatige zin onderkend. Het blijft echter onduidelijk hoe dreigingen zich verhouden tot publieke waarden en rechtsstatelijke uitgangspunten.¹

2. Aanleiding

2.1 Huidige situatie

Vanuit mijn rol binnen Bureau Open Source Software (BOSS) zie ik dagelijks dat talloze IV-onderdelen, van interne ontwikkeltrajecten tot publiek beschikbare portalen, leunen op OSS-componenten. Deze componenten worden toegepast in applicaties en platformen die worden gebruikt voor de uitvoering van publieke taken. Daarmee vormen zij een structurele bouwsteen van het overheids-IT-landschap.

In beleidskaders en interne documenten wordt deze afhankelijkheid steeds explicieter onderkend. De Nederlandse Digitaliseringsstrategie (NDS) benoemt digitale weerbaarheid en digitale autonomie als centrale uitgangspunten voor de verdere ontwikkeling van de digitale overheid (Rijksoverheid, 2025). Open Source Software wordt hiermee verbonden omdat het organisaties meer inzicht geeft in de werking van gebruikte componenten en de afhankelijkheid van individuele leveranciers kan verminderen. Daarmee wordt OSS niet zuiver meer als technische keuze benaderd, maar als onderdeel van een breder digitaal ecosysteem waarin overheid, markt en gemeenschap met elkaar zijn verweven.

¹ Copilot Business is uitsluitend gebruikt als schrijfhulp voor grammaticale, stilistische en redactionele ondersteuning. De inhoudelijke analyse, interpretatie van bronnen en conclusies zijn door de auteur opgesteld.

2.2 Gewenste situatie

Tegenover de huidige situatie staat het streven naar een digitale overheid die haar eigen infrastructuur betrouwbaar, beheersbaar en uitlegbaar kan inzetten bij de uitvoering van publieke taken. Dit veronderstelt dat afhankelijkheden van publiek beschikbare software inzichtelijk zijn en dat er voldoende regie bestaat op de manier waarop deze publiek beschikbare software bijdraagt aan continuïteit, veiligheid en publieke verantwoording over de inzet van deze software.

Binnen dit beeld wordt OSS niet langer gezien als doel, maar als middel dat kan bijdragen aan digitale weerbaarheid en digitale autonomie, mits het inzetten van OSS past binnen duidelijke kaders en met voldoende aandacht voor afspraken (governance), verantwoordelijkheid en samenhang binnen de bredere digitale infrastructuur.

2.3 Urgentie

Overheidsdiensten worden steeds vaker gerealiseerd in softwareleveringsketens waarbinnen softwarecomponenten van uiteenlopende herkomst samenkomen en waarop de overheid beperkt invloed heeft (Ministerie van Financiën, 2023). Uit het onderzoek van Kampourakis et al. (2025) blijkt uit observaties van 33 incident analyses op software-leveringsketens dat het aanvalsoppervlak alleen maar groter wordt. Dit betekent dat er meer potentiële aanvalspunten ontstaan voor misbruik doordat organisaties afhankelijker worden van een groeiend aantal componenten en onderlinge afhankelijkheden.

Uit de Nationale Digitaliseringsstrategie blijkt de urgentie; cyberaanvallen, storingen en te grote afhankelijkheden vormen naast kracht ook een risico voor de veiligheid en autonomie van overheidssystemen. Hiermee vormen ze een risico voor burgers en bedrijven (Digitale Overheid, 2025).

Het is daarom noodzakelijk om niet alleen naar de werking van software te kijken, maar ook naar de impact van OSS binnen kritieke infrastructuur. Dit onderzoek richt zich op het gebruik van open source software binnen de IV-Organisatie van de Belastingdienst en het cyberdreigingsbeeld dat hiermee samenhangt. Publieke waarden en de democratische rechtsstaat vormen hierbij het normatieve kader waarbinnen deze dreigingen worden geduid. Daarmee staat niet het waarderen van open source software als zodanig centraal, maar de betekenis van cyberdreigingen voor de uitvoering van publieke taken.

3. Afbakening

Dit onderzoek richt zich op de IV-Organisatie van de Belastingdienst, waarbij de focus ligt op het gebruik van open source componenten. Het gaat hierbij om systemen binnen de digitale infrastructuur waarmee de Belastingdienst haar publieke taken uitvoert. De IV-Organisatie wordt daarbij beschouwd in haar rol als ontwikkelaar, beheerder en gebruiker van software binnen verschillende softwareleveringsketens.

Het onderzoek beperkt zich inhoudelijk tot cyberdreigingen die samenhangen met open source software in software-ecosystemen, zoals beschreven in literatuur en beleidsdocumenten. Het gaat om dreigingen op ketenniveau, waaronder supply-chain risico's en vormen van cyberbedrog in digitale infrastructuren.

Buiten scope vallen technische kwetsbaarheidsanalyses of het analyseren van specifieke systemen of componenten. Dit onderzoek heeft een duidend karakter en richt zich op de samenhang en betekenis van onderwerpen, niet op het ontwerpen of implementeren van maatregelen.

4. Relevantie

4.1 Maatschappelijke relevantie

De Rijksoverheid is in toenemende mate afhankelijk van digitale infrastructuren voor het uitvoeren van publieke taken. Deze infrastructuren raken direct aan publieke waarden, zoals betrouwbaarheid, transparantie, rechtszekerheid en bescherming van burgers en vormen randvoorwaarden voor het functioneren van de democratische rechtsstaat. Cyberdreigingen binnen complexe software-ecosystemen kunnen deze waarden onder druk zetten en het vertrouwen in de overheid aantasten.

In het openbaar bestuur spelen publieke waarden een centrale rol bij het bepalen wat weloverwogen en rechtvaardig handelen is voor een bestuurder. Het is onderdeel van het werk van publieke bestuurders en raakt direct aan het algemeen belang (Rutgers, 2011).

De Rijksoverheid slaagt er onvoldoende in om burgers te beschermen tegen de gevolgen van overheidsoptreden (Staatscommissie rechtsstaat, 2024). Daarbij komt dat de taak en rol van uitvoeringsorganisaties zijn om het eerste contactpunt voor burgers te zijn. En het stelt dat inspraak en tegenspraak vanuit de uitvoering nodig is om ontsporing op tijd kenbaar te maken.

Binnen het beleid van de Rijksoverheid wordt digitale weerbaarheid op cyberincidenten steeds meer gekoppeld aan het borgen van publieke waarden en de democratische rechtsstaat (Digitale Overheid, 2026). Dit maakt cyberdreigingen rond open source software niet alleen een technisch vraagstuk, maar ook een maatschappelijk en een bestuurlijk vraagstuk. Dit onderzoek draagt bij aan het verkrijgen van inzicht in de samenhang.

4.2 Praktische relevantie

Binnen de IV-Organisatie van de Belastingdienst is open source software geen uitzondering meer, maar onderdeel van de dagelijkse praktijk (RijksAcademie voor Digitalisering en Informatisering Overheid, 2022). Inzet van open source software in bedrijfs-kritische systemen vraagt om het maken van bewuste keuzes over governance, het nemen van verantwoordelijkheid vanuit de inzet van open source componenten en de beheersbaarheid van deze componenten (Ministerie van Financiën, 2023). Interne beleidsdocumenten onderkennen dat op deze punten

spanning kan ontstaan. De interne procedures rondom deze processen zijn recentelijk herzien (Directoraat-Generaal Belastingdienst, persoonlijke communicatie, 2025). Dit onderzoek helpt cyberdreigingen in open source software te duiden in relatie tot publieke waarden en rechtsstatelijke uitgangspunten. Daarmee ondersteunt het beleidsmatige en bestuurlijke afwegingen binnen de IV-Organisatie zonder vooruit te lopen op concrete oplossingen.

5. Probleemstelling

In het rapport Online ontspoord beschrijven Van Huijstee et al. (2021) een taxonomie van schadelijk en immoreel gedrag op het internet, waarbij wordt beschreven hoe online omgevingen gedrag kunnen faciliteren dat zich in een schemergebied bevindt. Het rapport laat zien dat dit gedrag niet los kan worden gezien van de manier waarop digitale omgevingen zijn ingericht. Daarnaast wijst het rapport op mechanismen zoals ogenschijnlijke anonimiteit, het ontbreken van duidelijke online normenstelling en een beperkte online regie of toezicht, waardoor het schadelijk gedrag alleen maar versterkt wordt.

Hoewel het rapport niet expliciet een aparte categorie benoemt rondom cyberbedrog in digitale infrastructuren, komen in de taxonomie aanknopingspunten naar voren die deze dreiging combineren met online schadelijk en immoreel gedrag. In de context van open source krijgt deze vraag namelijk een specifieke betekenis; open source componenten zijn onderdeel van een complexe softwareleveringsketen waarin verantwoordelijkheid, herkomst van software en de integriteit van deze software niet eenduidig is vast te stellen. Dit kan leiden tot kwetsbaarheden in de softwareleveringsketen, bijvoorbeeld door gemanipuleerde pakketten of ongeoorloofde wijzigingen in open source componenten.

Voor de IV-Organisatie van de Belastingdienst, die als uitvoeringsorganisatie opereert binnen het kader van de democratische rechtsstaat, kan dit de vraag oproepen hoe cyberdreigingen bij het gebruik van open source software niet alleen technisch, maar ook normatief en institutioneel moeten worden geduïd.

5.1 Hoofdvraag

De onderstaande onderzoeksvragen zijn opgebouwd vanuit de literatuurverkenning van het vraagstuk. Daarbij wordt eerst gekeken naar open source software en cyberdreigingen, gevolgd door een normatieve duiding aan de hand van publieke waarden en de democratische rechtsstaat.

De hoofdvraag luidt: *Hoe verhouden cyberdreigingen bij het gebruik van open source componenten in systemen zich tot publieke waarden en de democratische rechtsstaat binnen de IV-Organisatie van de Belastingdienst?*

Dit leidt tot de deelvragen;

1. Hoe wordt binnen de IV-Organisatie van de Belastingdienst gebruik gemaakt van open source componenten in systemen en welke typen cyberdreigingen worden daarbij onderkend?

2. Hoe worden cyberdreigingen bij het gebruik van open source componenten binnen overheidssystemen beschreven in relevante literatuur en beleidsdocumenten?
3. Welke publieke waarden worden volgens beleidsdocumenten en literatuur geraakt door cyberdreigingen bij het gebruik van open source in systemen?
4. Hoe worden cyberdreigingen en bijbehorende risico's zoals eerder benoemd geduid in relatie tot de democratische rechtsstaat, zoals die binnen het Nederlandse overheidskader wordt begrepen?
5. Welke spanningen doen zich voor tussen cyberveiligheid, openheid van open source software en het borgen van publieke waarden binnen de Belastingdienst?

Eerst wordt het gebruik van open source software en de bijbehorende dreigingen in kaart gebracht. Vervolgens worden deze dreigingen geduid en verbonden aan publieke waarden en de democratische rechtsstaat. Tot slot wordt gekeken naar de spanningen die hieruit voortkomen.

6. Onderzoeksmethoden

Dit onderzoek wordt uitgevoerd als een kwalitatieve literatuurstudie. Het doel van deze literatuurstudie is inzicht te verkrijgen in hoe cyberdreigingen worden beschreven en geduid en hoe deze zich verhouden tot publieke waarden en de democratische rechtsstaat. Deze methode is gekozen omdat de hoofdvraag gericht is op het duiden van samenhang tussen technische, organisatorische en normatieve aspecten. Niet op het meten van feitelijke beveiligingsniveaus.

Naast een beschrijvende analyse bevat deze literatuurstudie een normatief-duidend element, waarbij publieke waarden en uitgangspunten van de democratische rechtsstaat worden gebruikt als kader. Deze waarden worden ontleend aan wetenschappelijke literatuur, beleidsdocumenten en juridische kaders. Deze worden niet empirisch getoetst. Dit sluit aan bij het doel van het onderzoek, waarin interpretatie en duiding centraal staan.

De onderzoeksvraag en deelvragen zijn bewust opgebouwd langs drie niveaus:

- Het technische niveau (cyberdreigingen in de software-leveringsketens)
- Het organisatorische niveau (gebruik, governance en verantwoordelijkheid binnen de IV-Organisatie)
- Het normatieve niveau (publieke waarden en de democratische rechtsstaat)

Deze opbouw maakt het expliciet hoe de analyse van beschrijving naar duiding verloopt. De selectie van literatuur is hierop afgestemd, waarbij per deelvraag is gezocht naar bronnen die dit specifieke niveau ondersteunen.

De literatuurstudie is gebaseerd op publiek beschikbare bronnen, waaronder wetenschappelijke publicaties, beleidsdocumenten, strategische rapporten en position papers. Daarnaast is er één intern document van de Belastingdienst gebruikt ter contextbepaling. Dit document is (nog) niet openbaar beschikbaar en wordt

daarom volgens APA 7 behandeld als persoonlijk document en niet als beschikbare bron ter ondersteuning.

Er is gezocht naar wetenschappelijke literatuur op het gebied van open source software, supply-chain aanvallen, cyberdreigingen, democratische rechtsstaat, weerbare rechtsstaat en publieke waarden. Daarbij is geselecteerd op literatuur die in wetenschappelijke tijdschriften is verschenen en onderworpen aan peer review. Daarnaast zijn bronnen meegenomen wanneer zij aantoonbaar bijdragen aan de beantwoording van één of meerdere deelvragen. Deze selectie draagt bij aan de betrouwbaarheid en de praktijkgerichte wetenschappelijke onderbouwing van de analyse. Dit zorgt ervoor dat de gebruikte literatuur zowel actueel, wetenschappelijk onderbouwd als inhoudelijk passend is bij het vraagstuk en de hoofdvraag kan ondersteunen.

Er is geen empirisch onderzoek uitgevoerd. Daarmee zijn er geen interviews gehouden, is er geen enquête uitgezet en geen zuiver technische kwaliteitsmetingen gedaan. Deze onderzoeksmethode is gericht op het duiden van onderwerpen en creëren van samenhang, niet op het meten van het beveiligingsniveau of het evalueren van een specifiek softwaresysteem.

Eventuele uitspraken over gevolgen voor specifieke groepen of instituties zijn gebaseerd op bestaande literatuur en beleidsdocumenten en vormen geen zelfstandig empirisch onderzoek.

Door literatuur uit diverse disciplines te combineren, waaronder cybersecurity, bestuurskunde en rechtsstatelijke theorie, levert de literatuurstudie een samenhangend beeld van het vraagstuk zoals dit binnen de IV-Organisatie van de Belastingdienst speelt.

Dit vraagstuk vraagt om een interdisciplinaire benadering. Open Source Software waar cyberdreigingen ontstaan, beperkt zich niet tot een technisch beveiligingsvraagstuk. Inzichten vanuit cyberveiligheid zijn nodig om het karakter en de mechanismen van dreigingen binnen softwareleveringsketens te begrijpen, terwijl bestuurskundige literatuur inzicht geeft in de manier waarop uitvoeringsorganisaties omgaan met afhankelijkheden en risico's. Rechtsstatelijke theorie is nodig om deze dreigingen helder te verwoorden in relatie tot publieke waarden en de rol van de uitvoerende macht binnen de democratische rechtsstaat. De combinatie van deze disciplines maakt het mogelijk om het vraagstuk zowel technisch, bestuurlijk als normatief te analyseren.

Vanuit het technische perspectief onderzoeken van cyberdreigingen in software-leveringsketen is onvoldoende om dit vraagstuk te beantwoorden. Inzichten in cybersecurity zijn noodzakelijk om het karakter en de werking van supply-chain dreigingen te begrijpen, maar bieden geen antwoord op hoe een uitvoeringsorganisatie om moet gaan met deze dreigingen. Vanuit bestuurskundig perspectief is het noodzakelijk om te begrijpen welke governance vraagstukken er zijn, de verantwoordelijkheden en de beheersing van risico's er een rol spelen. De rechtsstatelijke theorie is vereist om vast te stellen welke publieke waarden en wat

de rol van een uitvoeringsorganisatie is binnen de democratische rechtsstaat. De combinatie maakt dat het vraagstuk zowel analytisch als normatief kan worden beoordeeld.

7. Probleemanalyse

Deze probleemanalyse wordt vanuit verschillende invalshoeken benaderd en op verschillende abstractieniveaus. Op technisch niveau wordt er gekeken naar cyberdreigingen binnen de software-leveringsketens en het gebruik van componenten in deze keten. Op organisatorisch niveau wordt de IV-Organisatie van de Belastingdienst beschouwd in haar rol als uitvoeringsorganisatie, inclusief governance, verantwoordelijkheden en besluitvorming rondom het gebruik van open source. Op normatief niveau wordt het vraagstuk behandeld in relatie tot publieke waarden en de democratische rechtsstaat. Door dit vraagstuk op verschillende niveaus te combineren ontstaat een samenhangend beeld van het vraagstuk in technische, bestuurlijke en maatschappelijke context.

7.1 Beantwoording deelvraag 1 – Gebruik OSS en type cyberdreigingen

Binnen de IV-Organisatie van de Belastingdienst, Douane en Dienst Toeslagen is het gebruik van open source toegestaan en wordt er actief gebruik van gemaakt. Het interne beleidsstuk Open Source (persoonlijke communicatie, 2025) stelt dat dit op een verantwoorde manier moet gebeuren. Hierbij zijn governance, onderhoud en support expliciet belegd en de verantwoordelijkheid ligt primair bij de ontwikkelteams.

In dit kader spelen organisatorische functies zoals het Open Source Program Office (OSPO) zoals BOSS in internationale termen wordt getypeerd, en het Security Operations Center (SOC) (RijksAcademie voor Digitalisering en Informatisering Overheid, 2022) een rol bij het ondersteunen en beheersen van risico's rondom open source software. Het beleid legt daarbij nadruk op betrouwbaarheid, levensvatbaarheid en activiteit binnen de community van componenten, wat aansluit bij het perspectief van de software-leveringsketen (Analistennetwerk Nationale Veiligheid, 2022).

Samengevat worden cyberdreigingen binnen de IV-Organisatie vooral onderkend als dreigingen die ontstaan bij het ongeoorloofd wijzigen van open source componenten, risico's over ongewenste aanpassingen en gebrek aan afspraken over beheer en onderhoud.

7.2 Beantwoording deelvraag 2 – Duiding van risico's en onzekerheden

Cyberdreigingen bij softwarecomponenten worden in de literatuur voornamelijk beschreven vanuit het perspectief van de gehele software-supply-chain; de software-leveringsketen. Het ontbreken van inzicht in afhankelijkheden, de herkomst hiervan en het onderhoud maakt systemen kwetsbaar voor manipulatie en misbruik (Nationaal Cyber Security Centrum, 2023).

Om meer inzicht in deze afhankelijkheden te krijgen, wordt in beleid en praktijk gestuurd op het gebruik van een Software Bill of Material (SBOM), waarmee zichtbaar wordt welke componenten onderdeel zijn van een systeem en hoe deze zich tot elkaar verhouden (Nationaal Cyber Security Centrum, 2025). Dit onderstreept dat het risico niet alleen ligt in afzonderlijke componenten, maar in het ontbreken van overzicht en controle in de volledige keten.

Internationale studies bevestigen dat supply-chain aanvallen structureel voorkomen en verschillende vormen aannemen, zoals het aanpassen van updates, misbruiken van afhankelijkheden en het injecteren van kwaadwillende code (Andreoli et al., 2023, Gokkaya et al., 2026, Kampourakis et al., 2025, Kumar et al., 2025). De beschrijving van de Kaseya aanval in het artikel toont aan dat een ransomware-aanval grote gevolgen kan hebben voor de gehele organisatie (Beaumont, 2021). Vanuit deze literatuur wordt geen expliciet onderscheid gemaakt tussen gesloten software en open source software; de dreiging wordt vooral verklaard door de complexiteit van afhankelijkheden en het ontbreken van duidelijke governance afspraken. Dit betekent dat deze dreigingen niet alleen technische risico's vormen, maar direct invloed hebben op de manier waarop overheidssystemen functioneren. Daarmee ontstaat de vraag welke betekenis deze dreigingen hebben voor het handelen van de overheid en de publieke waarden die daarbij een rol spelen.

7.3 Beantwoording deelvraag 3 – Publieke Waarden

Publieke waarden geven aan wat wenselijk is in publiek handelen en wat als rechtvaardig en verantwoord wordt beschouwd. Hiermee functioneren deze waarden als beoordelingskader voor beleid en uitvoering (Rutgers, 2011). Rutgers (2011) beschouwt publieke waarden als normatieve maatstaven voor goed overheidshandelen.

In de context van digitale overheidssystemen waarin open source componenten worden ingezet, zijn waarden als transparantie, rechtszekerheid, betrouwbaarheid en bescherming van burgers relevant. Deze waarden krijgen betekenis wanneer de in deelvraag 2 beschreven cyberdreigingen worden beoordeeld vanuit het perspectief van overheidsfunctioneren. In het beleid wordt ook expliciet erkend dat digitalisering effect heeft op publieke waarden en de wijze waarop de overheid haar taken uitvoert (Digitale Overheid, 2026).

De cyberdreigingen die samenhangen met software-leveringsketens betekenen concreet dat bepaalde aspecten van overheidshandelen onder druk komen te staan. Beperkt inzicht in herkomst en werking van software beperkt de transparantie van systemen. Kwetsbaarheden en manipulatie van softwarecomponenten raken de betrouwbaarheid van systemen. Het ontbreken van duidelijke governance-afspraken kan gevolgen hebben voor de werking van systemen. Aanvallen op de software-leveringsketen kunnen leiden tot verstoringen, waardoor de beschikbaarheid van overheidsdiensten onder druk komt te staan (Nationaal Cyber Security Centrum, 2023, 2025).

De impact van deze dreigingen op systemen heeft direct gevolgen voor burgers, waardoor ook de beschermende rol van de overheid geraakt wordt (Staatscommissie rechtsstaat, 2024). Deze analyse laat zien dat cyberdreigingen bij het gebruik van open source componenten niet alleen technische risico's zijn, maar direct raken aan publieke waarden die richting geven aan het handelen van de overheid.

7.4 Beantwoording deelvraag 4 – Rechtsstaat

De democratische rechtsstaat wordt in dit onderzoek begrepen als een staatsvorm waarin de overheidsmacht is gebonden aan het recht en waarin burgers worden beschermd door en tegen de overheid (Staatscommissie rechtsstaat, 2024). Deze opvatting sluit aan bij de Nederlandse context, waarin wetgeving, democratische controle en rechtsbescherming centrale elementen zijn (Rijksoverheid, z.d.).

In analyses van de Nederlandse rechtsstaat wordt benadrukt dat de werking van de rechtsstaat onder druk kan komen te staan wanneer de overheid onvoldoende in staat is haar taak op een betrouwbare en controleerbare wijze uit te voeren (Honingh & Ham, 2024; Staatscommissie rechtsstaat, 2024). De Staatscommissie rechtsstaat beschrijft dit als het tekortschieten van de beschermende functie van de overheid, met name waar burgers afhankelijk zijn van het functioneren en uitvoering daarvan (Staatscommissie rechtsstaat, 2024). Dit kan worden gezien als een situatie waarin de praktische werking van de rechtsstaat onder druk komt te staan.

In de context van cyberdreigingen binnen software-leveringsketens betekent dit dat risico's zoals kwetsbaarheden, afhankelijkheden en manipulatie van software directe gevolgen kunnen hebben voor het functioneren van de overheid. Wanneer systemen niet betrouwbaar of voorspelbaar functioneren, wordt het moeilijker om besluiten te controleren, uitkomsten te verklaren en burgers adequaat te beschermen. Daarmee raken dergelijke dreigingen aan de kern van rechtsstatelijk handelen.

Deze ontwikkeling wordt ook breder geplaatst in analyses van de digitale samenleving, waarin wordt gesteld dat de weerbaarheid van de rechtsstaat afhankelijk is van de kwaliteit en uitvoering en het vermogen om met nieuwe technologische risico's om te gaan (Honingh & Ham, 2024; Tinnevelt, 2025). Cyberdreigingen zijn daarmee niet alleen een technisch vraagstuk, maar hebben directe implicaties voor de manier waarop de overheid haar rechtsstatelijke rol kan vervullen.

Vanuit dit perspectief ontstaat vervolgens de vraag welke spanningen optreden wanneer openheid, cyberveiligheid en publieke waarden gelijktijdig moeten worden geborgd.

7.5 Beantwoording deelvraag 5 – Spanningen

Bij het gebruik van open source software ontstaat er spanning tussen openheid en transparantie enerzijds en cyberveiligheid en betrouwbaarheid anderzijds. Openheid

en transparantie zijn belangrijk omdat zij bijdragen aan inzicht in software, controleerbaarheid en verantwoording (Digitale Overheid, 2026). Tegelijkertijd maakt deze openheid het mogelijk dat kwetsbaarheden in componenten en afhankelijkheden binnen de software-leveringsketen zichtbaar worden en misbruikt kunnen worden (Nationaal Cyber Security Centrum, 2023, 2025).

Voor de IV-Organisatie van de Belastingdienst betekent dit dat het vergroten van transparantie en openheid niet zonder gevolgen blijft voor de beheersing van cyberrisico's. Omgekeerd kan het versterken van de cyberveiligheid leiden tot beperkingen in openheid, bijvoorbeeld doordat minder inzicht wordt gegeven in gebruikte componenten, afhankelijkheden of in de inrichting van systemen. Publieke waarden functioneren daarbij als maatstaf voor goed overheidshandelen, maar kunnen in de praktijk met elkaar conflicteren (Rutgers, 2011).

Deze spanning laat zien dat publieke waarden zoals transparantie en betrouwbaarheid niet gelijktijdig en maximaal kunnen worden gerealiseerd zonder onderlinge afweging. In rechtsstatelijke zin betekent dit dat de overheid moet balanceren tussen controleerbaarheid en het beschermen van burgers en systemen (Staatscommissie rechtsstaat, 2024). Daarbij speelt ook de vraag hoe deze afweging in de praktijk wordt gemaakt (Tinnevelt, 2025). Daarmee ontstaat binnen het gebruik van open source software een structureel spanningsveld tussen openheid, controleerbaarheid en het weerbaar en beheersbaar houden van digitale systemen.

8. Oplossingsrichtingen

In het onderzoek van het Verwey-Jonker Instituut (2025) is breed beschreven welke mogelijke handelingsperspectieven er kunnen zijn voor verschillende organisatielagen binnen de overheid in relatie tot anti-institutionele denkbeelden over de democratische rechtsorde. In dit onderzoek worden verschillende perspectieven beschreven, waarvan één direct aansluit bij deze probleemanalyse. Dit is handelingsperspectief 12: Vergroten maatschappelijke weerbaarheid (Verwey-Jonker Instituut, & RadarAdvies, 2025, p. 95). Met name het versterken van de publieke waarde 'transparantie' sluit aan bij de bevinding dat expliciete afwegingen rond openheid en afhankelijkheden noodzakelijk zijn.

De analyse laat zien dat de oplossingsrichting niet ligt in het terugdringen van het gebruik van open source componenten, maar in het scherper vaststellen van de verantwoordelijkheden van de IV-Organisatie. Van welke open source componenten is de organisatie afhankelijk (bijvoorbeeld; zijn componenten bedrijfskritisch en zijn er andere afspraken nodig) en vanuit welk expliciet afwegingskader wordt open source ingezet in de IV-Organisatie. Een goede afweging tussen cyberveiligheid, openheid van zelfontwikkelde (of gebruikte) open source componenten en publieke waarden (openheid, transparantie) kan bijdragen aan een bewustere keuze waar wel of niet open source software kan worden gebruikt.

Dit betekent dat het probleem niet alleen ligt in het gebruik van open source componenten, maar in het ontbreken van expliciet ingerichte governance en

afwegingskaders. Tegelijkertijd betekent dit dat ook deze oplossingsrichting afwegingen vraagt, omdat meer sturing op afhankelijkheden en veiligheid kan leiden tot beperkingen in openheid en transparantie.

9. Kritische beschouwingen

Dit onderzoek heeft een duidend karakter en bevat geen empirisch onderzoek. Daardoor kunnen bevindingen uit dit rapport niet worden getoetst aan de uitvoeringspraktijk.

In mijn rol als adviseur open source binnen het CTO Office heeft mijn eigen perspectief mogelijk invloed gehad op de analyse. De focus op softwareketen afhankelijkheden, governance en het expliciet maken van besluiten over de inzet van open source kan ertoe hebben geleid dat op andere perspectieven minder nadruk is gelegd.

De focus lag daardoor vooral op beleid en governance en niet op de ervaringen van medewerkers binnen de IV-Organisatie. Dit kan in vervolgonderzoek via een casestudy of interviews worden onderzocht.

Deze analyse maakt duidelijk dat cyberdreigingen in software-leveringsketens niet alleen technische risico's vormen, maar vooral leiden tot spanningen in het borgen van publieke waarden binnen de Belastingdienst. Het gebruik van open source software vraagt daardoor om expliciete afwegingen tussen openheid, transparantie en cyberveiligheid. Daarmee ligt de kern van het vraagstuk niet in het gebruik van open source zelf, maar in de wijze waarop deze afwegingen worden gemaakt en geborgd binnen de IV-Organisatie.

Literatuurlijst

Analistennetwerk Nationale Veiligheid. (2022). Themarapportage ongewenste inmenging en beïnvloeding democratische rechtsstaat. <https://www.rijksoverheid.nl/documenten/2022/07/31/themarapportage-ongewenste-inmenging-en-beinvloeding>

Andreoli, A., Lounis, A., Debbabi, M., & Hanna, A. (2023). On the prevalence of software supply chain attacks: Empirical study and investigative framework. *Forensic Science International: Digital Investigation*, 44, 301508. <https://doi.org/10.1016/j.fsidi.2023.301508>

Beaumont, K. (2021, Juli 2). Kaseya supply chain attack delivers mass ransomware event to US companies. DoublePulsar. <https://doublepulsar.com/kaseya-supply-chain-attack-delivers-mass-ransomware-event-to-us-companies-76e4ec6ec64b>

Digitale Overheid. (2025, november 26). De Nederlandse Digitaliseringsstrategie Samen versnellen. <https://www.digitaleoverheid.nl/nederlandse-digitaliseringsstrategie-nds/>

Digitale Overheid. (2026, Januari 27). Publieke Waarden. <https://www.digitaleoverheid.nl/publieke-waarden/>

Gokkaya, B., Aniello, L., & Halak, B. (2026). Software supply chain: A taxonomy of attacks, mitigations and risk assessment strategies. *Journal of Information Security and Applications*, 97, 104324. <https://doi.org/10.1016/j.jisa.2025.104324>

Honingh, M., & Ham, C. (2024). Verkenning en verdieping democratische erosie en repsons in Nederland. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. <https://www.kennisopenbaarbestuur.nl/site/binaries/site-content/collections/documents/2024/04/12/verkenning-en-verdieping-democratische-erosie-en-respons-in-nederland/Verkenning+en+verdieping+democratische+erosie+in+Nederland+-+april++2024+finaal.pdf>

Kampourakis, V., Kavallieratos, G., Gkioulos, V., & Katsikas, S. (2025). Cracks in the chain: A technical analysis of real-life supply chain security incidents. *Computers & Security*, 159, 104673. <https://doi.org/10.1016/j.cose.2025.104673>

Microsoft. (2026). Copilot Business. (GPT-4o) [Generatieve AI]. <https://microsoft.com>

Ministerie van Financiën. (2020, september 14). Belastingdienst (31.066); brief van de staatssecretarissen van Financiën over de stand van zaken van de verbeteringen bij de Belastingdienst en de plannen voor de komende periode (EK, O). Eerste Kamer der Staten-Generaal. https://www.eerstekamer.nl/overig/20200922/bijlage_1_brief_van_de/document

Ministerie van Financiën. (2023). Meerjarig Departementaal Informatieplan Financiën 2023-2025. Officiële Bekendmakingen. <https://zoek.officielebekendmakingen.nl/blg-1057286.pdf>

Nationaal Cyber Security Centrum. (2023). Omgaan met risico's in de toeleveringsketen. Ministerie van Justitie en Veiligheid. <https://www.ncsc.nl/toeleveringsketen/omgaan-met-risicos-de-toeleveringsketen>

Nationaal Cyber Security Centrum. (2025). Software Bill of Materials (SBOM) Een betrouwbare life cycle. Ministerie van Justitie en Veiligheid. <https://www.ncsc.nl/toeleveringsketen/software-bill-materials-sbom-een-betrouwbare-life-cycle>

RijksAcademie voor Digitalisering en Informatisering Overheid. (2022, januari 25). Tax Talk 2: Cybersecurity bij de Belastingdienst. <https://www.it-academieoverheid.nl/actueel/nieuws/2022/01/18/tax-talk-2-cybersecurity-bij-de-belastingdienst>

Rijksoverheid. (2025). De Nederlandse Digitaliseringsstrategie (NDS). Digitale Overheid. https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2025/07/108.201-NDS-publicatie_v19-WEB.pdf

Rijksoverheid. (z.d.). Democratische rechtsstaat in Nederland. Rijksoverheid. <https://www.rijksoverheid.nl/onderwerpen/democratie/democratische-rechtsstaat-in-nederland>

Rutgers, M. (2011). Het pantheon van de publieke waarden. https://pure.uva.nl/ws/files/2216703/108322_343438.pdf

Staatscommissie rechtsstaat. (2024). De gebroken belofte van de rechtsstaat - tien verbetervoorstellen met oog voor de burger. <https://www.staatscommissierechtsstaat.nl/onderwerpen/r/rapport>

Supply chain attack on Kaseya compromises hundreds of firms. (2021, Juli). [https://doi.org/10.1016/S1361-3723\(21\)00068-3](https://doi.org/10.1016/S1361-3723(21)00068-3)

Tinnevelt, R. (2025). Rechtsstatelijke cultuur en weerbare rechtsstaat. *Beleid en Maatschappij*, 52(2), 144-166. <https://doi.org/10.5553/BenM/138900692025052002005>

Van Huijstee, M., Nieuwenhuizen, W., Sanders, M., Masson, E., & Boheemen, P. v. (2021). Online ontspoord: Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Rathenau Instituut. https://www.rathenau.nl/sites/default/files/2021-07/Rathenau_Instituut_Rapport_Online_ontspoord.pdf

Verwey-Jonker Instituut, & RadarAdvies. (2025). Anti-institutionalisme in Nederland: Exploratieve overzichtsstudie van gedachtegoed, organisatie, voedingsbodems, risico's en bestaande handelingsperspectieven. (WODC rapport 3522). <http://hdl.handle.net/20.500.12832/3490>

Artikelen slachtofferschap

De belofte van liefde, de realiteit van misleiding; Hoe kwetsbare gebruikers digitale signalen van datingfraude missen

Rhodee Tonnis

Minor Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool

“Na jaren van een slecht huwelijk dacht ik mij weer echt geliefd en gezien te voelen. Ik dacht eindelijk iemand gevonden te hebben die echt naar me luisterde.” Dit is het waargebeurde verhaal van Linda (50). Na een lange tijd van eenzaamheid durfde Linda een nieuwe stap te zetten en ze schreef zich in bij een datingsite. Op een bekende datingsite ontmoet ze een man die zegt in Zuid-Afrika te werken in de mijnbouw. Hij deelt zijn dromen over een eigen mijn, een nieuw begin, en de hoop ooit weer gelukkig te worden in de liefde. Zijn berichten raken Linda diep van binnen en ze toont haar medeleven. Voor haar is deze man liefdevol, attent, doordacht en lijkt hij oprecht geïnteresseerd. Hij vertelt Linda dat zijn droom bijna werkelijkheid kan worden, alleen heeft hij geld nodig. Ze twijfelt maar besluit toch dat ze hem gaat helpen. Een kleine lening, denkt ze. Maar het blijft niet bij één keer. “Het voelde als een soort betovering,” vertelt ze “hij wist precies wat hij moest zeggen” (Oplichters op het Internet, 2018, 1:18).

Uiteindelijk raakt Linda ruim 65.000 euro kwijt. Ze sluit leningen af, verkoopt spullen, en verliest niet alleen haar spaargeld, maar ook haar vertrouwen in mensen. Later blijkt dat er veel meer mensen zijn met dezelfde soort verhalen. Jaarlijks worden in Nederland honderden mensen slachtoffer van datingfraude, ook wel romance scams genoemd. Volgens cijfers van de Fraudehelpdesk zijn de slachtoffers in 2023 samen ruim 7,6 miljoen euro kwijtgeraakt, in 2022 lag dit bedrag nog op 4,3 miljoen euro (WNL, 2024). De slachtoffers verliezen niet alleen geld, maar ervaren ook gevoelens van schaamte, eenzaamheid en wantrouwen.

Opvallend is dat vooral kwetsbare gebruikers vaker slachtoffer worden. Ook blijkt dat veel van hen de digitale signalen van fraude niet tijdig herkennen. Ze zien de rode vlaggen pas als het te laat is: plots verdwijnt de “geliefde”, het profiel wordt verwijderd, en het geld is weg. Juist dat ongrijpbare moment waarop hoop omslaat in bedrog, maakt datingfraude zo verraderlijk. Dat maakt de kern van dit onderzoeksartikel de volgende vraag: “In hoeverre zijn kwetsbare gebruikers zich bewust van de digitale signalen die wijzen op datingfraude?”

In dit onderzoek wil niet alleen kennis delen, maar vooral ook herkenning bieden. Want achter elk slachtoffer zit geen dom of naïef persoon, maar iemand die simpelweg geloofde in iets wat mooi leek. Daarom koppelt dit artikel waargebeurde verhalen aan wetenschappelijk onderzoek over kwetsbaarheid, digitale signalen,

bewustzijn en weerbaarheid. Door de combinatie van praktijk en theorie wordt zichtbaar waar het misgaat, waarom mensen signalen niet herkennen, en welke interventies kunnen helpen om toekomstige slachtoffers beter te beschermen.

1. De werkwijze van daders en signalen van fraude

1.1 De opbouw van vertrouwen

Bij datingsfraude nemen de criminelen contact op met hun doelwit/slachtoffers via online datingsplatforms (of sociale netwerken). De criminelen gebruiken gesloten aantrekkelijke foto's voor hun nepprofiel. Na het matchen op de datingsite bouwen ze een relatie op met de slachtoffers met het uiteindelijke doel hen te misleiden en financieel uit te buiten (Buchanan & Whitty, 2014, pp. 4–5). Achter de schermen van een online liefdesrelatie, schuilt vanuit de daders vaak een zorgvuldig voorbereid plan. Uit recent onderzoek van Schokkenbroek en Snaphaan (2025) blijkt dat oplichters bij online datingfraude niet willekeurig handelen, maar werken via de stappen van een systematisch draaiboek. Het draaiboek laat zien dat datingsfraude niet bestaat uit één vast patroon, maar een dynamisch en flexibel proces is waarin daders hun strategie voortdurend aanpassen aan het gedrag en de emoties van hun slachtoffers (Schokkenbroek & Snaphaan, 2025).

De voorbereiding van de fraude begint vaak al ver voordat het eerste contact plaatsvindt. Veel oplichters zijn niet alleen maar maken onderdeel uit van georganiseerde criminele netwerken, met trainingsprogramma's waarin zij leren hoe ze vertrouwen kunnen opbouwen en emotionele zwaktes kunnen benutten. In sommige landen, zoals Nigeria, Ghana en Maleisië, bestaan complete trainingscentra waar nieuwe leden leren hoe ze slachtoffers kunnen misleiden (Schokkenbroek & Snaphaan, 2025).

1.2 De georganiseerde wereld achter datingsfraude

Hoewel datingsfraude op het eerste gezicht lijkt op een individueel misdrijf, blijkt uit verschillende onderzoeken dat de daders vaak deel uitmaken van internationaal gestructureerde criminele organisaties. Vanuit deze organisaties wordt professioneel en hiërarchisch gewerkt, met een duidelijke taakverdeling tussen verschillende leden. Achter alleen al één "romantisch nepprofiel", kan een volledig team schuilgaan dat volgens vaste scripts en stappen opereert. Binnen deze netwerken bestaan specifieke rollen: de 'scammers' onderhouden contact met slachtoffers, 'scriptwriters' ontwikkelen de standaardgesprekken en verhaallijnen, terwijl 'money mules' verantwoordelijk zijn voor het doorsluizen van geld via internationale rekeningen of cryptovaluta (Europol, 2024).

In landen als Nigeria, Ghana, Myanmar en Cambodja zijn zelfs zogenaamde scam compounds ontdekt: grootschalige fraudecomplexen waar tientallen tot honderden mensen gelijktijdig werken aan het benaderen van slachtoffers (United Nations Office on Drugs and Crime, 2024). Sommige van deze personen werken onder dwang of valse beloften en staan zelf onder controle van criminele leiders. Dit

laat zien dat de lijn tussen dader en slachtoffer in sommige gevallen vervaagt (UNODC, 2024).

De motivatie van de daders is niet altijd het financiële aspect. Sommige daders zien hun gedrag rationeel door zichzelf te zien als “digitale overlevende”: mensen die door werkloosheid, armoede of sociale ongelijkheid worden gedwongen om online fraude te plegen (Whitty, 2022). Andere daders zien het juist als een uitdaging, waarbij ze testen hoe goed hun vermogen is om anderen te manipuleren. Dit doen zij echt voor het gevoel van een ‘kick’. Deze uiteenlopende motivaties manifesteren zich in de operationele werkwijze van de netwerken waar veel van deze daders deel van uitmaken.

1.3 Koppeling met criminologische theorie

De manier waarop datingsfraude tot stand komt, kan goed worden verklaard aan de hand van de Routine Activity Theory van Cohen en Felson (1979). Volgens deze theorie ontstaat criminaliteit wanneer drie elementen gelijktijdig aanwezig zijn: een gemotiveerde dader, een geschikt doelwit en het ontbreken van toezicht of bescherming. In het geval van online datingfraude is de dader gemotiveerd door financieel gewin en beschikt hij over de kennis en middelen om slachtoffers te manipuleren. In deze vorm van oplichting betreft het niet alleen gemotiveerde daders, maar ook gedwongen daders die als slachtoffers gezien kunnen worden.

De slachtoffers vormen geschikte doelwitten doordat zij emotioneel kwetsbaar zijn, recent verlies hebben ervaren of onvoldoende digitaal vaardig zijn om misleiding te herkennen. Het gebrek aan toezicht blijkt uit de aard van de digitale omgeving: datingsapps en sociale netwerken zijn vaak anoniem, waardoor er weinig sociale controle of verificatie plaatsvindt.

Deze combinatie van factoren creëert een situatie waarin oplichters relatief vrij kunnen handelen, zonder directe consequenties. De Routine Activity Theory laat hiermee zien dat datingsfraude niet alleen het gevolg is van individuele keuzes of goedgelovigheid, maar van de digitale context waarin contact ontstaat. De anonimiteit, snelheid en afstand van onlinecommunicatie verlagen de drempel voor manipulatie en vergroten de kans dat daders hun slachtoffers langdurig kunnen beïnvloeden.

1.4 De werkwijze van daders

In georganiseerde netwerken wordt de werkwijze steeds meer geprofessionaliseerd. De daders in georganiseerde netwerken werken met playbooks: handleidingen met voorbeeldzinnen, gespreksscripts en scenario's om empathie en geloofwaardigheid op te wekken. Met behulp van gestolen of kunstmatig gegenereerde foto's, zoals deepfakes², creëren zij aantrekkelijke nepprofielen. Dit doen de daders door te zeggen een baan te hebben als arts, militair of ingenieur, vaak ondersteund met vervalste

² Een beeld, geluid of ander materiaal dat nep is en gemaakt is door artificial intelligence.

documenten en geloofwaardig bedachte levensverhalen. Zo ontstaat een digitaal personage dat niet alleen echt lijkt, maar ook emotioneel aansluit bij het profiel van het slachtoffer (Schokkenbroek & Snaphaan, 2025).

Zodra de dader zijn “doelwit” heeft bepaald, begint de zogenaamde *hunt*. Sommige oplichters kiezen bewust voor mensen die kwetsbaar lijken. Dit zijn personen die recent gescheiden zijn, weduwen of alleenstaande ouderen. Anderen gebruiken een massabbenadering en sturen daarbij duizenden berichten in de hoop dat er iemand reageert (Schokkenbroek & Snaphaan, 2025).

1.5 De emotionele valstrik in verschillende fasen

Wanneer er een gesprek tot stand komt, zeggen de criminelen vaak al in een vroeg stadium van contact verliefd te zijn op het slachtoffer. Dit is een belangrijk waarschuwingssignaal. Vervolgens verplaatsen ze het contact van de datingsite naar privékanalen, hierbij kan gedacht worden aan bijvoorbeeld e-mail of WhatsApp. De criminelen houden lange tijd, soms zelfs jaren, contact met het slachtoffer (Buchanan & Whitty, 2014, pp. 4–5).

Vanaf dat moment begint de groomingfase, waarin de dader het slachtoffer langzaam maar zeker emotioneel inpalmt. Deze fase kan weken, maanden of zelfs jaren duren. De oplichter doet dit door verhalen te delen over zijn of haar verleden, zogenaamd kwetsbare momenten en gezamenlijke toekomstplannen. Hierdoor ontstaat bij het slachtoffer een gevoel van exclusieve intimiteit: het idee dat de ander hen echt begrijpt. Tegelijkertijd beperkt de dader het contact met de buitenwereld door subtiele suggesties: “Je familie zal dit niet begrijpen” of “Laten we onze liefde voor onszelf houden”. Dit isolatiemechanisme zorgt ervoor dat het slachtoffer steeds afhankelijker wordt van de dader voor emotionele steun (Smeitink, 2021).

De oplichter gebruikt technieken als love bombing (het overspoelen met complimenten en liefdesverklaringen), mirroring (het spiegelen van interesses en waarden) en isolation (het ontmoedigen van contact met familie en vrienden). De basis van deze manipulatie is emotionele conditionering. In het begin, bij de love bombing fase, creëren oplichters een gevoel van verbondenheid door constante aandacht, complimenten en empathie.

Dagelijks ontvangen slachtoffers berichten vol genegenheid, waarin de dader zich voordoet als een zorgzame en betrouwbare partner. Deze intensieve communicatie zorgt voor een dopamine-effect: elke nieuwe boodschap levert een klein gevoel van geluk en bevestiging op. Net als bij een verslaving, raakt het slachtoffer afhankelijk van deze emotionele prikkels (Whitty & Buchanan, 2016). Soms sturen daders cadeautjes of hebben ze videogesprekken met het slachtoffer (Schokkenbroek & Snaphaan, 2025). Ze spreken over toekomstplannen en gebruikt soms religieuze taal (“God heeft ons samengebracht”). Hierdoor ontstaat al snel een gevoel van verbondenheid (Smeitink, 2021).

Bij deze videogesprekken wordt vaak gebruik gemaakt van stemvervorming of gemanipuleerde beelden. Dit doen oplichters om hun identiteit geloofwaardig te

houden. Langzaam groeit een gevoel van vertrouwen, intimiteit en afhankelijkheid. Wat voor het slachtoffer als een vertrouwde relatie voelt, is voor de dader slechts een zorgvuldig opgebouwde façade³ (Schokkenbroek & Snaphaan, 2025). Zo creëren de oplichters een “simulatie van liefde”: een zorgvuldig opgebouwd digitaal verhaal waarin slachtoffers geloven dat ze een echte relatie aangaan (Smeitink, 2021). Zodra er voldoende emotionele binding is ontstaan, begint de zogenaamde “stingfase”: het moment waarop de dader geld vraagt (Schokkenbroek & Snaphaan, 2025).

Dit is een tweede waarschuwingssignaal. Deze strategie gebruiken de oplichters om de bereidheid van de slachtoffers te testen. Hierbij gebruikt de dader vaak technieken als schuldinductie (“als je echt van me houdt, dan help je me”), medelijden, liefde en morele druk (Smeitink, 2021). Meestal gebeurt dit via een geloofwaardig ogend verhaal waarbij er een plotselinge crisis, medische noodsituatie of reisprobleem plaatsvindt, waardoor het slachtoffer in paniek handelt. De bedragen beginnen klein van “alleen wat hulp voor een ticket”, maar groeien snel. In sommige gevallen worden ook fictieve derden geïntroduceerd, zoals een arts of advocaat, om echtheid te versterken en het slachtoffer te kunnen overhalen (Schokkenbroek & Snaphaan, 2025).

Uit recent onderzoek van Lyu, Gao en Zhang (2025) blijkt dat tijdsdruk een belangrijke rol speelt in de vatbaarheid voor online fraude. Wanneer slachtoffers onder emotionele druk worden gezet, bijvoorbeeld door angst de relatie te verliezen of door plotselinge crisissituaties, neemt hun vermogen tot rationeel oordelen sterk af. Dit verklaart waarom slachtoffers in de ‘stingfase’ impulsief geld overmaken of toezeggingen doen, ondanks eerdere twijfels.

1.6 De escalatie & chantage

Wanneer het slachtoffer niet langer kan of wil betalen, schakelen sommige daders over op “squeeze fase”: de fase van chantage of afpersing. Hierbij gebruiken ze intieme berichten of foto's als dreigmiddel (sextortion), of dreigen ze met openbaarmaking of geweld. Op dit punt verbreken slachtoffers vaak contact, maar toch blijft het gevaar bestaan. Veel slachtoffers worden opnieuw benaderd, soms door dezelfde oplichter onder een nieuwe identiteit, soms door anderen die hun gegevens hebben gekocht via zogenoemde sucker lists. Ook zogenaamde “recovery scams”, waarbij criminelen zich voordoen als hulporganisaties die het verloren geld kunnen terughalen, komen vaak voor (Schokkenbroek & Snaphaan, 2025).

Online datingfraude is geen toeval of impuls, maar een zorgvuldig psychologisch proces. De oplichter observeert, manipuleert en past zijn gedrag aan op het slachtoffer, waardoor het moeilijk te herkennen en zeer effectief is. Wat begint als een onschuldige kennismaking, groeit vaak uit tot een web van emotionele afhankelijkheid waarin slachtoffers hun grenzen en vertrouwen verliezen. Inzicht in

³ Een valse, zorgvuldig opgebouwde schijn van liefde en oprechtheid waarmee de dader het slachtoffer manipuleert.

deze werkwijze helpt toekomstige slachtoffers weerbaarder te worden: door de gebruikte technieken – van snelle verliefdheid en overdreven complimenten tot plotselinge geldverzoeken – te herkennen, kunnen rode vlaggen eerder worden opgemerkt en misleiding sneller worden doorzien.

1.7 Schuld & loyaliteit

In de volgende fase verandert de toon geleidelijk. De dader introduceert schuldgevoelens en morele druk. Geldverzoeken worden verpakt als een bewijs van liefde of loyaliteit: “Als je echt van me houdt, help je me nu” en “Ik zou hetzelfde voor jou doen”. Deze uitspraken spelen in op het natuurlijke verlangen van mensen om geliefden te helpen, waardoor rationele grenzen vervagen. Psychologisch gezien is dit een vorm van cognitieve dissonantie: het slachtoffer ervaart spanning tussen de overtuiging dat de relatie echt is en de twijfel over de geldvraag. Om deze spanning te verminderen, kiezen veel slachtoffers ervoor te geloven in de liefde, zelfs vaak tegen beter weten in (Smeitink, 2021).

1.8 Traumabinding

Oplichters gebruiken daarnaast emotionele dreiging. Wanneer het slachtoffer aarzelt of vragen stelt, reageren daders vaak met woede, stilte of chantage. Sommigen dreigen zelfs met zelfmoord of met het beëindigen van de relatie. Deze emotionele wisselingen vanuit de daders, zorgen voor het creëren van verwarring en angst. Als gevolg probeert het slachtoffer nog meer om de relatie te redden. Dit proces staat in de psychologie bekendstaat als traumabinding: een emotionele band die ontstaat tussen slachtoffer en dader door afwisseling van beloning en straf (Whitty, 2019). Het resultaat is een diepgaande psychologische afhankelijkheid. Slachtoffers beginnen hun eigen waarneming in twijfel te trekken en ontwikkelen gevoelens van schaamte, schuld en wantrouwen. Deze gevoelens hebben zij tegenover zichzelf en anderen. Volgens onderzoek van Whitty en Buchanan (2016) ervaren veel slachtoffers deze emotionele schade zwaarder dan het financiële verlies. Ze rouwen niet alleen om hun geld, maar vooral om het verlies van wat zij dachten dat een echte liefde was.

De manipulatie eindigt niet altijd met het verbreken van contact. Sommige slachtoffers blijven maanden of zelfs jaren hopen dat de relatie echt was, zelfs nadat ze de waarheid weten. Dit staat bekend als: post-scam attachment. De dader heeft niet alleen geld gestolen, maar ook een deel van de identiteit en zelfwaardering van het slachtoffer. Dit laat zien hoe krachtig de psychologische mechanismen van misleiding zijn.

1.9 Iedereen slachtoffer

Hoewel online datingsfraude zich afspeelt in de digitale wereld, richt de aanval zich niet op technologie, maar op het menselijk brein. Daders weten feilloos in te spelen op emoties als liefde, vertrouwen, hoop en schuld. Uit diverse onderzoeken (o.a.

Buchanan & Whitty, 2014; Smeitink, 2021; Schokkenbroek & Snaphaan, 2025) blijkt dat slachtoffers niet misleid worden door domheid of onwetendheid, maar door doelbewuste psychologische beïnvloeding. Deze manipulatie is zo geleidelijk dat slachtoffers vaak pas beseffen wat er gebeurt wanneer het te laat is.

2. Kwetsbare groepen: wie loopt het meeste risico?

2.1 Emotionele kwetsbaarheid

Hoewel iedereen dus slachtoffer kan worden van online datingsfraude, blijkt uit verschillende onderzoeken dat bepaalde groepen gebruikers aanzienlijk kwetsbaarder zijn voor deze vorm van misleiding. Kwetsbaarheid ontstaat niet uit domheid of onwetendheid, maar uit een samenspel van emotionele, sociale en digitale factoren (Lazarus, Whittaker, McGuire & Platt, 2023).

De eerste risicogroep bestaat uit personen met een verhoogde behoefte aan emotionele verbondenheid. Dit zijn mensen die recent een scheiding, verlies van een partner of langdurige eenzaamheid hebben ervaren of doorgemaakt. Deze groep is gevoeliger voor de aandacht en affectie, die oplichters doelbewust inzetten. Vaak zijn vrouwen tussen de veertig en zestig jaar, die zich na een periode van relatiebreuk of verlies opnieuw op de datingsapps begeven slachtoffer (Whitty & Buchanan, 2016; Cross, Dragiewicz & Richards, 2018). Deze groep ervaart vaak een leegte in sociale of emotionele relaties, waardoor zij ontvankelijker worden voor de bevestiging en romantische beloftes die fraudeurs gebruiken.

2.2 Lage digitale geletterdheid

Een tweede risicogroep is de groep die laag digitaal geletterd is, deze groep heeft moeite met het herkennen van fraude. Uit onderzoek van Lazarus et al. (2023) blijkt dat een groot deel van de slachtoffers weliswaar hoogopgeleid is, maar onvoldoende digitale vaardigheden bezit om online risico's in te schatten. Vooral gebruikers die minder ervaring hebben met online datingplatforms of beperkte kennis hebben van digitale veiligheid, herkennen de rode vlaggen minder snel. Ook leeftijd kan een rol spelen. De oudere gebruikers op datingsapps vertrouwen vaker op intuïtie in plaats van kritisch te kijken naar online gedragspatronen, wat hun kwetsbaarheid vergroot (Saad & Abdullah, 2018).

2.3 Sociale isolatie en gebrek aan steun

Een derde belangrijke factor is sociale isolatie of beperkte sociale steun. Mensen met een klein netwerk om hun online-ervaringen mee te delen, hebben minder gelegenheid om waarschuwingen of twijfels te bespreken. Daardoor kan de manipulatie langer doorgaan. Dit is iets wat oplichters benutten, door slachtoffers te ontmoedigen om met familie of vrienden over de relatie te praten. Deze strategie versterkt de emotionele afhankelijkheid en vermindert de kans dat slachtoffers externe signalen van misleiding opmerken (Cross et al., 2018).

2.4 Psychologische kenmerken

Ook psychologische eigenschappen kunnen bijdragen aan kwetsbaarheid. Mensen met een sterk romantisch ideaalbeeld, een hoog empathisch vermogen of de neiging tot vertrouwen, gaan sneller mee in het verhaal van de oplichter. Emotionele gevoeligheid en een verlangen naar bevestiging maken hen vatbaar voor eerdergenoemde technieken zoals love bombing en mirroring, waarbij de dader zichzelf voordoot als de perfecte partner (Whitty, 2018).

Er kan worden gesteld dat kwetsbaarheid voor datingsfraude voortkomt uit een combinatie van emotionele behoefte, sociale isolatie en beperkte digitale weerbaarheid. Waar echte liefde begint met vertrouwen, begint datingsfraude vaak op dezelfde manier – maar wordt dat vertrouwen doelbewust uitgebuit. Door inzicht te krijgen in de kenmerken van kwetsbare groepen kan er worden ingespeeld op preventieve campagnes, voorlichtingsprogramma's en digitale bewustwordingsinitiatieven voor degenen die het grootste risico lopen.

3. Interventies: preventie als sleutel tot bescherming

3.1 Het belang van preventieve aanpak

Het voorkomen van datingsfraude vraagt om interventies die niet alleen informeren, maar ook gedragsverandering en bewustwording, stimuleren op het moment dat gebruikers het meest kwetsbaar zijn. Preventie is daarom de belangrijkste sleutel tegen digitale misleiding (Whitty, 2019).

3.2 Bestaande interventies

Er bestaan wereldwijd verschillende initiatieven die proberen om gebruikers te beschermen tegen online datingfraude. Een voorbeeld hiervan is het Britse programma "Stop, Think, Don't Send". Deze campagne richt zich op bewustwording door middel van korte onlinevideo's en social media berichten waarin slachtoffers hun verhaal delen. De nadruk ligt op drie preventieve stappen: stoppen voordat je geld overmaakt, nadenken over de geloofwaardigheid van het verhaal, en niet verzenden van geld of persoonlijke gegevens. Onderzoek toont aan dat herhaald contact met deze slogan het bewustzijn van risico's verhoogt (Cross, Dragiewicz & Richards, 2018).

3.3 Technologische samenwerking en meldsystemen

Een ander effectief voorbeeld, is de samenwerking tussen Match Group (eigenaar van o.a. Tinder, OkCupid en Hinge) en de Amerikaanse organisatie NO MORE, waarbij gebruikers via pop-upberichten en veiligheidsnotificaties worden gewaarschuwd bij verdacht gedrag. Deze vorm preventie blijkt een positief effect te hebben op de alertheid van gebruikers. Met name als deze waarschuwingen verschijnen op cruciale momenten, zoals bij het delen van persoonlijke informatie of het verplaatsen van contact naar WhatsApp (Lazarus et al., 2023).

3.4 Een innovatieve interventie: AI-videovoorlichting

Om preventie nog effectiever te maken, is het essentieel om gebruikers niet alleen te informeren, maar ook actief te confronteren met realistische voorbeelden van misleiding. Daarom stel ik in dit onderzoek een nieuwe interventie voor: een AI-gegenereerde voorlichtingsvideo die op datingsplatforms verplicht wordt getoond aan nieuwe en bestaande gebruikers. De video duurt ongeveer dertig seconden en wordt automatisch afgespeeld zodra het profiel is aangemaakt. Gebruikers kunnen deze niet overslaan of wegklikken, waardoor ze eigenlijk verplicht worden de video te kijken. De inhoud van de video toont herkenbare signalen van datingfraude die besproken zijn in 'Hoofdstuk 1: De werkwijze van daders en signalen van fraude'.

De video wordt elke zes maanden vernieuwd op basis van actuele fraudevormen en taalpatronen, die door opsporingsinstanties en datingplatforms worden gemeld. Dankzij AI-technologie kan de inhoud snel worden aangepast aan nieuwe trends. Door de samenwerking met grote datingsapps wordt de boodschap verspreid onder miljoenen gebruikers. Deze gezamenlijke aanpak verhoogt niet alleen de zichtbaarheid, maar ook de geloofwaardigheid van de waarschuwing.

3.5 Bewustwording en digitale bescherming

Door deze AI-gegenereerde video te combineren met bestaande pop-upmeldingen, ontstaat een sterke preventiestrategie. Deze combinatie van directe en voorbereidende interventies zorgt ervoor dat gebruikers leren omgaan met signalen van fraude. Zo kunnen de korte pop-up waarschuwingen het geleerde uit de video versterken, waardoor de kans dat slachtoffers rode vlaggen herkennen en tijdig handelen aanzienlijk toeneemt.

4. Conclusie

Dit onderzoek laat zien dat online datingfraude niet slechts een individueel incident is tussen twee personen, maar een ingewikkeld samenspel van psychologische beïnvloeding, digitale kwetsbaarheid en georganiseerde criminaliteit. Wat begint als een digitale ontmoeting vol hoop en affectie, verandert voor veel slachtoffers in een zorgvuldig vorm van misleiding. De analyse van zowel de werkwijze van daders, als de kwetsbaarheden van slachtoffers toont aan dat vertrouwen doelbewust wordt gebruikt.

De centrale onderzoeksvraag luidt: *In hoeverre zijn kwetsbare gebruikers zich bewust van de digitale signalen die wijzen op datingfraude?* Uit de bevindingen blijkt dat veel slachtoffers deze signalen niet tijdig herkennen. Dit komt niet door naïviteit of onwetendheid, maar omdat de manipulatie geleidelijk verloopt. Technieken als love bombing, mirroring en schuldinductie wekken gevoelens van verbondenheid op, waardoor slachtoffers hun oplettendheid verliezen. Vooral personen met een verhoogde behoefte aan emotionele steun, beperkte digitale geletterdheid of een klein sociaal netwerk blijken extra vatbaar te zijn voor deze vormen van misleiding. Een belangrijk inzicht uit dit onderzoek, is dat niet alle daders uit vrije wil handelen. Dit onderzoek wijst erop dat sommige daders binnen georganiseerde netwerken zelf

onder druk of dwang handelen. Individuen worden soms misleid, uitgebuit of zelfs gedwongen om fraude te plegen onder dreiging van geweld of opsluiting. In die zin ontstaat een moreel grijs gebied waarin slachtoffers soms ook slachtoffers maken. De voorgestelde AI-gegenereerde interventievideo kan bijdragen aan het vergroten van digitale weerbaarheid. Door gebruikers vroegtijdig te confronteren met herkenbare signalen van fraude zoals overhaaste liefdesverklaringen, geldverzoeken of verzoeken om communicatie buiten het platform kan preventief gehandeld worden. De combinatie van educatieve content en real-time waarschuwingen (zoals pop-ups) versterkt het bewustzijn en kan ervoor zorgen dat minder mensen slachtoffer worden.

Waar dit onderzoek begon met het verhaal van Linda, eindigt het met een bredere boodschap: achter elke klik, elk bericht en elk digitaal profiel schuilt een mens met gevoelens van hoop, liefde en vertrouwen. Online datingfraude raakt daarmee iets menselijks. Slachtoffers zijn geen naïeve gebruikers, maar mensen die geloofden in oprechtheid en sommige daders zijn geen monsters, maar individuen gevangen in systemen van misleiding en uitbuiting.

Literatuurlijst

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 20(3), 261–283. Geraadpleegd op 11 oktober 2025, van <https://doi.org/10.1080/1068316X.2013.772180>

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. Geraadpleegd op 11 oktober 2025, van <https://doi.org/10.2307/2094589>

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *British Journal of Criminology*, 58(6), 1303–1322. Geraadpleegd op 11 oktober 2025, van <https://doi.org/10.1093/bjc/azx044>

Europol. (2024). Online romance scams: Organized networks and emerging threats. Europol Intelligence Brief. Geraadpleegd op 15 oktober 2025.

KIJK (2022, 31 december). Eenzame singles OPGE LICHT via DATINGFRAUDE | Oplichters op het Internet | KIJK Aflevering S1A1 [Video]. YouTube. Geraadpleegd op 10 oktober 2025, van <https://www.youtube.com/watch?v=6YybQKvgEOM>

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000–2021). *Journal of Economic Criminology*, 2, 100013. Geraadpleegd op 11 oktober 2025, van <https://doi.org/10.1016/j.jeconc.2023.100013>

Lyu, C., Gao, S., & Zhang, Q. (2025). The impact of time pressure and type of fraud on susceptibility to online fraud. *Frontiers in Psychology*, 16, Article 1508363. Geraadpleegd op 13 oktober 2025, van <https://doi.org/10.3389/fpsyg.2025.1508363>

Saad, M. E., & Abdullah, S. N. H. S. (2018). Cyber romance crime victimization analysis using routine activity theory. *International Journal of Advanced Computer Science and Applications*, 9(9), 280–287. Geraadpleegd op 13 oktober 2025, van <https://doi.org/10.14569/IJACSA.2018.090937>

Schokkenbroek, J. M., & Snaphaan, T. (2025). Love as bait: A scoping review and crime script analysis of online romance scams. *Trauma, Violence & Abuse*. Advance online publication. Geraadpleegd op 10 oktober 2025, van <https://doi.org/10.1177/15248380251361046>

Smeitink, H. (2021, 10 februari). A postmodern love story: How romance scammers exploit the online dating experience through simulated love (Master's thesis, Universiteit Utrecht).

Fraudehulpdesk. Geraadpleegd op 10 oktober 2025, van <https://www.fraudehulpdesk.nl/wp-content/uploads/2021/02/Thesis-Hester-Smeitink.pdf>

United Nations Office on Drugs and Crime. (2024). Scam compounds and forced criminality in Southeast Asia. UNODC Regional Report. Geraadpleegd op 15 oktober 2025.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105–109. Geraadpleegd op 11 oktober 2025, van <https://doi.org/10.1089/cyber.2017.0304>

Whitty, M. T. (2019). The psychology of scams: Provoking and committing errors of judgement. *Crime, Law and Social Change*, 71(1), 63–76. Geraadpleegd op 11 oktober 2025, van <https://doi.org/10.1007/s10611-018-9816-6>

Whitty, M. T., & Buchanan, T. (2016). The psychology of the online romance scam. In *Cyberpsychology* (pp. 123–138). London: Routledge. Geraadpleegd op 13 oktober 2025.

WNL. (2024, 26 januari). Meer dan 7,6 miljoen euro schade door datingfraude. Geraadpleegd op 10 oktober 2025, van <https://wnl.tv/2024/01/26/meer-dan-76-miljoen-euro-schade-door-datingfraude>

De hardnekkigheid van phishing: waarom bewustwordingscampagnes burgers onvoldoende beschermen

Denise Zieleman

Minor Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool

Phishing is wereldwijd een van de meest voorkomende vormen van cybercriminaliteit en vormt ook in Nederland een urgent veiligheidsvraagstuk. Ondanks aanzienlijke investeringen van banken, overheid en politie in bewustwordingscampagnes blijft het slachtoffercijfer stabiel. Dit roept vragen op over de effectiviteit van de huidige interventies. De centrale onderzoeksvraag van dit artikel luidt: Waarom blijven burgers slachtoffer worden van phishing, ondanks bestaande bewustwordingscampagnes en hoe kunnen deze interventies effectiever worden gemaakt? Het onderzoek is uitgevoerd in de vorm van een systematische literatuurstudie, gebaseerd op drie deelvragen: (1) welke psychologische mechanismen vergroten de kwetsbaarheid voor phishing, (2) hoe effectief zijn bestaande bewustwordingscampagnes in Nederland en internationaal, en (3) hoe verklaren gedragsmodellen zoals de Protection Motivation Theory (PMT) de kloof tussen weten en doen? De resultaten laten zien dat het succes van phishing diep verankerd is in menselijke psychologie: urgentie, autoriteit, gewoontegedrag en cognitieve biases spelen hierbij een centrale rol. Campagnes vergroten de kennis, maar leiden zelden tot blijvende gedragsverandering, doordat ze vaak te generiek, te rationeel en onvoldoende herhalend zijn. De conclusie is dat effectievere interventies een sterkere gedragsgerichte focus vereisen. Aanbevolen wordt om nudging-technieken te integreren, herhaalde phishing-simulaties met feedback toe te passen en campagnes doelgroepgericht vorm te geven. Duurzame en herhaalde strategieën zijn noodzakelijk om de hardnekkige kloof tussen bewustzijn en veilig gedrag te overbruggen.

1. Inleiding

Op een doordeweekse ochtend in januari 2021 ontving een echtpaar uit Breda een e-mail die ogenschijnlijk van hun bank afkomstig was. De boodschap leek betrouwbaar: het logo klopte, de aanhef was persoonlijk en de toon zakelijk. Er stond dat hun bankpas “om veiligheidsredenen” opnieuw geactiveerd moest worden via een beveiligde link. Zonder argwaan volgden ze de instructies. Binnen enkele minuten werden tientallen transacties uitgevoerd en hun rekeningen waren leeg. In totaal verloren ze ruim €300.000 aan wat later een geraffineerde phishingaanval bleek (Nu.nl, 2021).

Dit incident staat niet op zichzelf. Phishing vormt al jaren een van de meest voorkomende vormen van cybercriminaliteit en is een vast onderdeel van het digitale dreigingslandschap. Criminelen gebruiken e mails, sms-berichten, sociale media en telefoongesprekken om slachtoffers te verleiden gevoelige informatieprijs te geven

of geld over te maken. Door de professionalisering van criminele netwerken en de beschikbaarheid van phishingkits is het probleem in Nederland de laatste jaren sterk toegenomen (Internet Organised Crime Threat Assessment, 2024).

Volgens de Veiligheidsmonitor 2023 gaf 0,8% van de Nederlanders aan het voorgaande jaar slachtoffer te zijn geweest van phishing (CBS, 2024). Hoewel dit percentage klein lijkt, gaat het om honderdduizenden mensen, en veel slachtoffers melden het niet uit schaamte of omdat ze denken dat melden geen zin heeft. Ondanks forse investeringen van banken, overheid en politie in bewustwordingscampagnes zoals Echt Niet Vandaag en de voorlichtingsacties van de Nederlandse Vereniging van Banken (NVB) blijft het aantal slachtoffers nagenoeg gelijk. Dit wijst op een structurele kloof tussen weten en doen: burgers herkennen phishing wel, maar handelen in de praktijk vaak nog onveilig (Akkermans, Derksen, Kennis, Kloosterman, & Moons, 2024).

Dit onderzoek richt zich op de vraag waarom bewustwordingscampagnes tegen phishing onvoldoende gedragsverandering opleveren en hoe zij effectiever kunnen worden ingericht. Daarbij wordt gebruikgemaakt van de Protection Motivation Theory (PMT), die verklaart hoe perceptie van dreiging en vertrouwen in eigen kunnen bepalen of mensen beschermend gedrag vertonen. De resultaten bieden 1 handvatten voor effectiever beleid en praktische interventies die bijdragen aan duurzame digitale weerbaarheid in Nederland.

2. Theoretisch kader en literatuurverkenning

In dit hoofdstuk wordt de centrale onderzoeksvraag theoretisch onderbouwd. Er wordt ingegaan op psychologische mechanismen die de kwetsbaarheid voor phishing vergroten (paragraaf 2.1), de effectiviteit van bestaande bewustwordingscampagnes in Nederland en internationaal (paragraaf 2.2), en de verklaringen die gedragsmodellen bieden voor de kloof tussen weten en doen (paragraaf 2.3).

De hoofdvraag in dit onderzoek luidt: *Waarom blijven burgers slachtoffer worden van phishing, ondanks bestaande bewustwordingscampagnes, en hoe kunnen deze interventies effectiever worden gemaakt?*

Om deze hoofdvraag te beantwoorden, zijn de volgende deelvragen opgesteld:

1. Welke psychologische mechanismen vergroten de kwetsbaarheid voor phishing?
2. Hoe effectief zijn bestaande bewustwordingscampagnes in Nederland en internationaal?
3. Hoe verklaren gedragsmodellen zoals de Protection Motivation Theory (PMT) de kloof tussen weten en doen?

In de volgende paragrafen wordt deze driedeling gevolgd en wordt per thema de relevante wetenschappelijke literatuur besproken.

2.1 Psychologische mechanismen achter phishing

Phishing is geen puur technisch fenomeen, maar een sociale aanval die steunt op menselijke besluitvorming en gedragsmechanismen. Onderzoek toont aan dat aanvallers systematisch inspelen op bekende cognitieve biases en emoties om slachtoffers te manipuleren (Rayan & Marett, 2014).

Een eerste mechanisme is urgentie. Door druk uit te oefenen (“uw account wordt binnen 24 uur geblokkeerd”) wordt rationele besluitvorming omzeild. Gebruikers ervaren stress en nemen impulsieve beslissingen. Urgentie versterkt ook het gevoel van schaarste, een bekend beïnvloedingsprincipe (Cialdini, 2009). Daarnaast speelt autoriteit een grote rol. Wanneer e-mails lijken te komen van banken, de Belastingdienst of grote technologiebedrijven, zijn burgers eerder geneigd te gehoorzamen. Autoriteit vergroot daarmee de kans dat verzoeken zonder kritisch nadenken worden opgevolgd (Williams, Hinds, & Joinson, 2018). Gewoontegedrag en routine zijn eveneens belangrijke factoren. Mensen klikken vaak routinematig op links in e-mails, zelfs wanneer zij training hebben ontvangen. Routine verlaagt alertheid en maakt dat subtiele signalen van phishing over het hoofd worden gezien (Starman, Bell, Auton, Brakey, & Wiggins, 2024). Ook verschillende cognitieve biases verhogen de kwetsbaarheid. De optimism bias en overconfidence effect zorgen ervoor dat burgers hun eigen weerbaarheid overschatten (“ik trap daar niet in”) (Hadlington, 2017). De availability heuristic verklaart waarom alertheid tijdelijk toeneemt na nieuws over phishing, maar daarna snel weer inzakt. Daarnaast speelt loss aversion (verlies weegt zwaarder dan winst) een belangrijke rol: dreigingen als “uw tegoed wordt verwijderd” hebben extra effect (Tversky & Kahneman, 1991). Ten slotte is er emotionele manipulatie. Emoties als angst, nieuwsgierigheid en hebzucht worden vaak aangesproken. Tijdens de coronapandemie werden phishingmails verstuurd over vaccins en steunmaatregelen, die inspeelden op angst en onzekerheid (Internet Organised Crime Threat Assessment, 2024). Deze mechanismen maken duidelijk dat phishing diep in menselijke psychologie verankerd is. Zoals in hoofdstuk 4 zal blijken, verklaart dit waarom bewustwordingscampagnes die zich uitsluitend richten op kennis vaak falen.

2.2 Effectiviteit van bewustwordingscampagnes

Bewustwordingscampagnes zijn een centraal instrument in het bestrijden van phishing. Ze richten zich op het vergroten van kennis en alertheid onder burgers. Toch is de effectiviteit van dergelijke campagnes beperkt. In Nederland is de campagne Echt Niet Vandaag een prominent voorbeeld. Banken benadrukken hierin dat zij nooit vragen om pincodes of overboekingen. Veel Nederlanders kennen de slogan, maar in praktijksituaties bleek dit onvoldoende om veilig gedrag te garanderen. Burgers reageerden alsnog impulsief bij realistische phishingpogingen.

Internationaal zien we vergelijkbare patronen. In het Verenigd Koninkrijk wordt via de campagne Take Five to Stop Fraud benadrukt dat burgers “vijf seconden moeten nadenken” voordat ze reageren. Hoewel de campagne brede bekendheid geniet, rapporteerde UK Finance dat de verliezen door phishing niet substantieel

afnamen (ANNUAL FRAUD REPORT). In de Verenigde Staten voert de Federal Trade Commission (FTC) grootschalige campagnes, maar volgens cijfers van het FBI Internet Crime Complaint Center blijft phishing daar de meest gemelde cybercrime (FBI San Francisco, 2024).

Wetenschappelijke studies bevestigen dit beeld. Martens, De Wolf en De Marez laten zien dat kennisgerichte campagnes wel leiden tot meer herkenning, maar dat gedragsverandering uitblijft. Canield, Fischhoff en Davis benadrukken dat interventies die gebruikers actief confronteren met phishing, zoals simulaties, significant effectiever zijn (Canield, Fischhoff, & Davis, 2016). Een belangrijk knelpunt is dat campagnes vaak een generiek publiek aanspreken. Zij houden te weinig rekening met specifieke doelgroepen zoals ouderen, jongeren of laaggeletterden, die elk andere kwetsbaarheden hebben. Daarnaast ontbreekt vaak structurele herhaling, campagnes zijn vaak incidenteel, terwijl gedragsverandering continu onderhoud vraagt.

2.3 Gedragsmodel en de kloof tussen weten en doen

Om te begrijpen waarom bewustwordingscampagnes over phishing vaak beperkt effectief zijn, biedt de Protection Motivation Theory (PMT) van Rogers een bruikbaar kader. Deze theorie verklaart waarom mensen, ondanks kennis van risico's, toch onveilig gedrag vertonen. Volgens PMT wordt beschermend gedrag bepaald door twee denkprocessen:

1. Threat appraisal: de inschatting van hoe ernstig en waarschijnlijk de dreiging is.
2. Coping appraisal: het vertrouwen dat men de dreiging effectief kan aanpakken. Pas wanneer iemand zowel de dreiging hoog inschat als gelooft dat hij iets kan doen, is de kans groot dat hij veilig handelt (Marikyan & Papagiannidis, 2025).

Phishers spelen bewust in op de threat appraisal door urgentie, autoriteit en verliesframes te gebruiken ("uw rekening wordt vandaag geblokkeerd"). Hierdoor stijgt het gevoel van dreiging, maar blijft vaak weinig tijd over voor rationeel handelen (Tversky & Kahneman, 1991) (Rayan & Marett, 2014).

Onderzoek toont echter dat een hoge dreigingsperceptie niet automatisch tot veilig gedrag leidt, maar dat angst zonder handelingsperspectief juist kan leiden tot stress of vermijding. Daarom is de coping appraisal cruciaal. Deze omvat drie factoren:

1. Response efficacy: het geloof dat de aanbevolen actie werkt.
 2. Self-efficacy: het vertrouwen dat men dit zelf kan uitvoeren.
 3. Response costs: de moeite of onzekerheid die veilig handelen kost.
- Campagnes vergroten vaak de dreiging, maar niet deze copingfactoren. Burgers weten wel dat phishing gevaarlijk is, maar niet precies wat ze moeten doen. Dit gebrek aan handelingsperspectief leidt tot uitstel of impulsief klikken, een patroon dat PMT voorspelt. De Nederlandse campagne Echt Niet Vandaag illustreert dit: veel mensen herkenden phishing, maar wisten niet waar ze konden melden of hoe ze een

bericht konden verifiëren. Dit leverde bewustzijn op, maar nauwelijks gedragsverandering. Effectieve campagnes zouden zich daarom moeten richten op het versterken van self-efficacy (via realistische phishing-simulaties en feedback), het verhogen van response efficacy (door te tonen dat melden werkt) en het verlagen van response costs (bijvoorbeeld via een “Meld phishing”-knop of automatische waarschuwingen). Daarnaast is een doelgroepgerichte benadering noodzakelijk. Ouderen hebben baat bij duidelijke, stapsgewijze instructies, terwijl jongeren beter reageren op interactieve of geïntegreerde digitale oplossingen (Brandley-Beil, Coventry, Dixon, Joinson, & Briggs, 2022).

Samenvattend verklaart de PMT dat de kloof tussen weten en doen vooral ontstaat door een tekort aan handelingsperspectief en zelfvertrouwen. Dreiging zonder praktische houvast leidt tot angst en vermijding, terwijl dreiging met handelingsmogelijkheden juist tot actie aanzet. Voor effectieve phishingpreventie is het daarom essentieel dat campagnes zich niet alleen richten op risico's, maar vooral op het versterken van coping appraisal, zodat veilig handelen vanzelfsprekend wordt.

3. Methoden

In dit onderzoek is gekozen voor een secundaire analyse van bestaande datasets en evaluatierapporten waarin slachtofferschap van phishing en de effectiviteit van bewustwordingscampagnes centraal staan. De kern van de Nederlandse data is afkomstig uit de Veiligheidsmonitor 2023 van het Centraal Bureau voor de Statistiek. Voor internationale vergelijking zijn meldingsdata gebruikt van het FBI Internet Crime Complaint Center en van UK Finance. Deze databronnen zijn gekozen vanwege hun representativiteit en betrouwbaarheid en bieden gezamenlijk inzicht in zowel de prevalentie, de impact als de effectiviteit van campagnes.

3.1 Participanten

De CBS Veiligheidsmonitor 2023 heeft een steekproef van circa 32.000 Nederlanders van 15 jaar en ouder. Van deze respondenten gaf 0,8% aan in de afgelopen twaalf maanden slachtoffer te zijn geweest van phishing (CBS, 2024). Dit percentage lijkt klein, maar omgerekend naar de gehele bevolking gaat het om enkele honderdduizenden slachtoffers. De dataset bevat demografische variabelen zoals leeftijd, geslacht, opleidingsniveau en woonplaats, die analyses van risicogroepen mogelijk maken.

De internationale datasets zijn groter maar verschillen qua participanten. Het FBI IC3-rapport 2023 is gebaseerd op meer dan 300.000 meldingen van phishing in de Verenigde Staten, waarvan ongeveer 40% door ouderen werd gedaan. De financiële schade liep uiteen van enkele tientallen dollars tot meer dan \$100.000 per incident (FBI San Francisco, 2024). UK Finance analyseerde in 2022 ruim 195.000 meldingen van consumenten en bedrijven, waarbij zowel directe schade als psychologische impact in kaart werd gebracht (ANNUAL FRAUD REPORT).

3.2 Operationalisatie

De variabelen uit de verschillende datasets zijn gehercodeerd en geordend naar vier impactcategorieën die in de literatuur vaak worden gebruikt: emotioneel/psychisch, lichamelijk/fysiek, sociaal/gedragsmatig en financieel/materieel (Lee, Kang, & Kim, 2023). In de CBS Veiligheidsmonitor werd bijvoorbeeld gevraagd of slachtoffers last hadden van angst, boosheid of slaapproblemen na een cybercrime-incident. Deze werden gecodeerd als emotionele en lichamelijke gevolgen. Het verlies van vertrouwen in anderen en het vermijden van onlineactiviteiten vielen onder sociale gevolgen. Financiële schade werd gemeten in euro's en gekoppeld aan meldgedrag (bijvoorbeeld of slachtoffers compensatie ontvingen van bank of verzekering) (CBS, 2024).

De IC3-dataset rapporteerde vooral financiële en materiële schade, maar ook 'tijdverlies' door herstelacties (FBI San Francisco, 2024). UK Finance verzamelde aanvullende gegevens over psychologische en gedragsmatige effecten, zoals schaamte, wantrouwen en veranderingen in online koopgedrag (ANNUAL FRAUD REPORT). Voor de evaluatie van Echt Niet Vandaag lag de nadruk op gedragsuitkomsten: klikgedrag, het doorgeven van inloggegevens en meldingsbereidheid. Deze zijn geoperationaliseerd als indicatoren van weerbaarheid in praktijksituaties.

3.3 Analyse van behoeften

Naast impact is gekeken naar de behoeften van slachtoffers. In de CBS Veiligheidsmonitor werd gevraagd naar informatiebehoefte, steunbehoefte en meldgedrag. Hierbij kwamen terugkerende thema's naar voren zoals opsporing en bestraffing van de dader, emotionele steun, praktische hulp bij schadeherstel en preventietips (CBS, 2024). Factoranalyse in eerdere studies laat zien dat deze behoeften vaak te groeperen zijn in drie dimensies: vergelding, preventie en ondersteuning (Reanaud, Flowerday, Warkentin, Cockshott, & Orgeron, 2018) (Canield, Fischhoff, & Davis, Quantifying Phishing Susceptibility for Detection and Behavior Decisions, 2016). De evaluatie van Echt Niet Vandaag onderzocht in hoeverre de campagne deze behoeften adresseerde. Uit de resultaten bleek dat burgers de slogan wel kenden, maar dat zij vaak geen handelingsperspectief ervoeren. De behoefte aan concrete, praktische tips en directe feedback na phishingpogingen bleef daardoor grotendeels on vervuld.

3.4 Betrouwbaarheid en validiteit

De betrouwbaarheid van de gebruikte data is hoog, aangezien alle datasets afkomstig zijn van gerenommeerde instituten (CBS, FBI, UK Finance). Validiteit is versterkt door triangulatie van verschillende bronnen: surveydata, meldingsdata en campagnestudies. Toch zijn er beperkingen. Zelfrapportages in surveys zijn gevoelig voor onderrapportage door schaamte. Bij de IC3 en UK Finance-data is sprake van meldingsbias: niet iedereen doet aangifte of melding. Verder zijn veel internationale

studies context gebonden: resultaten uit de VS en het VK zijn niet altijd generaliseerbaar naar de Nederlandse situatie.

3.5 Reflectie

Het gebruik van secundaire data is passend gezien de gevoeligheid van het onderwerp. Experimenteel onderzoek met echte slachtoffers zou ethisch problematisch zijn. Wel onderstreept dit onderzoek de noodzaak van aanvullend empirisch werk. Vooral longitudinale studies naar de effecten van herhaalde phishing-simulaties en naar de rol van sociale normen in Nederland zijn dringend gewenst.

4. Resultaten

De resultaten van dit onderzoek zijn geordend langs de drie deelvragen die in hoofdstuk 2 zijn opgesteld. Waar mogelijk zijn de bevindingen vergeleken tussen Nederlandse en internationale datasets, en gekoppeld aan bestaande literatuur. Dit hoofdstuk bespreekt achtereenvolgens de psychologische mechanismen die de kwetsbaarheid voor phishing vergroten (paragraaf 4.1), de effectiviteit van bewustwordingscampagnes (paragraaf 4.2) en de verklaringen die gedragsmodellen bieden voor de kloof tussen weten en doen (paragraaf 4.3).

4.1 Psychologische mechanismen (deelvraag 1)

Uit de analyse blijkt dat phishing zijn succes grotendeels dankt aan psychologische mechanismen die diep in menselijk gedrag verankerd zijn. In zowel Nederlandse surveydata als internationale literatuur keren dezelfde factoren terug (CBS, 2024) (Rayan & Marett, 2014; Williams, Hinds, & Joinson, 2018). Urgentie is een van de meest dominante mechanismen. In meldingen bij het FBI IC3 werd vaak aangegeven dat slachtoffers haast voelden door zinnen als “uw account wordt binnen 24 uur geblokkeerd”. Dit mechanisme wordt versterkt door verliesaversie: mensen zijn gevoeliger voor mogelijk verlies (toegang tot account, geld) dan voor potentiële winst (Tversky & Kahneman, 1991). Daarnaast speelt autoriteit een doorslaggevende rol. Uit experimenten van Williams blijkt dat e-mails die lijken te komen van banken of de Belastingdienst driemaal vaker worden geopend en beantwoord dan neutrale berichten (Williams, Hinds, & Joinson, 2018). Ook bij Echt Niet Vandaag werd zichtbaar dat burgers vooral gevoelig waren voor mails die visueel sterk leken op communicatie van hun bank. Gewoontegedrag vormt een ander risico. Mensen klikken routinematig op links, zelfs wanneer zij training hadden ontvangen. Dit patroon werd ook zichtbaar in de IC3-meldingen, waar veel slachtoffers aangaven “gewoon” te hebben doorgeklikt zonder na te denken. Verder wijzen meerdere studies op cognitieve biases. Zo zorgt optimism bias ervoor dat mensen hun eigen kwetsbaarheid onderschatten (“ik trap daar niet in”), terwijl availability heuristic verklaart dat alertheid slechts tijdelijk toeneemt na nieuwsberichten over phishing (Tversky & Kahneman, 1991). Ten slotte spelen emoties zoals angst,

nieuwsgierigheid en schaamte een rol. Tijdens de coronapandemie rapporteerde Europol (Internet Organised Crime Threat Assessment, 2024) een toename van phishingberichten die inspeelden op angst en onzekerheid over vaccins of steunmaatregelen. Dit bevestigt dat phishing niet slechts een rationeel probleem is, maar een emotioneel geladen aanvalsvorm. Samenvattend laten de data zien dat psychologische mechanismen elkaar versterken. Urgentie en autoriteit verkleinen de ruimte voor kritische reflectie, terwijl gewoontegedrag en biases alertheid verder verminderen. Dit verklaart waarom slachtoffers ondanks kennis toch handelen tegen hun eigen voornemens in.

4.2 Effectiviteit van bewustwordingscampagnes (deelvraag 2)

In Nederland was de campagne Echt Niet Vandaag weliswaar breed bekend mensen herkende de slogan, maar in praktijksimulaties klikte een aanzienlijk deel nog steeds op phishinglinks. Dit bevestigt dat kennis niet automatisch leidt tot veilig gedrag. In het Verenigd Koninkrijk rapporteerde UK Finance vergelijkbare bevindingen rond de campagne Take Five to Stop Fraud. Hoewel veel burgers de boodschap kenden, daalden de verliezen door phishing nauwelijks. In de VS tonen de IC3-data dat phishing ook in 2023 de meest gerapporteerde cybercrimevorm bleef, ondanks langdurige investeringen in grootschalige FTC-campagnes (FBI San Francisco, 2024). Wetenschappelijke literatuur ondersteunt dit beeld. Martens, De Wolf en De Marez vonden dat kennisgerichte campagnes wel de herkenning van phishing vergroten, maar dat gedragsverandering uitblijft. Canield, Fischhoff en Davis benadrukken dat simulaties en feedback veel effectiever zijn. Een belangrijk knelpunt is de generieke aanpak van campagnes. Specifieke doelgroepen zoals ouderen, jongeren en laaggeletterden hebben elk andere kwetsbaarheden, maar campagnes richten zich vaak op “de burger” in het algemeen. Dit verklaart mede waarom het slachtoffercijfer in Nederland al jaren rond de 0,8% blijft hangen (CBS, 2024). Samengevat leveren bewustwordingscampagnes vooral cognitieve winst op (herkenning), maar weinig gedragswinst (veilig handelen).

4.3 Gedragsmodellen en de kloof tussen weten en doen (deelvraag 3)

De resultaten laten zien dat de Protection Motivation Theory (PMT) goed verklaart waarom kennis over phishing niet automatisch leidt tot veilig gedrag. Volgens PMT wordt beschermend gedrag bepaald door twee processen namelijk Threat appraisal en Coping appraisal. Alleen wanneer beide hoog zijn, volgt beschermend gedrag, zoals het niet openen van verdachte links of het melden van phishing.

Threat appraisal. Uit de CBS Veiligheidsmonitor (CBS, 2024) blijkt dat de meeste Nederlanders phishing als een groot risico zien. Toch blijven veel mensen kwetsbaar. In de IC3- (FBI San Francisco, 2024) en UK Finance-data (ANNUAL FRAUD REPORT) meldden slachtoffers dat zij berichten vertrouwden vanwege urgentie of officiële opmaak. Dit wijst erop dat een hoge risicoperceptie op zichzelf niet genoeg is: mensen voelen de dreiging wel, maar weten niet goed wat ze moeten

doen. PMT voorspelt dat een hoge dreiging zonder handelingsperspectief juist kan leiden tot stress of vermijding.

Coping appraisal. Er is gebrek aan handelingsperspectief. Hoewel veel mensen de campagne Echt niet vandaag herkenden, wist slechts een klein deel hoe ze phishing effectief konden melden of controleren. Dit duidt op lage self efficacy en beperkte response efficacy. Implicaties Campagnes die vooral angst oproepen zonder concrete handelingsopties te bieden, blijken ineffectief of zelfs contraproductief. PMT laat zien dat juist de coping appraisal cruciaal is: mensen moeten niet alleen weten dat phishing gevaarlijk is, maar ook voelen dat ze iets kunnen doen. Daarom moeten campagnes inzetten op:

1. Oefening en feedback om self-efficacy te versterken.
2. Duidelijke uitleg over waarom veilig handelen werkt (response efficacy).
3. Eenvoudige meldsystemen die de drempel verlagen (lage response costs).

Samenvattend

De kloof tussen weten en doen ontstaat omdat veel campagnes de dreiging vergroten, maar het handelingsvermogen van burgers onvoldoende versterken. Volgens de PMT is effectieve gedragsverandering pas mogelijk wanneer mensen niet alleen bewust zijn van het risico, maar ook vertrouwen hebben in hun eigen vermogen om het te voorkomen.

5 Conclusie en discussie

5.1 Conclusie

De centrale onderzoeksvraag luidde: Waarom blijven burgers slachtoffer worden van phishing, ondanks bestaande bewustwordingscampagnes, en hoe kunnen deze interventies effectiever worden gemaakt? Uit dit onderzoek blijkt dat het hardnekkige karakter van phishing niet te verklaren is door onwetendheid, maar door een gebrek aan gedragsmatige weerbaarheid. Burgers weten vaak wel wat phishing is, maar handelen daar in stressvolle situaties niet naar. De oorzaak daarvan ligt op drie niveaus.

Ten eerste tonen de psychologische mechanismen (hoofdstuk 4.1) aan dat menselijke emoties en denkpatronen zoals urgentie, autoriteit, gewoontegedrag en rationele besluitvorming onder druk zetten. Deze automatische reacties maken dat mensen impulsief handelen, zelfs als ze risico's herkennen.

Ten tweede blijkt uit de analyse van bewustwordingscampagnes (hoofdstuk 4.2) dat kennis wel wordt vergroot, maar gedrag nauwelijks verandert. Campagnes zijn vaak te generiek, eenmalig en vooral informatief, terwijl gedrag vraagt om herhaling, oefening en context. Ten derde verklaart de Protection Motivation Theory (PMT) (hoofdstuk 4.3) waarom deze kloof tussen weten en doen blijft bestaan.

Campagnes vergroten vooral de dreigingsperceptie (threat appraisal), maar versterken zelden het vertrouwen dat men iets *kán* doen (coping appraisal). Angst zonder handelingsperspectief leidt tot passiviteit in plaats van actie. De kernconclusie

luit daarom dat effectieve phishingpreventie niet begint bij meer informatie, maar bij meer handelingsvermogen. Campagnes moeten burgers niet alleen waarschuwen, maar hen leren handelen door vertrouwen, feedback en eenvoud centraal te stellen. Alleen door het versterken van self efficacy, response efficacy en het verlagen van response costs kunnen interventies leiden tot duurzame gedragsverandering. Met andere woorden: bewustwording is een voorwaarde, maar geen garantie voor veiligheid. Pas wanneer veilig gedrag de makkelijke, automatische keuze wordt, kan de samenleving structureel weerbaarder worden tegen phishing.

5.2 Discussie

De resultaten van dit onderzoek laten zien dat phishing in Nederland niet alleen een technisch, maar vooral een gedragsmatig probleem is. Ondanks jarenlange investeringen in bewustwordingscampagnes blijft het aantal slachtoffers nagenoeg gelijk. Dit bevestigt dat de huidige preventiestrategieën te eenzijdig zijn gericht op kennis en waarschuwingen, terwijl gedragsverandering juist wordt bepaald door motivatie, handelingsperspectief en vertrouwen in eigen kunnen. Vanuit de Protection Motivation Theory (PMT) blijkt dat veel campagnes wel de dreiging benadrukken, maar te weinig aandacht besteden aan coping appraisal, het geloof dat mensen daadwerkelijk iets kunnen doen om zich te beschermen. Dit gebrek aan handelingsperspectief verklaart waarom burgers ondanks bewustzijn toch risicovol gedrag vertonen.

Campagnes die angst aanwakken zonder concrete handelingsopties te bieden, kunnen zelfs averechts werken en leiden tot vermijding of desinteresse. Voor beleid en praktijk betekent dit dat de nadruk moet verschuiven van angstcommunicatie naar handelingsgerichte ondersteuning. Banken en overheden zouden meer moeten investeren in gedragsinterventies die self-efficacy en response efficacy versterken, bijvoorbeeld via korte phishingsimulaties met directe feedback, of door veilig handelen eenvoudiger te maken dan risicovol handelen. Daarnaast is doelgroep differentiatie essentieel: ouderen profiteren van duidelijke visuele instructies, terwijl jongeren beter reageren op automatische beveiligingsopties in digitale platforms.

Ook vraagt dit om een herziening van de nationale cyberweerbaarheidsstrategie. In plaats van bewustwording als einddoel te zien, zou het beleid zich moeten richten op duurzaam veilig gedrag. Dit kan door gedragsmodellen zoals PMT structureel te integreren in campagneontwikkeling, onderwijs en publiekscommunicatie.

Samenvattend tonen de bevindingen aan dat kennisoverdracht alleen niet voldoende is om phishing te verminderen. Effectieve preventie vraagt om een gedragsgerichte benadering waarin handelingsperspectief, motivatie en vertrouwen centraal staan, een verschuiving van informeren naar activeren.

5.3 Aanbevelingen

Op basis van de resultaten van dit onderzoek kunnen verschillende aanbevelingen worden gedaan om bewustwordingscampagnes tegen phishing effectiever te maken.

De bevindingen laten zien dat kennisvergroting alleen onvoldoende is om duurzaam veilig gedrag te stimuleren. Campagnes en beleid zouden daarom sterker moeten inspelen op gedragsverandering en handelingsperspectief.

Ontwikkel gedragsgerichte campagnes. Bewustwordingsinitiatieven dienen niet alleen te informeren, maar vooral te activeren. Gebruik gedragsinterventies zoals nudging, herhaling en positieve feedback om gewenst gedrag te versterken. Campagnes die inspelen op gewoontegedrag en emoties blijken effectiever dan rationele waarschuwingen.

Implementeer phishing-simulaties met directe feedback. Herhaalde, realistische phishingtests helpen burgers om hun handelingsvaardigheden te oefenen en zelfvertrouwen op te bouwen (self-efficacy). Feedbackmomenten na een simulatie vergroten bovendien het inzicht in kwetsbaar gedrag en versterken de leerervaring.

Pas communicatie aan op specifieke doelgroepen. Effectieve interventies houden rekening met verschillen in leeftijd, digitale geletterdheid en context. Ouderen hebben baat bij duidelijke, visuele instructies; jongeren reageren beter op interactieve of gamified vormen van bewustwording. Campagnes moeten daarom modulair en doelgroepgericht worden ontworpen.

Verlaag de drempel om veilig te handelen. Vergroot de response efficacy door burgers praktische hulpmiddelen te bieden, zoals een geïntegreerde “Meld phishing”-knop, automatische waarschuwingen in e-mailclients of snelle meldingsprocedures bij banken en overheidsdiensten. Veilig handelen moet eenvoudiger zijn dan risicovol klikken.

Verschuif beleidsfocus van kennis naar gedrag. Cyberweerbaarheidsbeleid zou minder nadruk moeten leggen op kennisoverdracht en meer op duurzaam gedrag. Door gedragsmodellen zoals de Protection Motivation Theory structureel te integreren in communicatie en onderwijs, kan veilig digitaal handelen de standaard worden in plaats van de uitzondering.

Literatuurlijst

- Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024, Maart 1). Veiligheidsmonitor 2023. Opgeroepen op Oktober 2025, van Centraal Bureau voor de Statistiek: <https://www.cbs.nl/nl/nl/longread/rapportages/2024/veiligheidsmonitor-2023/5-online-criminaliteit>
- ANNUAL FRAUD REPORT. (sd). Opgeroepen op Oktober 2025, van UK Finance: https://www.ukfinance.org.uk/system/files/202305/Annual%20Fraud%20Report%202023_0.pdf
- Brandley-Beil, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022, Oktober 21). Exploring Age and Gender

Differences in ICT Cybersecurity Behaviour. Opgeroepen op Oktober 2025, van Wiley Online Library: <https://onlinelibrary.wiley.com/doi/10.1155/2022/2693080>

Canfield, C. I., Fischho , B., & Davis, A. (2016, Augustus 25). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Opgeroepen op Oktober 2025, van Sage Journals: <https://journals.sagepub.com/doi/10.1177/0018720816665025>

CBS. (2024, Maart 1). Veiligheidsmonitor 2023. Opgeroepen op Oktober 2025, van Centraal Bureau voor de Statistiek: <https://download.cbs.nl/maatwerk/Veiligheidsmonitor-2023.pdf>

Cialdini, R. B. (2009). Influence: Science and practice (5th ed.). In R. B. Cialdini, Influence: Science and practice (5th ed.) (p. 254). Boston: Pearson Education. FBI San Francisco. (2024, April 4).

Federal Bureau of Investigation Internet Crime Report 2023. Opgeroepen op Oktober 2025, van FBI: https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Hadlington, L. (2017, Juli 5). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Opgeroepen op Oktober 2025, van Heliyon A Cell Press journal: [https://www.cell.com/heliyon/fulltext/S2405-8440\(17\)309982?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844017309982%3Fshowall%3Dtrue](https://www.cell.com/heliyon/fulltext/S2405-8440(17)309982?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2405844017309982%3Fshowall%3Dtrue)

Internet Organised Crime Threat Assessment. (2024, Juli 22). Opgeroepen op Oktober 2025, van Europol: <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf> Lee, S.-

H., Kang, I., & Kim, H.-w. (2023, September 15). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? Opgeroepen op Oktober 2025, van ScienceDirect: <https://www.sciencedirect.com/science/article/abs/pii/S0160791X23001665>

Marikeyan, D., & Papagiannidis, S. (2025, Juni 20). Protection Motivation Theory (PMT). Opgeroepen op Oktober 2025, van TheoryHub: <https://open.ncl.ac.uk/theories/10/protection-motivation-theory/>

Nu.nl. (2021, November 10). Bredaas echtpaar via phishing bestolen van 3 ton, veertien verdachten opgepakt. Opgeroepen op Oktober 2025, van Nu.nl:

<https://www.nu.nl/tech/6166991/bredaas-echtpaar-via-phishing-bestolen-van-3-ton-veertien-verdachten-opgepakt.html>

Rayan, W. T., & Marett, K. (2014, December 8). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Opgeroepen op Oktober 2025*, van Taylor & Francis: <https://www.tandfonline.com/doi/abs/10.2753/MIS0742-1222270111>

Reanaud, K., Flowerday, S., Warkentin, M., Cockshott, P., & Orgeron, C. (2018, Juli 27). Is de verantwoording voor cyberbeveiligingsrisico's redelijk en verstandig? *Opgeroepen op Oktober 2025*, van ScienceDirect: <https://www.sciencedirect.com/science/article/abs/pii/S0167404818303262?via%3Dihub>

Starman, D., Bell, E. A., Auton, J. C., Brakey, G. R., & Wiggins, M. W. (2024, Mei 9). The roles of phishing knowledge, cue utilization, and decision styles in phishing email detection. *Opgeroepen op Oktober 2025*, van ScienceDirect: <https://www.sciencedirect.com/science/article/pii/S0003687024000863>

Tang, J. (2018, Oktober 15). Exploring the relationships between gamification and motivational needs in technology design. *Opgeroepen op Oktober 2025*, van Emerald insight: <https://www.emerald.com/ijcs/article/media/115826/pdfviewer/773701>

Tversky, A., & Kahneman, D. (1991, November 1). Loss Aversion in Riskless Choice: A Reference-Dependent Model. *Opgeroepen op Oktober 2025*, van Oxford Academic: <https://academic.oup.com/qje/article/abstract/106/4/1039/1873382?redirectedFrom=fulltext&login=false>

Williams, E. J., Hinds, J., & Joinson, A. N. (2018, Juli 19). Exploring susceptibility to phishing in the workplace. *Opgeroepen op Oktober 2025*, van ScienceDirect: <https://researchinformation.bris.ac.uk/ws/portalfiles/portal/176333279/susceptability.pdf>

Artikelen democratische rechtsstaat

Van online narratief naar radicale overtuiging

Jordy Kortink

Master Veiligheid en Digitalisering, Hogeschool Saxion

1.. Inleiding

Auteursnoot: De inhoud van dit artikel komt volledig voor rekening van de auteur. Hoewel de auteur werkzaam is bij de Nationale Politie, weerspiegelt dit artikel niet noodzakelijkerwijs de standpunten, beleidsopvattingen of officiële communicatie van de Nationale Politie. Bij het opstellen van dit artikel is gebruikgemaakt van AI-ondersteuning, specifiek ChatGPT van OpenAI (2026), voor het herformuleren van zinnen en taalcontrole. De inhoudelijke analyse en conclusies zijn volledig door de onderzoeker zelf opgesteld.

Online radicalisering vormt een groeiende uitdaging binnen de Nederlandse samenleving, waarbij online omgevingen een steeds belangrijkere rol spelen in de verspreiding en versterking van anti-institutionele overtuigingen. Online platforms maken het mogelijk om laagdrempelig toegang te krijgen tot alternatieve narratieven en contact te leggen met gelijkgestemden, waardoor overtuigingen collectief kunnen worden versterkt. In de literatuur wordt beschreven dat dergelijke processen kunnen bijdragen aan groepsvorming, polarisatie en ideologische verharding (Chen et al., 2021; Sunstein, 2002; Van Halderen et al., 2024). Wanneer het vertrouwen in overheid en andere instituties structureel afneemt, kan dit de legitimiteit van overheidsoptreden aantasten en de democratische rechtsstaat onder druk zetten (Algemene Inlichtingen- en Veiligheidsdienst [AIVD], 2023).

Tegen de achtergrond van digitalisering, online radicalisering en toenemend institutioneel wantrouwen vormt de soevereinenbeweging een relevante casus voor de politiepraktijk. Binnen deze beweging staat het idee centraal dat de overheid en haar instituties hun legitimiteit hebben verloren (AIVD, 2023). De beweging kent geen eenduidig profiel, maar onderzoek laat zien dat het relatief vaak gaat om mannen van middelbare leeftijd die in eerdere fasen van hun leven negatieve ervaringen hebben gehad met overheidsinstanties, bijvoorbeeld op juridisch of financieel gebied (Verwey-Jonker Instituut & RadarAdvies, 2025). Deze ervaringen kunnen bijdragen aan een groeiend wantrouwen richting de overheid en vormen regelmatig een voedingsbodem voor het omarmen van alternatieve juridische en politieke overtuigingen.

In tegenstelling tot zogenoemde 'zelfontbranders', die vaak op jongere leeftijd en in korte tijd radicaliseren, lijkt binnen de soevereinenbeweging vaker sprake van een geleidelijk proces waarin persoonlijke ervaringen, online informatie en groepsdynamiek elkaar versterken. Radicaliseringsprocessen binnen deze beweging

kunnen daarom niet uitsluitend online of offline worden begrepen, maar ontstaan juist in de wisselwerking tussen beide domeinen.

Tegen deze achtergrond staat in dit onderzoek de vraag centraal hoe online omgevingen bijdragen aan radicaliseringsprocessen onder aanhangers van de soevereinenbeweging en welke implicaties dit heeft voor de rol van de politie in het signaleren en adresseren van deze processen.

2. Onderzoeksvragen

Op basis van de geschetste ontwikkelingen rondom digitalisering, online radicalisering en de opkomst van de soevereinenbeweging richt dit onderzoek zich op de relatie tussen online omgevingen en radicaliseringsprocessen. Daarbij ligt de focus op de wijze waarop online platforms bijdragen aan de verspreiding en versterking van ideologische narratieven onder aanhangers van de soevereinenbeweging. Op basis van de verkregen inzichten worden in de discussie en conclusie implicaties voor de politiepraktijk geformuleerd.

De centrale onderzoeksvraag luidt: *Hoe dragen online omgevingen bij aan radicaliseringsprocessen onder aanhangers van de soevereinenbeweging en welke implicaties heeft dit voor de rol van de politie in het omgaan met online radicalisering?*

Om deze vraag te beantwoorden worden de volgende deelvragen gehanteerd:

1. Welke kenmerken en ideologische narratieven kenmerken de soevereinenbeweging?
2. Welke mechanismen van online radicalisering worden in de literatuur beschreven?
3. Welke rol spelen digitale platforms en online gemeenschappen in de verspreiding, bevestiging en versterking van radicaliseringsprocessen onder aanhangers van de soevereinenbeweging?

Deze deelvragen structureren de analyse in dit onderzoek en vormen de basis voor zowel de literatuurstudie als het expertinterview.

3. Methodologie

Dit onderzoek richt zich op het verkrijgen van inzicht in de rol van online omgevingen bij radicaliseringsprocessen onder aanhangers van de soevereinenbeweging en de implicaties hiervan voor de politie. Gezien het verkennende en verklarende karakter van de onderzoeksvraag is gekozen voor een kwalitatieve onderzoeksopzet. Een kwalitatieve benadering maakt het mogelijk om onderliggende mechanismen, interpretaties en betekenissen te analyseren die ten grondslag liggen aan complexe sociale processen zoals radicalisering (Baarda et al., 2021). Deze benadering sluit aan bij het doel van dit onderzoek om radicaliseringsprocessen in hun sociale en digitale context te begrijpen.

Het onderzoek heeft een interdisciplinair karakter en combineert inzichten uit de sociologie, psychologie en veiligheidsstudies. Vanuit de sociologie wordt aandacht besteed aan groepsvorming en sociale netwerken, vanuit de psychologie aan

complotdenken, identiteitsvorming en groepspolarisatie, en vanuit de veiligheidsstudies aan radicalisering en de implicaties voor de democratische rechtsstaat. Deze combinatie van disciplines maakt het mogelijk om zowel individuele als structurele aspecten van online radicalisering te analyseren.

Het onderzoek bestaat uit een literatuurstudie en een expertinterview. De literatuurstudie vormt de basis van het theoretisch kader en richt zich op online radicalisering, digitale platforms, complotdenken en de soevereinenbeweging. In databanken zoals Google Scholar en via de Saxion-bibliotheek is gezocht naar wetenschappelijke publicaties met zoektermen als online radicalization, echo chambers, algorithmic amplification, conspiracy theories, sovereign citizens en institutional distrust. Bij de selectie is prioriteit gegeven aan peer-reviewed artikelen, recente publicaties en bronnen die direct relevant zijn voor de onderzoeksvraag. Daarnaast zijn gezaghebbende Nederlandse beleids- en onderzoeksrapporten gebruikt, waaronder publicaties van de AIVD en het WODC-onderzoek van Verwey-Jonker Instituut en RadarAdvies.

Aanvullend op de literatuurstudie is een semigestructureerd expertinterview uitgevoerd met een geanonimiseerde politieprofessional met ervaring op het gebied van radicalisering, extremisme en informatiegestuurd politiewerk (persoonlijke communicatie, 18 maart 2026). Het doel van dit interview was om de bevindingen uit de literatuur te toetsen aan praktijkervaringen en deze waar nodig te verdiepen en te nuanceren. Expertinterviews kunnen waardevolle contextuele informatie opleveren die helpt om theoretische inzichten beter te duiden (Baarda et al., 2021). De literatuur en interviewgegevens zijn thematisch geanalyseerd. Daarbij is gezocht naar terugkerende patronen en mechanismen die een rol spelen bij online radicalisering, zoals echo-kamers, groepspolarisatie, digitale gemeenschapsvorming en institutioneel wantrouwen. Op basis van deze analyse is een conceptueel model ontwikkeld. Dit model moet worden beschouwd als een analytische synthese van de in dit onderzoek geselecteerde literatuur en niet als een volledig of definitief model van online radicalisering.

Omdat het onderzoek is gebaseerd op literatuur en een expertinterview en geen persoonsgegevens van burgers verwerkt, zijn de ethische risico's beperkt. Wel is zorgvuldig omgegaan met vertrouwelijkheid. De respondent is geanonimiseerd. Vanwege vertrouwelijkheid is de interviewuitwerking niet als bijlage opgenomen. Dit onderzoek biedt daarmee een interdisciplinair en praktijkgericht perspectief op de rol van online omgevingen bij radicaliseringsprocessen onder aanhangers van de soevereinenbeweging en de betekenis daarvan voor het politiewerk in een digitaliserende samenleving.

4. Theoretisch kader

4.1 Online radicalisering

Radicalisering wordt in de literatuur doorgaans beschreven als een proces waarin individuen of groepen geleidelijk overtuigingen ontwikkelen die in toenemende mate

op gespannen voet kunnen komen te staan met bestaande maatschappelijke en politieke structuren. Dit proces gaat vaak gepaard met gevoelens van onrecht, wantrouwen tegenover instituties en identificatie met alternatieve ideologische narratieven (Chen et al., 2021).

Online omgevingen kunnen dit proces versterken doordat zij laagdrempelige toegang bieden tot alternatieve interpretaties van maatschappelijke gebeurtenissen en tot gemeenschappen van gelijkgestemden (Del Vicario et al., 2016; Greijdanus et al., 2020). Binnen dergelijke omgevingen kunnen overtuigingen worden bevestigd en gelegitimeerd, terwijl het vertrouwen in gevestigde instituties verder afneemt. Onderzoek naar complottheorieën laat zien dat dergelijke narratieven kunnen bijdragen aan institutioneel wantrouwen en de verspreiding van misinformatie (Napolitano & Reuter, 2021). Daarnaast faciliteren online platforms de vorming van netwerken waarin informatie selectief wordt gedeeld en bevestigd (Del Vicario et al., 2016; Greijdanus et al., 2020). Hierdoor kunnen overtuigingen geleidelijk verharderen en kan de afstand tot dominante maatschappelijke narratieven toenemen. Online radicalisering kent daarmee veelal een gradueel karakter, waarbij individuen zich via verschillende tussenstappen ontwikkelen richting meer vergaande en potentieel extremistische overtuigingen (Verwey-Jonker Instituut & RadarAdvies, 2025; AIVD, 2023).

4.2 De soevereinenbeweging

De soevereinenbeweging bestaat uit personen die stellen dat zij zich buiten het staatsrechtelijk systeem kunnen plaatsen en daardoor niet gebonden zouden zijn aan wetten of overheidsregels (Verwey-Jonker Instituut & RadarAdvies, 2025; Van Es et al., 2025). Binnen de beweging circuleren uiteenlopende interpretaties van soevereiniteit, staatsrecht en individuele autonomie. Hoewel geen sprake is van een sterk gecentraliseerde organisatie, delen veel aanhangers een diep wantrouwen tegenover overheidsinstanties en andere publieke instituties, wat een belangrijke basis vormt voor hun overtuigingen (AIVD, 2023; Verwey-Jonker Instituut & RadarAdvies, 2025).

Onderzoek laat zien dat aanhangers van anti-institutionele overtuigingen vaak, maar zeker niet uitsluitend, mannen van middelbare of oudere leeftijd zijn die negatieve ervaringen met overheidsinstanties hebben opgedaan en zich in toenemende mate miskend of niet gehoord voelen door instituties (Verwey-Jonker Instituut & RadarAdvies, 2025).

Volgens de AIVD (2023) wordt binnen anti-institutionele en soevereine netwerken een narratief verspreid waarin de legitimiteit van de staat structureel ter discussie wordt gesteld. Daarnaast laat recent Nederlands onderzoek zien dat binnen de beweging pseudojuridische redeneringen worden gebruikt waarmee individuen menen zich aan overheidsgezag te kunnen onttrekken. Van Es et al. (2025) beschrijven hoe dergelijke opvattingen zich manifesteren in zowel strafbaar gedrag als in verhoren van verdachten. Deze ideeën vertonen sterke overeenkomsten met de

zogenoemde Organized Pseudolegal Commercial Arguments (OPCA), zoals beschreven door Netolitzky (2016).

Online omgevingen spelen een centrale rol in de verspreiding van deze ideeën. Omdat de beweging slechts beperkt formeel is georganiseerd, vormen digitale netwerken de belangrijkste infrastructuur voor het delen van informatie, documenten en ervaringen. Websites, Telegramgroepen en podcasts functioneren daarbij als informele platforms waarop ideeën, documenten en strategieën worden gedeeld (Verwey-Jonker Instituut & RadarAdvies, 2025). Binnen deze netwerken worden persoonlijke frustraties, juridische interpretaties en anti-institutionele narratieven met elkaar verbonden, waardoor bestaande overtuigingen verder kunnen worden bevestigd en versterkt.

Hoewel de overgrote meerderheid van aanhangers niet geweldsbereid is, kan anti-institutioneel gedachtegoed in sommige gevallen leiden tot vergaande confrontaties met overheidsinstanties (Verwey-Jonker Instituut & RadarAdvies, 2025; AIVD, 2023). Wanneer de legitimiteit van de staat volledig wordt verworpen, kunnen conflicten ontstaan met politie, gemeenten of de rechtspraak, bijvoorbeeld rond belastingheffing, handhaving of juridische procedures (Van Es et al., 2025; Verwey-Jonker Instituut & RadarAdvies, 2025). Vanuit veiligheidsperspectief is het daarom relevant om te begrijpen hoe deze overtuigingen zich ontwikkelen en welke rol online omgevingen daarin spelen.

4.3 Digitale gemeenschappen en radicaliseringsprocessen

Digitale gemeenschappen spelen een belangrijke rol in radicaliseringsprocessen doordat zij nieuwe vormen van interactie, groepsvorming en mobilisatie mogelijk maken (Greijdanus et al., 2020; Van Halderen et al., 2024). Waar radicaliseringsprocessen traditioneel vaak verbonden waren met fysieke netwerken, bieden online platforms de mogelijkheid om snel en laagdrempelig in contact te komen met gelijkgestemden en alternatieve narratieven (Del Vicario et al., 2016; Verwey-Jonker Instituut & RadarAdvies, 2025). Hierdoor kunnen individuele overtuigingen niet alleen worden gevormd, maar ook collectief worden bevestigd en versterkt (Del Vicario et al., 2016; Sunstein, 2002).

Volgens Greijdanus et al. (2020) dragen digitale platforms bij aan collectieve actie doordat individuele ervaringen worden verbonden aan bredere ideologische kaders en online gemeenschappen worden gevormd. Hierdoor kan mobilisatie plaatsvinden zonder formele organisatiestructuren. Binnen de soevereinenbeweging betekent dit dat individuen zich kunnen aansluiten bij informele netwerken waarin wantrouwen tegenover instituties wordt gedeeld, bevestigd en verder versterkt (Verwey-Jonker Instituut & RadarAdvies, 2025).

Een belangrijk mechanisme binnen digitale gemeenschappen is de vorming van echo chambers. Binnen dergelijke omgevingen worden gebruikers vooral blootgesteld aan informatie die aansluit bij hun bestaande overtuigingen. Del Vicario et al. (2016) laten zien dat selectieve blootstelling aan informatie leidt tot homogene

netwerken waarin afwijkende perspectieven beperkt zichtbaar zijn. Ook Cinelli et al. (2021) tonen aan dat informatie zich op sociale media vooral verspreidt tussen gebruikers met vergelijkbare overtuigingen. Hierdoor kunnen bestaande opvattingen verder worden bevestigd en kan polarisatie toenemen.

Algoritmische aanbevelingssystemen kunnen deze processen versterken doordat content wordt aangeboden op basis van eerder gedrag. Tegelijkertijd bestaat in de literatuur discussie over de precieze invloed van algoritmen, omdat gebruikers niet uitsluitend passief worden beïnvloed, maar ook actief selecteren welke informatie zij consumeren (Cinelli et al., 2021; Del Vicario et al., 2016). Online radicalisering moet daarom worden begrepen als het resultaat van een wisselwerking tussen platformdynamieken, groepsprocessen en individuele keuzes.

Binnen deze context spelen complotachtige en anti-institutionele narratieven een centrale rol. Dergelijke narratieven bieden ogenschijnlijk eenvoudige verklaringen voor complexe maatschappelijke ontwikkelingen en kunnen het wantrouwen tegenover instituties versterken (Napolitano & Reuter, 2021). In Nederland beschrijven de AIVD (2023) en Verwey-Jonker Instituut en RadarAdvies (2025) hoe binnen anti-institutionele bewegingen het idee van een 'kwaadaardige elite' een overkoepelend narratief vormt. Dit narratief kan bijdragen aan de delegitimatie van de democratische rechtsorde doordat overheidsinstanties worden gepresenteerd als onbetrouwbaar of vijandig (AIVD, 2023; Verwey-Jonker Instituut & RadarAdvies, 2025).

Online dynamieken blijven niet beperkt tot het digitale domein. Van Es et al. (2025) laten zien dat pseudojuridische overtuigingen binnen de soevereinenbeweging kunnen doorwerken in concrete interacties met de overheid en in sommige gevallen gepaard gaan met strafbaar gedrag. Daarnaast beschrijven Lapidot-Lefler en Barak (2015) het online disinhibition effect, waarbij kenmerken van online communicatie, zoals anonimiteit en het ontbreken van directe sociale controle, kunnen bijdragen aan verminderde gedragsremming. Dit kan verklaren waarom online omgevingen ruimte bieden voor scherpere, meer confronterende of normoverschrijdende uitingen.

Deze inzichten laten zien dat online radicalisering voortkomt uit een samenspel van groepsvorming, echo chambers, algoritmische versterking, complotnarratieven en psychologische processen. Daarbij zijn online en offline dynamieken nauw met elkaar verweven. Voor de politie is inzicht in deze mechanismen van belang om radicaliseringsprocessen tijdig te herkennen en adequaat te duiden.

4.4 Conceptueel model van online radicalisering binnen de soevereinenbeweging

Op basis van de besproken literatuur is een conceptueel model ontwikkeld waarin de belangrijkste mechanismen van online radicalisering binnen de soevereinenbeweging worden samengebracht. Het model bouwt voort op inzichten over online radicalisering, digitale groepsdynamiek en anti-institutioneel

gedachtegoed, en moet worden beschouwd als een analytische synthese van de in dit onderzoek geselecteerde bronnen. Het betreft nadrukkelijk geen volledig of universeel model van radicalisering, maar een heuristisch hulpmiddel dat de voor dit onderzoek meest relevante mechanismen inzichtelijk maakt.

Het model beschrijft online radicalisering als een dynamisch proces waarin digitale, sociale en cognitieve mechanismen op elkaar inwerken. In tegenstelling tot een lineair stappenplan laat het model zien hoe verschillende factoren gelijktijdig aanwezig kunnen zijn en elkaar onderling kunnen versterken.

Het proces begint met toegang tot alternatieve narratieven via digitale platforms. Deze narratieven bieden afwijkende interpretaties van maatschappelijke en politieke ontwikkelingen en kunnen bijdragen aan twijfel aan de legitimiteit van instituties (AIVD, 2023; Verwey-Jonker Instituut & RadarAdvies, 2025). Vervolgens faciliteren online omgevingen de vorming van digitale gemeenschappen, waarin individuen in contact komen met gelijkgestemden en erkenning vinden voor hun opvattingen. Dit versterkt groepsidentiteit en normaliseert afwijkende overtuigingen (Greijdanus et al., 2020; Del Vicario et al., 2016).

Binnen deze gemeenschappen dragen echo chambers en algoritmische aanbevelingssystemen bij aan verdere bevestiging van bestaande overtuigingen. Gebruikers worden vooral blootgesteld aan informatie die aansluit bij hun wereldbeeld, waardoor alternatieve perspectieven minder zichtbaar worden (Del Vicario et al., 2016; Cinelli et al., 2021). Hoewel de precieze invloed van algoritmen onderwerp van wetenschappelijke discussie is, kan de combinatie van selectieve blootstelling en groepsinteractie bijdragen aan ideologische verharding en toenemend institutioneel wantrouwen (Del Vicario et al., 2016; AIVD, 2023; Verwey-Jonker Instituut & RadarAdvies, 2025).

In een latere fase kunnen deze overtuigingen doorwerken in gedrag. Binnen de soevereinenbeweging kan dit zich uiten in het gebruik van pseudojuridische argumenten, het afwijzen van overheidsgezag en spanningen in de interactie met overheidsinstanties. Nederlandse studies wijzen erop dat online informatie-uitwisseling en groepsdynamiek kunnen bijdragen aan het legitimeren van normafwijkend gedrag (Verwey-Jonker Instituut & RadarAdvies, 2025; Van Es et al., 2025).

Het model benadrukt dat online en offline processen nauw met elkaar verweven zijn. Digitale omgevingen functioneren niet alleen als informatiebron, maar ook als sociale context waarin overtuigingen worden gevormd, bevestigd en gelegitimeerd. In offline situaties kunnen deze overtuigingen vervolgens zichtbaar worden in concrete interacties met overheidsinstanties, bijvoorbeeld bij handhaving, juridische procedures of contact met gemeenten. Door de terugkoppeling van deze ervaringen naar digitale gemeenschappen laat het model zien dat radicaliseringsprocessen zichzelf kunnen versterken.

Het model vormt de basis voor de verdere analyse in dit onderzoek (zie figuur 1).



Figuur 1
Conceptueel model van online radicalisering binnen de soevereinenbeweging (eigen bewerking).

4.5 De rol van politie in online omgevingen

De verschuiving van maatschappelijke interacties naar online platforms heeft directe gevolgen voor de wijze waarop politieorganisaties signalen van radicalisering herkennen en duiden. Traditionele signaleringsstructuren zijn voornamelijk gericht op fysieke netwerken, lokale gemeenschappen en zichtbaar gedrag in de offline wereld, terwijl online radicaliseringsprocessen zich juist kunnen ontwikkelen binnen fluïde digitale gemeenschappen en informele netwerken. Hierdoor worden signalen diffuser en moeilijker te interpreteren (Van Halderen et al., 2024; Verwey-Jonker Instituut & RadarAdvies, 2025). Dit vraagt om een aanpassing van bestaande werkwijzen binnen het politiewerk.

Van Halderen et al. (2024) benadrukken dat politiewerk in digitale omgevingen niet uitsluitend gericht moet zijn op handhaving. Online aanwezigheid kan ook bijdragen aan het opbouwen van vertrouwen, het signaleren en duiden van misinformatie en het vroegtijdig herkennen van maatschappelijke spanningen.

Daarmee krijgt de politie niet alleen een handhavende, maar ook een communicatieve en signalerende rol in digitale omgevingen.

Ook uit het expertinterview blijkt dat het duiden van online radicalisering complex is. De geïnterviewde politieprofessional benadrukt dat online uitingen vaak moeilijk te interpreteren zijn en dat het onderscheid tussen extreme meningen en daadwerkelijke dreiging niet altijd duidelijk is (persoonlijke communicatie, 18 maart 2026). Deze bevinding onderstreept dat de betekenis van online signalen sterk afhankelijk is van context en professionele interpretatie.

Daarnaast roept online politiewerk vragen op over legitimiteit, privacy en de verhouding tussen veiligheid en fundamentele rechten. Juist omdat anti-institutionele bewegingen de legitimiteit van de overheid ter discussie stellen, is een zorgvuldige en proportionele benadering van belang. Het signaleren en duiden van online radicalisering moet daarom steeds plaatsvinden binnen de kaders van de democratische rechtsstaat (Van Halderen et al., 2024; AIVD, 2023).

Voor politieorganisaties betekent dit dat inzicht in online radicaliseringsprocessen essentieel is om digitale gemeenschappen beter te begrijpen en passende handelingsperspectieven te ontwikkelen. Dit vraagt om een combinatie van technologische kennis, contextueel begrip en strategische online aanwezigheid.

4.6 Conceptuele samenvatting

Op basis van de besproken literatuur kan online radicalisering worden begrepen als een dynamisch proces waarin digitale platforms, groepsdynamiek en ideologische narratieven elkaar wederzijds versterken. Online omgevingen faciliteren de verspreiding van alternatieve interpretaties van maatschappelijke gebeurtenissen en de vorming van digitale gemeenschappen waarin deze interpretaties worden bevestigd, gedeeld en versterkt (Del Vicario et al., 2016; Greijdanus et al., 2020). Deze dynamiek sluit aan bij inzichten over groepspolarisatie en echo chambers (Sunstein, 2002; Del Vicario et al., 2016).

Binnen de soevereinenbeweging krijgt dit proces een specifieke invulling doordat anti-institutionele narratieven, zoals het idee van een illegitieme overheid, centraal staan. Wanneer dergelijke narratieven in online netwerken worden herhaald en gelegitimeerd, kan het wantrouwen tegenover instituties toenemen en kan de legitimiteit van de democratische rechtsstaat verder worden ondermijnd (AIVD, 2023; Verwey-Jonker Instituut & RadarAdvies, 2025).

Voor de politie betekent dit dat radicaliseringsprocessen zich in toenemende mate online afspelen en daardoor minder zichtbaar zijn binnen traditionele signaleringsstructuren. Dit vraagt om aangepaste vormen van duiding, signalering en interactie, waarbij zorgvuldig moet worden omgegaan met publieke waarden zoals legitimiteit, proportionaliteit en respect voor fundamentele rechten (Van Halderen et al., 2024).

Het conceptueel model vat deze mechanismen samen en vormt de basis voor de verdere analyse in dit onderzoek.

5. Discussie

5.1 Beperkingen en reflectie

Hoewel deze studie inzicht biedt in de rol van online omgevingen bij radicaliseringsprocessen onder aanhangers van de soevereinenbeweging, kent het onderzoek enkele beperkingen. In de eerste plaats is het onderzoek voornamelijk gebaseerd op literatuuronderzoek en één expertinterview. Daardoor blijft de empirische onderbouwing van specifieke radicaliseringsprocessen binnen de Nederlandse context beperkt. De bevindingen zijn daarom niet zonder meer generaliseerbaar naar alle aanhangers van de soevereinenbeweging of naar andere vormen van radicalisering.

Daarnaast richt een belangrijk deel van de geraadpleegde literatuur zich op bredere vormen van online extremisme en complotdenken. Hoewel deze inzichten relevant zijn, zijn zij niet altijd één-op-één toepasbaar op de specifieke kenmerken van de soevereinenbeweging. De interpretatie van de bevindingen vraagt daarom om terughoudendheid.

Een derde beperking betreft de veranderlijkheid van digitale platforms. Algoritmen, platformregels en online gemeenschappen ontwikkelen zich voortdurend, waardoor wetenschappelijke literatuur relatief snel kan verouderen. Dit maakt het lastig om op basis van bestaande bronnen langdurig geldende conclusies te trekken.

Tegelijkertijd laat dit onderzoek zien dat online radicalisering het best kan worden begrepen als een samenspel van technologische, sociale en psychologische mechanismen. De combinatie van literatuur en praktijkkennis biedt een bruikbaar analytisch perspectief, maar vraagt om verdere empirische toetsing.

Toekomstig onderzoek kan dit perspectief verdiepen door online interacties binnen de soevereinenbeweging systematisch te analyseren, bijvoorbeeld via digitale netwerkanalyses of aanvullende interviews met professionals. Daarmee kan beter inzicht worden verkregen in de wijze waarop online processen doorwerken in offline gedrag en in de vraag hoe politieorganisaties hier effectief en proportioneel op kunnen inspelen.

5.2 Implicaties voor de politiepraktijk

De bevindingen van dit onderzoek laten zien dat online radicaliseringsprocessen zich in toenemende mate afspelen binnen dynamische en deels moeilijk zichtbare digitale omgevingen. Dit vraagt om een aanpassing van bestaande werkwijzen binnen de politie.

In de eerste plaats is het van belang dat politieorganisaties investeren in hun online signaleringscapaciteit. Radicaliseringsprocessen binnen de soevereinenbeweging ontwikkelen zich deels via open online platforms en digitale

netwerken. Signalering kan daarom niet uitsluitend plaatsvinden via fysieke netwerken of traditionele informatiebronnen. Het zorgvuldig volgen van open bronnen en het ontwikkelen van expertise in het herkennen van relevante online signalen zijn hierbij essentieel, mits dit plaatsvindt binnen juridische en proportionele kaders.

Daarnaast blijkt uit zowel de literatuur als het expertinterview dat het duiden van online uitingen complex is (persoonlijke communicatie, 18 maart 2026). Het onderscheid tussen extreme opvattingen en daadwerkelijke dreiging is niet altijd eenduidig. Dit vraagt om versterking van het analytisch vermogen van professionals, bijvoorbeeld door training op het gebied van online gedrag, contextanalyse en radicaliseringsprocessen.

Een derde implicatie betreft de rol van de politie in online omgevingen. Van Halderen et al. (2024) benadrukken dat online aanwezigheid kan bijdragen aan vroegsignalering, vertrouwen en het signaleren en duiden van misinformatie. Dit vraagt om een politie die zich niet uitsluitend als handhaver positioneert, maar ook als zichtbare en benaderbare communicatiepartner.

Daarnaast is een goede verbinding tussen intelligence en operationele teams van belang. Uit het expertinterview blijkt dat signalen niet altijd eenvoudig worden vertaald naar concrete handelingsperspectieven (persoonlijke communicatie, 18 maart 2026). Een nauwere samenwerking tussen analyse en operatie kan bijdragen aan effectievere en tijdigere interventies.

Gezamenlijk laten deze implicaties zien dat het omgaan met online radicalisering vraagt om een combinatie van technologische kennis, contextueel inzicht en organisatorische afstemming. Daarbij moeten veiligheid, legitimiteit en respect voor fundamentele rechten steeds zorgvuldig met elkaar in balans worden gebracht.

6. Conclusie

Het doel van dit onderzoek was om inzicht te verkrijgen in de wijze waarop online omgevingen bijdragen aan radicaliseringsprocessen onder aanhangers van de soevereinenbeweging en welke implicaties dit heeft voor de rol van de politie.

Op basis van de literatuur en het expertinterview kan worden geconcludeerd dat online omgevingen een belangrijke rol spelen in de verspreiding en versterking van anti-institutionele narratieven. Digitale platforms bieden toegang tot alternatieve interpretaties van maatschappelijke gebeurtenissen en faciliteren de vorming van digitale gemeenschappen waarin deze overtuigingen worden bevestigd en gelegitimeerd.

Binnen deze online omgevingen versterken verschillende mechanismen elkaar. Toegang tot alternatieve narratieven, digitale gemeenschapsvorming, echo chambers, algoritmische aanbevelingssystemen en groepspolarisatie kunnen gezamenlijk bijdragen aan ideologische verharding en toenemend wantrouwen tegenover instituties. In sommige gevallen kan dit doorwerken in gedrag,

bijvoorbeeld in het gebruik van pseudojuridische argumenten en confrontaties met overheidsinstanties.

Voor de politie betekent dit dat radicaliseringsprocessen zich in belangrijke mate online kunnen ontwikkelen en daardoor minder zichtbaar zijn binnen traditionele signaleringsstructuren. Dit vraagt om versterking van online signaleringscapaciteit, het analytisch vermogen van professionals en een zorgvuldige online aanwezigheid binnen de kaders van de democratische rechtsstaat.

Zoals ook uit het expertinterview blijkt, zijn online uitingen vaak moeilijk te duiden en is het onderscheid tussen extreme opvattingen en daadwerkelijke dreiging niet altijd eenduidig (persoonlijke communicatie, 18 maart 2026). Dit onderstreept dat inzicht in de context en dynamiek van online gemeenschappen essentieel is voor het ontwikkelen van passende handelingsperspectieven.

Concluderend kan worden gesteld dat digitale platforms niet slechts communicatiemiddelen zijn, maar een sociale infrastructuur vormen waarin radicaliseringsprocessen zich kunnen ontwikkelen en versterken. Voor de politie betekent dit dat signalering, duiding en interactie in online omgevingen een structureel onderdeel moeten vormen van politiewerk in een digitaliserende samenleving.

Literatuurlijst

Algemene Inlichtingen- en Veiligheidsdienst. (2023). Anti-institutioneel extremisme in Nederland: Een ernstige dreiging voor de democratische rechtsorde. <https://www.aivd.nl/documenten/2023/05/25/anti-institutioneel-extremisme-in-nederland-een-ernstige-dreiging-voor-de-democratische-rechtsorde>

Baarda, D. B., Bakker, E., Fischer, T., Julsing, M., Peters, V., & Van der Velden, T. (2021). Basisboek kwalitatief onderzoek (5e ed.). Noordhoff.

Chen, L. L., Mirpuri, S., Rao, N., & Law, N. (2021). Conceptualization and measurement of digital citizenship across disciplines. *Educational Research Review*, 33, 100379. <https://doi.org/10.1016/j.edurev.2021.100379>

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), e2023301118. <https://doi.org/10.1073/pnas.2023301118>

Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., & Quattrociocchi, W. (2016). The spreading of misinformation online. *Proceedings of the National Academy of Sciences*, 113(3), 554–559. <https://doi.org/10.1073/pnas.1517441113>

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

Lapidot-Lefler, N., & Barak, A. (2015). The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 9(2), Article 3. <https://doi.org/10.5817/CP2015-2-3>

Napolitano, M. G., & Reuter, K. (2021). What is a conspiracy theory? *Erkenntnis*, 88(5), 2035–2062. <https://doi.org/10.1007/s10670-021-00441-6>

Netolitzky, D. J. (2016). The history of the organized pseudolegal commercial argument phenomenon in Canada. *Alberta Law Review*, 53(3), 609–641.

OpenAI. (2026). ChatGPT (Versie GPT-5.5) [Generatieve AI]. <https://chatgpt.com>

Sunstein, C. R. (2002). The law of group polarization. *Journal of Political Philosophy*, 10(2), 175–195. <https://doi.org/10.1111/1467-9760.00148>

Van Es, L., Van Prooijen, J.-W., Van Buuren, J., & Van Veldhuizen, A. P. (2025). How pseudolegal advice manifests itself in criminal offending and suspect interrogations of sovereign citizens in the Netherlands. *Deviant Behavior*. Advance online publication. <https://doi.org/10.1080/01639625.2025.2599959>

Van Halderen, R. C., Tjoelker, R., & Spithoven, R. (2024). Met gezag online: Online schadelijk gedrag, publieke waarden en de politiefunctie. In M. Walrave, C. Van de Heyning, J. Janssen, & E. Kolthoff (Red.), *Misbruik van beelden: Cahiers Politiestudies*, 70 (pp. 185–200). Gompel&Svacina.

Verwey-Jonker Instituut & RadarAdvies. (2025). Anti-institutionalisme in Nederland: Exploratieve overzichtsstudie van gedachtegoed, organisatie, voedingsbodems, risico's en bestaande handelingsperspectieven. WODC.

Deepfakes en democratische veiligheid

Reijer Bakker

Minor Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool

1. Inleiding

1.1 Introductie en actualiteit

Tijdens de Europese verkiezingen in 2024 ontstond er commotie rond kunstmatige intelligentie (AI)-gegenereerde video's van Nederlandse politici. Deze video's bevatten uitspraken die deze politici nooit hadden gedaan. De politici in kwestie waren Geert Wilders, Caroline van der Plas en Rob Jetten. Dit was het resultaat van een onderzoek van BNR, waarbij ten minste drie deepfakevideo's door de filters van Meta en X wisten te glippen. Dit gebeurde toch, ondanks dat beide bedrijven toezeggingen hebben gedaan om misleidende content af te weren (NOS, 2024).

Dit onderzoek is een voorbeeld van een toenemend probleem: grote platformen als Meta en X blijken niet in staat om te allen tijde valse politieke content tijdig te detecteren. Waar deepfakes begonnen als experimenteel werk, worden ze steeds vaker ingezet in de publieke sfeer, met grote gevolgen voor de democratische veiligheid en de juistheid van informatie op het internet.

Het onderzoek van BNR roept een valide vraag op: *hoe kwetsbaar zijn verkiezingsprocessen wanneer foutieve informatie, zoals deepfakes, op het internet circuleert?*

1.2 Probleemstelling en relevantie

De opkomst van deepfakes (video, audio, afbeeldingen) die met AI-technieken zodanig zijn gemanipuleerd dat ze vrijwel niet van echt te onderscheiden zijn, stelt de integriteit van informatievoorziening en het publieke vertrouwen op de proef. In het politieke domein kan dit leiden tot verwarring onder kiezers, polarisatie en de ondermijning van instituties.

Hoewel techbedrijven zich hebben gecommitteerd aan het weren van misleidende content, blijkt in de praktijk dat de genomen maatregelen nog onvoldoende zijn. Het voorbeeld van de Nederlandse deepfakes die door filters glipten ondanks toezeggingen van Meta en X, toont aan dat de dreiging serieus genomen dient te worden. Dit roept de vraag op of we diepgaandere inventarisatie van risico's, consequenties en oplossingen moeten voeren om democratische veiligheid te waarborgen.

Verkiezingen vormen de kern van de democratie. Als algoritmes de media beïnvloeden op een manier die eerlijke en goed geïnformeerde keuzes in de weg staat, dan raakt dat niet alleen het vertrouwen in de media, maar ondermijnt het de fundamenten van de democratische rechtsstaat zelf.

1.3 Doel en onderzoeksvragen

Dit onderzoeksartikel heeft als doel om te onderzoeken in hoeverre deepfakes een bedreiging vormen voor de democratische integriteit van verkiezingen, en welke interventies mogelijk ingezet kunnen worden om die dreiging te beperken. De centrale vraag van dit onderzoek luidt: *“In hoeverre vormen deepfakes een bedreiging voor democratische veiligheid en verkiezingsintegriteit?”*

Ter beantwoording van de hoofdvraag, zijn de volgende deelvragen geformuleerd:

Deelvraag 1: “Welke vormen van deepfakes worden gebruikt in politieke contexten, en via welke kanalen worden deze verspreid?”

Deelvraag 2: “Wat zijn de potentiële gevolgen van deepfakes voor publieke opinie en vertrouwen in verkiezingsprocessen?”

Deelvraag 3: “In hoeverre zijn bestaande wet- en regelgeving en technologische maatregelen toereikend om deepfakes tegen te gaan?”

2. Betogende analyse

2.1 Uitleg en vormen van deepfakes

Juridische definitie. De Europese AI Act omschrijft een deepfake als “door AI gegenereerd of gemanipuleerd beeld, audio- of videomateriaal dat een gelijkenis vertoont met bestaande personen, voorwerpen, plaatsen, entiteiten of gebeurtenissen, en door een persoon ten onrechte voor authentiek of waarheidsgetrouw zou worden aangezien” (EU AI Act, 2024). Deze juridische definitie toont dat deepfakes niet enkel betrekking hebben op bekende personen, maar ook op beelden of geluiden die de indruk wekken echt te zijn. Daarmee onderscheidt de wet zich van de technologische omschrijving van deepfakes (InView, z.d.).

Technologische definitie. Vanuit technologisch oogpunt worden deepfakes gemaakt met behulp van AI. De AI wordt geleerd bestaande beelden of stemmen te imiteren. Vaak spelen Generative Adversarial Networks (GAN's) een rol: twee algoritmes ‘spelen’ tegen elkaar, het ene genereert beelden, het andere probeert die als echt of nep te bestempelen, waardoor de uiteindelijk geproduceerde output steeds realistischer wordt. De technische drempel voor het maken van deepfakes is inmiddels sterk verlaagd. Er bestaan veel online tools en apps waarmee gebruikers, zonder diepgaande kennis, overtuigende video's en audiofragmenten kunnen produceren. Daardoor verschuift het gebruik van deepfakes van experimenteel naar mogelijk schadelijke intenties zoals politieke manipulatie (TechTarget, 2025).

Vormen van deepfakes. Er zijn verschillende vormen van deepfakes. De meest voorkomende vorm van deepfakes is de video-deepfake. Hierbij worden gezichten en bewegingen gemanipuleerd om iemand uitspraken of handelingen te laten verrichten die nooit zijn gedaan. Naast deze vorm van deepfakes bestaan ook audio-deepfakes. Hierbij wordt iemands stem nagemaakt met behulp van AI. Ook komen afbeeldings-deepfakes veel voor. Dit zijn stilstaande beelden of foto's die zijn aangepast of volledig gegenereerd door AI. Deze beelden worden bijvoorbeeld gebruikt voor

misleidende nieuwsberichten of reclame. De verschillende vormen van deepfakes worden met name verspreid via sociale media. Door de algoritmes op sociale media bereiken deze deepfakes snel een groot publiek. Dit draagt bij aan het feit dat het voor gebruikers van sociale media steeds moeilijker wordt om te beoordelen welke beelden echt zijn en welke gemanipuleerd zijn (Vaccar & Chadwick, 2020).

2.2 Impact op democratische processen

Van misleiding naar wantrouwen. Deepfakes vormen niet alleen een technologisch probleem, maar ook een maatschappelijk en democratisch vraagstuk. De eerste generatie deepfakes waren met name bedoeld voor entertainment en satire, maar het huidige gebruik wordt steeds vaker ingezet voor beïnvloeding en manipulatie. Het gevaar ligt niet alleen in de directe misleiding van het publiek, maar vooral in de gevolgen voor het vertrouwen in informatiebronnen, de media en politieke instituties. Tegenwoordig vinden campagnes steeds vaker digitaal plaats. Hierbij is de informatieverschaffing op sociale media cruciaal voor de campagne. Twijfel over de echtheid van beeld- en videomateriaal kan dit ernstig ondermijnen.

Een belangrijk concept in dit verband is het zogenaamde “liar’s dividend”. Deze term verwijst naar het feit dat niet alleen nepbeelden twijfel zaaien, maar ook authentieke beelden deels hun geloofwaardigheid verliezen. Zodra burgers weten dat deepfakes bestaan, kan alles, zelfs echte video’s, ter discussie worden gesteld (Vaccari & Chadwick, 2020). Hierdoor verschuift het probleem van desinformatie naar een groter wantrouwen, waarbij de waarheid zelf ter discussie komt te staan. Politici kunnen bijvoorbeeld echte beelden van controversiële uitspraken afdoen als deepfake, terwijl kiezers moeite hebben om feit van fictie te onderscheiden.

Dit groeiende wantrouwen heeft directe gevolgen voor de stabiliteit van de democratische rechtsstaat. Besluitvorming in een democratie vereist een goed geïnformeerde bevolking dat toegang heeft tot betrouwbare informatie. Wanneer burgers structureel twijfelen aan de echtheid van wat zij zien en horen, wordt dit democratische proces ernstig ondermijnd. Zoals Westerlund (2019) stelt, creëren deepfakes enorme onzekerheid waarin burgers steeds minder vertrouwen hebben in visuele bewijzen, iets wat lange tijd werd beschouwd als een van de meest betrouwbare vormen van informatie.

Hoewel er momenteel nog relatief weinig onderzoek is gedaan naar de langetermijneffecten van deepfakes op verkiezingsuitkomsten, wijzen bestaande onderzoeken erop dat het verlies van vertrouwen een krachtig effect heeft. Bij gevallen van misleiding kan de angst of verwachting dat deepfakes bestaan al voldoende zijn om de geloofwaardigheid van politieke communicatie te ondermijnen. Zo vormen deepfakes een fundamentele bedreiging voor het publieke debat en de democratische veiligheid.

Verspreiding via sociale media. De verspreiding van deepfakes vindt grotendeels plaats via sociale media, waar de snelheid van verspreiding enorm snel is. Platforms als X, Meta en TikTok spelen hierin een centrale rol. De algoritmes die deze

platformen aansturen zijn ontworpen om gebruikers zo lang mogelijk vast te houden door content aan te bieden die inspeelt op emoties. Sensationele of controversiële berichten, zoals deepfakes, presteren vaak beter dan neutrale informatie. Doordat deepfakes zich zo ontzettend snel verspreiden, kunnen gebruikers het zien voordat platforms zelf kunnen ingrijpen (Westerlund, 2019).

Tijdens de Europese verkiezingen van 2024 bleek hoe kwetsbaar het huidige systeem is. Onderzoek van BNR toonde aan dat ten minste drie deepfakevideo's van Nederlandse politici op X en Meta wisten te komen, ondanks toezeggingen van beide bedrijven om misleidende content te weren. Deze video's werden duizenden keren bekeken voordat ze verwijderd werden. Deze incidenten tonen aan dat de technische detectiesystemen van de platforms niet toereikend zijn, zeker wanneer deepfakes kort voor belangrijke politieke gebeurtenissen verschijnen. Het gevolg is dat misleidende beelden zich binnen enkele uren kunnen verspreiden onder een groot publiek, vaak te laat om de schade nog te herstellen (NOS, 2024).

Naast de snelheid is ook de wijze waarop gebruikers met inhoud omgaan van belang. Met likes, reacties en delen verhogen gebruikers de zichtbaarheid van deepfakes zonder dat dit opvalt. Als een video viral wordt, wordt deze door het algoritme eerder weergegeven. Deze dynamiek resulteert in een constante strijd tussen de ontwikkelaars van deepfakes en de 5 partijen die ze proberen te beschermen. Er worden nieuwe detectiemethoden gecreëerd, terwijl de deepfake-algoritmes tegelijkertijd zich ontwikkelen. Dit leidt ertoe dat platforms steeds achter de feiten aanlopen (Chesney & Citron, 2019).

De mix van algoritmes, het gedrag van gebruikers en een gebrek aan detectie leidt tot een situatie waarin onjuiste informatie sneller verspreidt dan de werkelijkheid. Sociale media dienen niet alleen als een middel voor communicatie, maar creëren ook onzekerheid en wantrouwen. Deze dynamiek vergroot de democratische kwetsbaarheid die in de eerdere paragraaf is toegelicht: wanneer burgers steeds te maken krijgen met twijfelachtige beelden waarvan ze niet zeker zijn of ze echt zijn, wordt hun capaciteit om goed geïnformeerde beslissingen te nemen ondermijnd.

Gevolgen voor democratie. De verspreiding van deepfakes heeft aanzienlijke impact op de wijze waarop mensen informatie evalueren en politieke beslissingen nemen. Democratische processen zijn gebaseerd op informatie die een onderscheid maakt tussen werkelijkheid en verzinzel. Als dit onderscheid niet mogelijk is, kan de legitimiteit van verkiezingen onder druk komen te staan. Deepfakes kunnen ervoor zorgen dat kiezers onjuiste veronderstellingen maken over politici, beleid en/of gebeurtenissen. Dit heeft een directe impact op het stemgedrag van individuen. Dit wordt eveneens aangetoond door een studie van het Rathenau Instituut (2021), dat desinformatie, zelfs na het correctieproces, een blijvende impact kan uitoefenen op de overtuigingen van burgers en hun vertrouwen in informatievoorziening en politiek.

Naast directe beïnvloeding van kiezers, heeft de opkomst van deepfakes ook een breder effect op het vertrouwen in media en overheid. Burgers die meerdere

malen worden geconfronteerd met twijfelachtige beelden, ontwikkelen een sceptische houding tegenover alle vormen van visuele informatie. Hierdoor kunnen ook betrouwbare nieuwsbronnen en officiële instanties geloofwaardigheid verliezen. Wanneer het publiek niet langer gelooft in de authenticiteit van informatie, verliest de overheid haar vermogen om burgers effectief te informeren. Dit proces van vermindering van vertrouwen is niet alleen schadelijk voor verkiezingen, maar tast de bredere maatschappij ook aan (Chesney & Citron, 2019).

Daarnaast vergroot de aanwezigheid van deepfakes het risico op polarisatie. Groepen die sowieso al ideologisch van elkaar verschillen, kunnen deepfakes gebruiken om hun eigen overtuigingen te versterken en tegenstanders in diskrediet te brengen. Sociale media versterken dit effect doordat gebruikers vooral berichten zien die aansluiten bij hun bestaande opvattingen. Hierdoor ontstaat een versterkende loop waarin wantrouwen en vijandbeelden groeien. Politieke leiders of andere actoren kunnen dit bewust inzetten als strategie om verdeeldheid te zaaien of de geloofwaardigheid van de media te ondermijnen (Westerlund, 2019).

De bedreiging van deepfakes richt zich niet alleen op de directe gevolgen van misleiding, maar ook op het fundament van democratische legitimiteit. Als de grens tussen feit en fictie vervaagt, vermindert de kans om rationele, op feiten gebaseerde beslissingen te nemen. Dit vormt een blijvende bedreiging voor de democratische veiligheid, waarbij niet alleen het vertrouwen in informatie, maar ook het vertrouwen in het systeem in gevaar komt.

2.3 Interventies en oplossingen

Technologische maatregelen. Een concrete technologische interventie is het gebruik van watermerken in AI-gegenereerde video's. Meta heeft recent de tool Video Seal gelanceerd, waarmee onzichtbare watermerken automatisch worden toegevoegd aan video's die door AI zijn gemaakt. Deze watermerken werken als een belangrijk kenmerk voor authenticiteit en zijn speciaal ontworpen om aanwezig te blijven, zelfs wanneer de video wordt gecomprimeerd of bewerkt. Op die manier kan worden vastgesteld of een video daadwerkelijk door AI is geproduceerd of dat het authentieke content betreft (Meta AI, 2024).

Deze vorm van "in-video watermarking" wordt gezien als een veelbelovende aanpak om deepfakes te onderscheiden van echte video's, maar het is geen waterdichte oplossing. Kwaadwillenden zouden namelijk technieken kunnen ontwikkelen om de watermerken te verwijderen of de video zo te manipuleren dat het watermerk minder zichtbaar wordt, waardoor de betrouwbaarheid van deze methode onder druk kan komen te staan.

Juridische en beleidsmaatregelen. Op juridisch en beleidsmatig vlak vormt de Europese AI Act een belangrijke stap richting de regulering. Aangenomen in 2024, bevat de wet specifieke bepalingen over transparantie bij het gebruik van AI. Volgens artikel 50 moeten aanbieders duidelijk aangeven wanneer beeld, audio- of videomateriaal door AI is gegenereerd of gemanipuleerd, vooral wanneer deepfakes

door een gemiddeld persoon als authentiek zouden kunnen worden beschouwd. Het doel is misleiding te voorkomen en burgers bewust te maken van waar digitale content vandaan komt, waarbij de verantwoordelijkheid niet alleen bij het publiek, maar ook bij de makers en verspreiders ligt (EU AI Act, 2024).

Toch kent de AI Act duidelijke beperkingen. De handhaving is in handen van nationale toezichthouders, wat kan leiden tot verschillen in de uitvoering tussen lidstaten. Artikel 99 van de AI Act verplicht lidstaten om regels en handhavingsmaatregelen vast te stellen, evenals proportionele sancties voor overtredingen. Boetes voor overtreding van de AI Act kunnen oplopen tot wel 35 miljoen euro (EU AI Act, 2024). Echter, blijken deze maatregelen nog onvoldoende te zijn om de verspreiding van deepfakes effectief te voorkomen, vooral wanneer deze worden geproduceerd buiten de EU en via Europese platforms worden verspreid.

Maatschappelijke en educatieve interventies. Netwerk Mediawijsheid voert campagnes zoals 'Blijf scherp, stem bewust', waarin burgers worden getraind in het herkennen van desinformatie in verkiezingstijd. Door middel van video's, artikelen en checklists worden mensen bewust gemaakt van de risico's van nepnieuws en krijgen ze handvatten om betrouwbare van onbetrouwbare informatie te onderscheiden. Op deze manier probeert het Netwerk de mediageletterdheid van kiezers te verhogen en hen te helpen weloverwogen keuzes te maken (Netwerk Mediawijsheid, 2025).

Daarnaast biedt het ECP via isdatechtzo.nl een uitgebreide verkiezings-toolkit aan, met hulpmiddelen zoals posters, animaties en praktische tips om desinformatie tijdens verkiezingen te herkennen en te weerleggen. Deze toolkit is bedoeld voor zowel individuele burgers als organisaties die actief willen bijdragen aan een geïnformeerde samenleving (ECP, 2024).

Ook op schoolniveau is er aandacht voor mediageletterdheid. Op [Mediawijsheid.nl](https://mediawijsheid.nl) staan lesmaterialen klaar over nepnieuws, waarmee leerlingen de basisvaardigheden leren om informatie kritisch te beoordelen. Docenten kunnen hiermee lessen vormgeven die leerlingen niet alleen bewust maken van de gevaren van desinformatie, maar hen ook leren hoe ze zelf betrouwbare bronnen kunnen vinden en controleren (Mediawijsheid, z.d.).

De acties, waaronder campagnes, toolkits en schoolmateriaal, zijn heldere en gerichte acties om de mediageletterdheid te verbeteren en burgers te helpen om desinformatie te identificeren. Ze bieden ondersteuning en bereiken zowel kiezers als leerlingen, waardoor de bewustwording toeneemt. Het is echter moeilijk om precies te evalueren in welke mate deze initiatieven het gedrag van mensen beïnvloeden en of ze hen daadwerkelijk beter beschermen tegen misleiding. Hoewel de interventies veelbelovend zijn, is het nog steeds onduidelijk of ze in de praktijk het gewenste resultaat opleveren.

2.4 Kritische reflectie en toekomstperspectief

Hoewel de genoemde maatregelen waardevol zijn en helpen bij het bestrijden en vergroten van de bewustwording over deepfakes, zijn er toch beperkingen.

Watermerken zoals Video Seal zijn nog vrij recent en worden niet overal gebruikt; bepaalde deepfakes kunnen de watermerken vermijden. Juridische acties hebben te maken met jurisdictieproblemen, aangezien deepfakes vaak wereldwijd worden verspreid. Educatieve activiteiten zijn van groot belang, maar ze vereisen tijd om effect te behalen en zijn afhankelijk van de betrokkenheid van scholen en publieke ondersteuning. Er is ook onzekerheid of ze in de praktijk het gewenste resultaat behalen.

Voor een duurzame strategie is de integratie van technologie, beleid en onderwijs essentieel. Platforms, overheidsinstellingen en kennisinstellingen zouden gezamenlijk moeten werken aan open standaarden voor watermarking, gezamenlijke handhavingssystemen en uitgebreide educatieve programma's om de bewustwording over deepfakes te vergroten. Enkel op die manier kan de democratische veiligheid op een effectieve manier worden beschermd in een periode waarin technologieën razendsnel evolueren.

2.4 Samenloop

De betogende analyse toont aan dat deepfakes een veelzijdige en groeiende bedreiging vormen voor de democratische veiligheid. Vanuit technisch perspectief worden deepfakes steeds realistischer en eenvoudiger te vervaardigen, wat de kans op misbruik aanzienlijk heeft verminderd en kwaadwillenden relatief eenvoudig manipulaties kunnen uitvoeren. De Europese Unie probeert op juridisch gebied meer openheid en verantwoordelijkheid te bevorderen bij producenten en verspreiders van media door middel van de AI Act. Toch blijft de snelle groei van generatieve AI een obstakel voor een doeltreffende handhaving, waardoor de huidige wetgeving soms niet inspeelt op de technologische vooruitgang.

De grootste impact van deepfakes doet zich echter voor op maatschappelijk niveau. Ze ondermijnen het publieke vertrouwen in informatie, versterken polarisatie en vergroten de kans dat kiezers worden misleid. Sociale mediaplatforms dragen door middel van hun 8 algoritmes bij aan de snelle en brede verspreiding van deze content, terwijl huidige detectiemechanismen, beleid en educatieve initiatieven vaak tekortschieten of onvoldoende worden toegepast.

De huidige interventies, zoals technologische detectie, wettelijke regulering en educatieve programma's vormen gezamenlijk een belangrijke eerste stap in de bestrijding van de risico's van deepfakes. Toch zijn deze maatregelen nog onvoldoende geïntegreerd en is er behoefte aan een meer samenhangende aanpak. Een duurzame strategie vraagt om een gecombineerde inzet van technologie, beleid en maatschappelijke weerbaarheid, zodat burgers beter beschermd worden tegen digitale manipulatie en desinformatie. In het volgende hoofdstuk worden de belangrijkste bevindingen samengevat en worden aanbevelingen gepresenteerd om de democratische integriteit beter te waarborgen.

3. Conclusie

De analyse van dit onderzoek toont aan dat deepfakes een groeiende en veelzijdige bedreiging vormen voor de democratische veiligheid. Waar de technologie ooit bedoeld was voor innovatie en creatief gebruik, blijkt dat deepfakes steeds vaker worden ingezet om te misleiden, te manipuleren of twijfel te zaaien. De hoofdvraag: “In hoeverre vormen deepfakes een bedreiging voor democratische veiligheid en verkiezingsintegriteit?” kan als volgt worden beantwoord: deepfakes vormen een enorme en toenemende bedreiging voor de betrouwbaarheid van informatie en daarmee voor het functioneren van de democratie zelf. Dit heeft een directe, negatieve impact op de integriteit van verkiezingen.

De betogende analyse toont aan dat deze dreiging zich op drie verschillende niveaus manifesteert. Allereerst schaden deepfakes het vertrouwen van het publiek: mensen zijn onzeker over de authenticiteit van audiovisueel materiaal, wat resulteert in wantrouwen tegenover media en politieke instellingen. Daarnaast bevorderen sociale media de verspreiding van deepfakes door middel van algoritmen die sensatie en emoties waarderen, wat leidt tot een snellere verspreiding van misleidende beelden dan echte informatie. Daarnaast blijkt dat de huidige detectiesystemen, het beleid voor moderatie en de juridische richtlijnen nog niet genoeg bescherming bieden.

De huidige interventies, zoals de AI Act met daarin de transparantieplichting, de ontwikkeling van watermerk- en detectietools, en educatieve initiatieven gericht op digitale geletterdheid zijn waardevolle stappen in de goede richting. Toch blijft de aanpak in de praktijk onvoldoende: maatregelen worden vaak afzonderlijk genomen, zonder een gezamenlijke strategie die technologie, beleid en maatschappij met elkaar verbindt. Dit benadeelt de effectiviteit van de maatregelen en voorkomt de beoogde preventieve werking. Om de democratische veiligheid structureel te versterken, zijn aanvullende stappen nodig die zowel technisch als maatschappelijk van aard zijn. De volgende aanbevelingen kunnen daaraan bijdragen:

1. Ontwikkel een Europese standaard voor detectie en labeling van deepfakes. Door consistente richtlijnen op te stellen voor watermerken en AI-detectie, kunnen platforms en overheden effectiever samenwerken en misleiding sneller opsporen.
2. Richt een onafhankelijk toezichtsorgaan op voor digitale authenticiteit. Een instantie die toezicht houdt op de naleving van de AI Act en coördineert tussen diverse lidstaten kan de handhaving verbeteren en de grensoverschrijdende verspreiding effectiever bestrijden.
3. Vergroot digitale weerbaarheid via structureel onderwijs. Digitale geletterdheid moet een vaste plek krijgen in het onderwijs en publieke voorlichting. Burgers moeten leren hoe ze de echtheid van informatie kunnen beoordelen, vooral tijdens verkiezingsperiodes waarin de juistheid en volledigheid van informatie cruciaal is. Deepfakes zijn dus niet alleen een technisch fenomeen, maar ook een kwestie van maatschappelijke veiligheid.

die het fundament van de democratie aantast. Samenwerking tussen de overheid, technologiebedrijven, het onderwijs en de bevolking is de enige manier om het vertrouwen in informatie en instellingen te herstellen. Een werkwijze die gebaseerd is op verantwoordelijkheid, transparantie en leren kan bijdragen aan het waarborgen van de democratie, vooral nu het steeds moeilijker wordt om echt van nep te onderscheiden.

Literatuurlijst

Birrer, A. (2024). What we know and don't know about deepfakes: A systematic review of empirical research. *Social Media + Society*, 10(4), 20563051241253138. Geraadpleegd op 12 oktober 2025, van <https://journals.sagepub.com/doi/full/10.1177/14614448241253138>

Citron, D. K., & Chesney, R. (2019, januari). Deepfakes and the new disinformation war. *Foreign Affairs*. Geraadpleegd van https://scholarship.law.bu.edu/shorter_works/76/

ECP. (2024, 5 juni). AI en verkiezingen: Netwerk Mediawijsheid. ECP. Geraadpleegd op 16 oktober 2025, van <https://ecp.nl/ai-en-verkiezingen-netwerk-mediawijsheid>

Fernandez, P., Elsahar, H., Yalniz, I. Z., & Mourachko, A. (2024, 12 december). Video Seal: Open and video watermarking. Meta, van <https://ai.meta.com/research/publications/video-seal-open-and-efficient-video-watermarking>

InView. (z.d.). Bedrijfsjuridische berichten: Vermelding gebruik AI bij AI-gegenereerde content. Geraadpleegd op 6 oktober 2025, https://www.inview.nl/document/idb5430cfe028b47ab947ac67118f70aaa/bedrijfsjuridisch-e-berichten-vermelding-gebruik-ai-bij-ai-gegenereerde-content?ctx=WKNL_CSL_15&tab=tekst&searchid=3443589640

Mediawijsheid.nl. (z.d.). Lesmateriaal. Mediawijsheid.nl. Geraadpleegd op 16 oktober 2025, van <https://www.mediawijsheid.nl/lesmateriaal>

Netwerk Mediawijsheid. (2025, 9 oktober). Blijf scherp, stem bewust: Campagne tegen desinformatie in verkiezingstijd. Netwerk Mediawijsheid. Geraadpleegd op 16 oktober 2025, van <https://netwerkmediawijsheid.nl/blijf-scherp-stem-bewust-campagne-desinformatie-verkiezingstijd>

NOS. (2024, 24 mei). Deepfakes politici op Meta en X, ondanks afspraken over weren ervan. NOS. Geraadpleegd op 6 oktober 2025, van <https://nos.nl/artikel/2521690-deepfakes-politici-op-meta-en-x-ondanks-afspraken-over-weren-ervan>

Rathenau Instituut. (2020, 13 oktober). Digitale dreigingen voor de democratie: Over nieuwe technologie en desinformatie. Den Haag. Geraadpleegd op 13 oktober 2025, van <https://www.rathenau.nl/nl/digitalisering/digitale-dreigingen-voor-de-democratie>

van Vaccari, C. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video messages. *Social Media + Society*, 6(2), 2056305120903408. Geraadpleegd op 12 oktober 2025, van <https://journals.sagepub.com/doi/10.1177/2056305120903408>

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 3–15. Geraadpleegd op 12 oktober 2025, van https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20%20D%20-%20Final.pdf

Yasar, K., Barney, N., & Wigmore, I. (2025, 22 mei). What is deepfake technology? TechTarget. Geraadpleegd op 6 oktober 2025, <https://www.techtarget.com/whatis/definition/deepfake>

Doxing van politieagenten

Maike Berkenpas

Master Veiligheid en Digitalisering, Hogeschool Saxion

1. Inleiding

1.1 Achtergrond

Volgens MacAllister (2017) is doxing een vorm van cyberintimidatie waarbij persoonsgegevens van iemand openbaar worden gemaakt. Dit kan gaan om een adres, telefoonnummer, werkgever of gegevens van familieleden, vaak met de intentie om diegene te intimideren, vernederen, bedreigen of te straffen (Douglas, 2016). De term is vermoedelijk afkomstig uit de hackercultuur en afgeleid van 'docs' of documenten (Van Huijstee et al., 2021). Doxing staat vaak niet op zichzelf, maar maakt onderdeel uit van bredere vormen van online intimidatie, zoals wraakporno en bedreiging (Van Huijstee et al., 2021).

Volgens Douglas (2016) is informatie die gebruikt wordt voor doxing veelal publieke informatie, maar sommige informatie is verspreid over verschillende bronnen en moeilijk te vinden. Door deze informatie te verzamelen en te combineren kan alsnog een gedetailleerd beeld van een persoon worden opgebouwd. Daarnaast kunnen deze gegevens ook afkomstig zijn uit overheids- of organisatiebestanden die via een beveiligingslek zijn verkregen (Douglas, 2016). Doxing wordt al gesignaleerd sinds begin jaren 2000, maar het fenomeen is tijdens de coronapandemie meer zichtbaar geworden (Van Huijstee et al., 2021). Het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) publiceerde in 'het Dreigingsbeeld Terrorismen' (2020) dat woede en ontevredenheid over coronamaatregelen ervoor hebben gezorgd dat activisten meer persoonsgegevens hebben gedoxed over mensen die werken bij de politie of politici. Dit is ingezet als intimidatietactiek (Von Piekartz, 2020).

Voorbeelden uit de praktijk. In januari 2021 werden undercoveragenten ('Romeo's') massaal gedoxed omdat zij werden gezien als vertegenwoordigers van de coronamaatregelen (Von Piekartz & Bahara, 2021). Tijdens de avondklokrellen werd de onlinejacht op de undercoveragenten in Telegram- en Facebookgroepen geïntensiveerd. Hierdoor werden enkele adresgegevens van agenten bekend. Bij één agent is een vuurwerkbom in de tuin gegooid, zijn kinderen waren thuis. Dit laat zien dat doxing een ernstige vorm van online intimidatie is, het raakt direct aan iemands fysieke veiligheid (Von Piekartz & Bahara, 2021). Een recenter voorbeeld zijn de meerdaagse protesten in Apeldoorn tegen de opening van een asielzoekerscentrum. Hierbij is een verdachte aangehouden op verdenking van doxing (Politie, 2026b).

Politie in de Maatschappij. Onze democratie en rechtsstaat lijken vanzelfsprekend, maar vereisen voortdurend onderhoud. Maatschappelijke ontwikkelingen zoals internationalisering, digitalisering en opkomst van sociale media hebben hier een belangrijke invloed op (Ministerie van Justitie en Veiligheid,

2023). De politiefunctie is een essentiële pijler van de democratische rechtsstaat en richt zich op het handhaven van normen en regels en het beschermen van burgers. Hoewel de politie hierin een centrale rol vervult, dragen ook andere publieke en private partijen bij aan het beschermen van burgers en de handhaving van openbare orde en veiligheid (Bijleveld et al., 2021). Binnen die politiefunctie speelt de politie een centrale rol. Dit blijkt onder meer uit het feit dat het geweldsmonopolie van de democratische gelegitimeerde overheid is toebedeeld aan de politie en de krijgsmacht (Ministerie van Justitie en Veiligheid, 2023).

1.2 Aanleiding

Het *Wetboek van Strafrecht* (2024, Artikel 285d) stelt doxing strafbaar. Sindsdien worden ook doxingzaken van politieagenten geregistreerd. In 2024 ging het om 23 zaken en in 2025 om 27 zaken (Politie, 2026a). De politiecijfers geven niet duidelijk weer of het gaat om meldingen of strafzaken. Daarom zijn ook cijfers van het Openbaar Ministerie (OM) relevant. Het OM behandelde in 2024 40 doxingzaken en in 2025 101 zaken (*Kamerstukken II*, 29628, nr. 1318, 2026). Hoewel niet bekend is hoeveel zaken politieagenten betroffen, wijzen deze cijfers op een toename van doxing. Gezien de centrale rol van de politie binnen de democratische rechtsstaat roept dit de vraag op welke gevolgen doxing heeft voor politieagenten en de uitvoering van de politietaak.

1.3 Doel- en vraagstelling

Het doel van deze probleemanalyse is om inzicht te verkrijgen in de aard, oorzaken en gevolgen van doxing van politieagenten en de mogelijke impact hiervan op publieke waarden en de democratische rechtsstaat.

De hoofdvraag luidt als volgt:

Hoe vormt doxing van politieagenten een bedreiging voor de democratische rechtsstaat?

1. Hoe manifesteert doxing van politieagenten zich in de praktijk?
2. Welke factoren verklaren waarom politieagenten worden gedoxed?
3. Welke gevolgen heeft doxing op de uitvoering van de politietaak en hoe raakt dit het functioneren van de democratische rechtsstaat?

1.4 AI-verantwoording

Er is gebruik gemaakt van ChatGPT (OpenAI, 2026), uitsluitend als controle middel voor taal, spelling en grammatica fouten. De gegenereerde output is kritisch beoordeeld en waar nodig aangepast of niet overgenomen zodat de inhoud en conclusies het resultaat blijven van eigen werk.

2. Methoden

In dit hoofdstuk worden de onderzoeksmethoden beschreven die zijn toegepast in deze probleemanalyse.

2.1 Deskresearch en literatuuronderzoek

Deskresearch is een onderzoeksmethode waarbij gebruik wordt gemaakt van bestaande bronnen en documenten om een onderzoeksvraag te beantwoorden (Baarda et al., 2021). Er is gebruik gemaakt van overheidsdocumenten, zoals beleidsdocumenten, onderzoeken en een kamerbrief. Ook zijn Nederlandse en Europese wet- en regelgeving meegenomen.

Literatuuronderzoek draagt bij aan een beter begrip van het vraagstuk en biedt een wetenschappelijke basis voor interpretaties en conclusies (Baarda et al., 2021). In deze probleemanalyse is gekozen voor een interdisciplinaire benadering, waarbij inzichten vanuit rechtswetenschap, psychologie, criminologie en bestuurskunde zijn gecombineerd.

Voor het verzamelen van literatuur is gebruikgemaakt van verschillende databanken, waaronder Google Scholar, ResearchGate en de bibliotheek van Saxion Hogeschool. Via de bibliotheek zijn Nexus Uni, ScienceDirect, Springer Link en IEEE geraadpleegd. Deze databanken zijn geselecteerd omdat zij toegang bieden tot wetenschappelijke en peer-reviewed artikelen. Daarnaast is gebruikgemaakt van reeds bekende literatuur.

Alle zoektermen zijn zowel in het Nederlands als Engels gebruikt. In Tabel 1 worden per deelvraag de Nederlandse en Engelse zoektermen weergegeven en is kort ingegaan op de thema's van deze probleemanalyse. Daarnaast is gebruik gemaakt van sneeuwbal methode, waarbij vanuit reeds gevonden literatuur wordt doorverwezen naar andere relevante bronnen. Deze methode is toegepast om aanvullende literatuur te verzamelen die aansluit bij de onderzoeksvragen en centrale thema's van dit onderzoek.

Voor de inclusie- en exclusiecriteria is gekeken naar de relevantie van bronnen voor de onderzoeksthema's. Waar mogelijk is gebruikgemaakt van recente en peer-reviewed artikelen. Oudere publicatiedatums zoals die van Suler (2004), Bandura (1999) en Sykes en Matza (1957) zijn meegenomen vanwege de theoretische waarde van de publicatie. Bronnen zijn uitgesloten wanneer deze geen betrouwbare herkomst hadden, bijvoorbeeld wanneer bronvermelding niet gekoppeld was aan uitspraken.

De belangrijkste theoretische uitgangspunten zijn gebaseerd op onder meer Douglas (2016), Trottier (2017), Suler (2004), Bandura (1999), Sykes en Matza (1957), Huey et al. (2025), Shjarback (2017) en Capellan et al. (2020).

Tabel 1

Zoektermen en thema's per deelvraag

Deelvraag (DV)	Nederlandse zoektermen	Engelse zoektermen	Thema's
DV 1 manifestatie	Doxing, doxxing, vormen, classificatie, sociale media, online intimidatie, digitaal vigilantisme, politieagenten	Doxing, doxxing, classification, social media, online harassment, digital vigilantism, police officers	Typen doxing en rol van sociale media bij doxing
DV 2 verklaringen	Doxing, neutralisatietechnieken, morele ontkoppeling, online ontremmingseffect, motieven, verklaringen	Doxing, doxxing, neutralization techniques, moral disengagement, online disinhibition effect, motives, explanations	Factoren en mechanismen achter doxing
DV 3 gevolgen	Democratische rechtsstaat, publieke waarden, grondrechten, privacy, veiligheid, legitimiteit, openbare orde, handhaving, de-policing	Rule of law, public values, policing, privacy, safety, legitimacy, public order, law enforcement, de-policing	Effecten en gevolgen van doxing op politietaak, politieorganisatie en democratische rechtsstaat

2.2 Validiteit en betrouwbaarheid

Validiteit heeft betrekking op de mate waarin het onderzoek daadwerkelijk meet of onderzoekt wat beoogd wordt. Betrouwbaarheid heeft betrekking op de mate waarin de onderzoeksresultaten consistent zijn en niet worden beïnvloed door toevallige factoren (Baarda et al., 2021). De validiteit is versterkt door de zoektermen en thema's af te stemmen op de hoofd- en deelvragen en bronnen te selecteren op relevantie. De betrouwbaarheid is vergroot door gebruik te maken van peer-reviewed artikelen en officiële bronnen, zoals wetgeving en beleidsdocumenten van de overheid. Bronnen zonder betrouwbare herkomst zijn uitgesloten.

3. Manifestatie van doxing

In dit hoofdstuk wordt de eerste deelvraag beantwoord. In paragraaf 3.1 toelichting gegeven op verschillende typen doxing en rol van sociale mediaplatforms.

3.1 Classificatie van doxing

Douglas (2016) categoriseert doxing op drie verschillende manieren namelijk: deanonimisering, targetting en delegitimiserend. Deanonimisering houdt in dat persoonsgegevens openbaar worden gemaakt waardoor een voorheen anonieme persoon identificeerbaar wordt (Douglas, 2016). Een voorbeeld hiervan zijn undercoveragenten die tijdens de coronaprotesten werden gedoxed, waardoor ze niet langer anoniem konden opereren (zie subparagraaf 1.1.1).

Targetting doxing betreft het openbaar maken van informatie waarmee een slachtoffer fysiek gelokaliseerd kan worden, zoals adresgegevens. Hierdoor neemt het risico op fysieke intimidatie toe (Douglas, 2016). Targetting doxing volgt vaak na deanonimisering, dit komt omdat de identiteit eerst bekend moet zijn voordat locatiegegevens kunnen worden verspreid (Douglas, 2016). In het eerste voorbeeld uit hoofdstuk 1 werd zelfs een vuurwerkbom in een tuin van een agent gegooit.

Bij delegitimiserende doxing worden persoonsgegevens openbaar gemaakt om de reputatie of geloofwaardigheid van een slachtoffer te ondermijnen (Douglas, 2016). Deze vorm van doxing gaat vaak gepaard met targetting doxing. Het verschil is dat de delegitimiserende vorm 'bewijs' levert om een persoon te targetten (Douglas, 2016). De doxing van de undercoveragenten tijdens de coronaprotesten kan ook als delegitimiserend worden gezien, zij werden online neergezet als vertegenwoordigers van het coronabeleid en daarmee gezien als legitiem doelwit van vergelding (Von Piekartz & Bahara, 2021).

3.2 Digitaal vigilantisme en online platforms

Digitaal vigilantisme (DV) wordt door Trottier (2017) omschreven als een proces waarbij burgers collectief verontwaardigd raken over het gedrag van andere burgers en daarop reageren door middel van gecoördineerde vergeldingsacties via digitale media, waaronder mobiele apparaten en sociale mediaplatforms. Onder andere omvat het publiekelijk 'naming and shaming', waarbij personen openlijk aan de schandpaal kunnen worden genageld (Trottier, 2017). Volgens Trottier (2017) moet DV gezien worden binnen een onlinecultuur waarin burgers zich gemakkelijk kunnen organiseren via het internet. Daarnaast leven we in een samenleving waarin steeds meer informatie digitaal beschikbaar is. Trottier benoemt dat binnen deze context DV kan leiden tot schadelijk gedrag, zoals online intimidatie, cyberpesten en doxing (2017). Verder wordt DV mogelijk gemaakt doordat op digitale platforms het makkelijk is om gezamenlijk in actie te komen. Mensen kunnen zich dus snel verzamelen en informatie delen, zonder dat daar veel controle op is (Slavkovik et al., 2015).

Volgens Trottier (2017) faciliteren sociale mediaplatforms zoals Facebook, X (voorheen Twitter) en Reddit dat informatie over een bepaald doelwit wordt besproken, persoonlijke gegevens te publiceren en anderen op te roepen tot actie. Bovendien maken mobiele apparaten (zoals smartphones) het mogelijk om ongewenst gedrag in 'real time' vast te leggen en direct online te publiceren (Trottier, 2017).

4. Verklaring van doxing

In dit hoofdstuk wordt de tweede deelvraag beantwoord. In paragraaf 4.1 de motieven van doxing toegelicht en in paragraaf 4.2 zijn mechanismen en factoren van het plegen van doxing uitgelegd.

4.1 Motieven om te doxen

Er zijn verschillende motieven om iemand te doxen. MacAllister (2017) stelt dat doxing gebaseerd is op de intentie van de doxer. Zij benoemt de term 'punching down doxing' wat betekent dat doxing wordt uitgevoerd met kwaadaardige bedoelingen. Doxing kan ook uitgevoerd worden voor politieke doeleinden. Dit wordt gedaan als een middel om transparantie te vergroten, vermeende onrechtvaardigheid bloot te leggen of nieuwswaardige informatie voor het publieke belang aan het licht brengen. Dit kan bijvoorbeeld gaan over multinationals, leger of racistische politieagenten. De laatste categorie die MacAllister (2017) benoemd is 'unmasking'. Hierbij wordt doxing gebruikt als een middel voor interne regulering door leden van onlinegemeenschappen (zoals hackers en forums). Hackers gebruiken doxing om de identiteit van mede-hackers te onthullen die om welke reden dan ook in opspraak is geraakt bij de andere in de gemeenschap. Daarentegen beschouwt Trottier (2017) doxing als een vorm van DV waarbij individuen recht proberen te bereiken door gebeurtenissen aan de kaak te stellen die juridische en morele grenzen hebben overschreden.

Enkele andere motieven die Huey et al. (2025) benoemen zijn toegespitst op doxen van politieagenten, zoals het onder druk zetten en bedreigen van politieagenten, wat mogelijk kan voorkomen dat zij hun taken effectief kunnen uitvoeren. Breder gezien kunnen doelen van het doxen van politieagenten ook zijn om de samenleving te ontregelen, het uitlokken van harde reactie van autoriteiten en steun krijgen voor bepaalde doelen door daders te presenteren die opkomen voor een onderdrukkende overheid.

4.2 Mechanismen achter doxing

Het is belangrijk om bestaande literatuur te koppelen aan redenen voor doxing. Op die manier wordt inzicht gegeven waarom daders zich schuldig maken aan doxing. In deze paragraaf wordt daarom ingegaan op de theorie 'online disinhibition effect' van Suler, de neutralisatietechnieken van Sykes en Matza en moral disengagement theorie van Bandura. Vervolgens wordt bij elke theorie een koppeling gegeven aan doxing.

Online disinhibition effect. Volgens Suler (2004) gedragen mensen zich online minder geremd dan offline, dit noemt hij ook wel 'online disinhibition effect'. Er zijn drie belangrijke factoren die de vermindering van remmingen en controle kunnen verklaren. De eerste factor is anonimiteit. Wanneer individuen hun online gedrag kunnen loskoppelen aan hun offline identiteit en leven maken zij zich minder zorgen over hun gedrag of het delen van persoonlijke informatie (Suler, 2005). De tweede

factor is onzichtbaarheid, want in veel online situaties kunnen mensen elkaar niet zien. Het ontbreken van oogcontact en communicatie face-to-face zorgt ervoor dat mensen zich minder geremd voelen en anders kunnen gedragen (Suler, 2005). En de derde factor is asynchroniteit, communicatie online is vaak asynchroon. Dit betekent dat er geen tijds- of plaatsgebonden beperkingen zijn. Mensen hoeven niet per se met elkaar te communiceren op hetzelfde moment (Suler, 2005).

Neutralisatietechnieken. Volgens Sykes en Matza (1957) rechtvaardigen daders schadelijk gedrag via neutralisatietechnieken. Een eerste techniek is ontkenning van verantwoordelijkheid, waarbij gedrag wordt toegeschreven aan externe omstandigheden of druk van anderen (Mckie, 2019). Daarnaast kan sprake zijn van ontkenning van schade, waarbij de gevolgen worden gebagatelliseerd (Agnew & Peters, 1986). Dit sluit aan bij de online disinhibition effect van Suler (2004), waarbij online gedrag minder echt voelt en de gevolgen voor anderen minder zichtbaar lijken. Een andere neutralisatietechniek is ontkenning van het slachtoffer, waarbij daders vinden dat het slachtoffer het gedrag verdient (McKie, 2019; Moore & McMullan, 2009). Bij doxing kan dit voorkomen wanneer politieoptreden online wordt verspreid en agenten als schuldige worden gezien. De vierde techniek is veroordeling van de veroordelaars. Dit verwijst naar het verschuiven van de schuld naar degenen die het gedrag afkeuren (Sykes & Matza, 1957). In dit geval kan dat de politie of overheid zijn. Tot slot kan sprake zijn van beroep op hogere loyaliteiten, waarbij gedrag wordt gerechtvaardigd vanuit trouw aan een groep of ideologie die belangrijker wordt gevonden dan de wet (Sykes & Matza, 1957; Siponen et al., 2020). Dit is zichtbaar in het voorbeeld uit paragraaf 1.1.1. Waarbij undercoveragenten werden gezien als de vertegenwoordigers van de coronamaatregelen, waardoor daders hun handelen rechtvaardigden als verzet tegen overheidsbeleid.

Moral disengagement. Bandura (1999) was een van de eerste die het concept *moral disengagement* heeft uitgewerkt. Moral disengagement is een proces waarbij individuen hun interne morele normen verzwakken om schadelijk gedrag te rechtvaardigen (Bandura 1999; Wang & Ngai, 2020). Met andere woorden praten mensen hun gedrag goed, ook al weten ze dat het eigenlijk verkeerd is. Wat belangrijk is dat de situatie waarin iemand bevindt invloed kan hebben op hoe makkelijk dit gebeurt (Corkum & Shead, 2025). Online is het vaak makkelijker om je moreel te ontkoppelen, omdat communicatie snel verloopt en mensen anoniem kunnen blijven (Parlangeli et al., 2019). Toegepast op doxing kan moral disengagement verklaren waarom daders de negatieve gevolgen bagatelliseren en hun gedrag als gerechtvaardigd beschouwen.

Koppeling theorieën. De hierboven besproken theorieën vullen elkaar aan in het verklaren waarom mensen doxen. Hierbij richten de theorieën zich wel op verschillende aspecten. Zo wordt in paragraaf 4.2.1 vooral een verklaring gegeven vanuit verschillende factoren die kunnen bijdragen aan het ontstaan van gedrag online. De theorieën in paragraaf 4.2.2 en 4.2.3 richten zich beiden op het rechtvaardigen van schadelijk gedrag. Moral disengagement is een breder en

abstracter proces waarbij personen bijvoorbeeld kunnen geloven dat doxing gerechtvaardigd is om onrecht aan het licht te brengen. Terwijl neutralisatietechnieken concretere rechtvaardigingen bieden, zoals het bagatelliseren van de schade of beschuldigen van het slachtoffer (McCormack & Chowdhury, 2024). De toepassing van deze theorieën is een eigen analytische interpretatie op basis van de literatuur.

5. De politietaak en de democratische rechtsstaat

In dit hoofdstuk wordt de derde deelvraag beantwoord. Het hoofdstuk bespreekt de gevolgen van doxing voor de uitvoering van de politietaak (paragraaf 5.1) en de democratische rechtsstaat (paragraaf 5.2).

5.1 Politietaak in de democratische rechtsstaat

In Nederland leven we in vrijheid in een democratische rechtsstaat. In een democratische rechtsstaat ligt de uiteindelijke macht bij het volk, terwijl de overheid gebonden blijft aan het recht (Raad voor het Openbaar Bestuur, 2020). Het zorgt ervoor dat het recht waaraan de staat is gebonden voortkomt uit de wil van het volk en de rechtsstaat waarborgt vervolgens dat deze democratische gelegitimeerde macht niet misbruik maakt van hun macht (Raad voor het Openbaar Bestuur, 2020). De politie heeft drie kerntaken: beschermen, begrenzen en bekrachtigen. Beschermen houdt in dat de politie optreedt in noodsituaties om de veiligheid van burgers te waarborgen. Begrenzen richt zich op het stoppen en beheersen van ongeoorloofd gedrag. Bekrachtigen betekent het ondersteunen van gewenst gedrag door samenwerking met burgers en andere organisaties te bevorderen om veiligheid te waarborgen (Politie, z.d.). Met betrekking tot deze deelvraag zijn vooral de kerntaken beschermen en begrenzen van toepassing.

5.2 Gevolgen van doxing op democratische rechtsstaat

De *Politiewet 2012* (2013, Artikel 3) bepaalt dat de politie belast is met de handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Het uitvoeren van politietaken op het gebied van openbare orde kan ertoe leiden dat politieagenten en hun familie door doxing worden blootgesteld aan intimidatie en verlies van privacy. Volgens Capellan et al. (2020) kan externe druk vanuit media, politiek en publiek leiden tot de-policing. De-policing verwijst naar een situatie waarin politieagenten minder proactief optreden om de kans te verkleinen dat zij betrokken raken bij controversiële incidenten (Shjarback, 2017). Minder proactief optreden kan zich uiten in het minder snel uitvoeren van controles, onderzoeken te doen of geweld te gebruiken (Mourtgos & Adams, 2019; Rosenfeld & Wallman, 2019; Shjarback et al., 2017; Wolfe & Nix, 2016). Dit kan bijvoorbeeld zichtbaar worden bij demonstraties of openbare ordeverstoringen. Bij terughoudender optreden kan dit de handhaving van de openbare orde bemoeilijken en gevolgen hebben voor de veiligheid van omstanders en politieagenten. Daarbij kan de-policing

indirect gevolgen hebben voor de legitimiteit van de politie. Legitimiteit heeft betrekking op de erkenning van het gezag en de bevoegdheden van de politie door burgers (Beetham, 1991). Wanneer doxing leidt tot terughoudender optreden en het gezag van de politie onder druk komt te staan, kan dit gevolgen hebben voor het functioneren van het openbare orde- en veiligheidssysteem. In de Leidraad risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid van het Analistennetwerk Nationale Veiligheid (2022) wordt dit beschreven onder impactcriterium 5.2. Volgens deze leidraad kan online en offline intimidatie van openbare orde- en veiligheidsfunctionarissen een aantasting vormen van het openbare orde- en veiligheidssysteem binnen een democratische rechtsstaat (Analistennetwerk Nationale Veiligheid, 2022). Doxing van politieagenten past binnen deze categorie, omdat het gericht is op intimidatie en beïnvloeding van agenten.

De ernst van doxing blijkt ook uit de strafbaarstelling in het *Wetboek van Strafrecht* (2024, Artikel 285d). Specifiek in het tweede lid van dit artikel (*Wetboek van Strafrecht*, 2024, Artikel 285d, lid 2) is bepaald dat een zwaardere straf kan worden opgelegd wanneer het feit wordt gepleegd tegen onder andere politieagenten in uitoefening van hun functie. Deze wettelijke bescherming weerspiegelt het belang van de publieke waarden die door doxing onder druk kunnen staan. Privacy en veiligheid zijn publieke waarden die binnen de democratische rechtsstaat worden beschermd. Volgens Rutgers (2011) raken deze waarden het algemeen belang en geven richting aan hoe de samenleving is ingericht en functioneert. Volgens artikel 10 van de *Grondwet* heeft iedereen recht op het respecteren van zijn persoonlijke levenssfeer. De wet stelt regels ter bescherming van deze persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens (*Grondwet*, 2023, Artikel 10, lid 2). Ook in het *Europees Verdrag voor de Rechten van de Mens* (EVRM) wordt deze wet bevestigd onder artikel 8 (1950, Artikel 8). Dit artikel stelt dat iedereen het recht heeft op respect van zijn privéleven, familie- en gezinsleven, eigen woning en correspondentie. Doxing, het zonder toestemming openbaar maken van persoonlijke gegevens, staat haaks op deze fundamentele rechten en vormt daarmee een directe inbreuk op deze publieke waarden binnen de democratische rechtsstaat.

6. Conclusie en oplossingsrichtingen

In dit hoofdstuk wordt ingegaan op de conclusie van de probleemanalyse en worden oplossingsrichtingen aangedragen om doxing tegen te gaan.

6.1 Conclusie

Uit de probleemanalyse blijkt dat doxing van politieagenten een bedreiging kan vormen voor de democratische rechtsstaat. Er bestaan verschillende typen doxing. Deze vormen van doxing leiden tot online intimidatie, maar kunnen zich ook ontwikkelen tot offline bedreigingen en geweld. Sociale mediaplatforms spelen een

belangrijke rol doordat zij het eenvoudig maken om persoonsgegevens te verzamelen, verspreiden en anderen te mobiliseren.

Verschillende factoren kunnen verklaren waarom politieagenten worden gedoxed. Daders kunnen handelen vanuit uiteenlopende motieven, zoals vergelding, politieke overtuigingen of het blootleggen van vermeend onrecht. Daarnaast bieden online omstandigheden, zoals anonimiteit en asynchrone communicatie, mogelijkheden om minder geremd te handelen.

De gevolgen van doxing reiken verder dan het individuele slachtoffer. Naast het verlies van privacy kunnen politieagenten geconfronteerd worden met intimidatie en bedreigingen. Daardoor kunnen zij terughoudender optreden in de uitvoering van hun werkzaamheden. De politie vervult namelijk een centrale rol binnen de democratische rechtsstaat door de handhaving van de openbare orde en veiligheid. Daarnaast vormt doxing een inbreuk op fundamentele publieke waarden zoals privacy en veiligheid. Deze waarden worden beschermd in de Grondwet en EVRM. Daarom kan worden geconcludeerd dat doxing van politieagenten niet alleen een vorm van online intimidatie is, maar ook een fenomeen dat publieke waarden aantast en het functioneren van de democratische rechtsstaat onder druk kan zetten.

6.2 Oplossingsrichtingen

Preventie. Volgens Huey et al. (2025) is een belangrijk uitgangspunt het verbeteren van educatie en training voor politieagenten gericht op het beschermen van hun persoonsgegevens. Daarnaast is het van belang dat agenten leren omgaan met situaties waarin zij te maken krijgen met online intimidatie, zoals doxing. Dit omvat onder andere training in digitale hygiëne, het gebruik maken van veilige communicatieplatforms en het verwijderen van informatie uit openbaar toegankelijke databanken. Deze preventieve maatregelen zijn relevant omdat uit de literatuur blijkt dat doxing plaatsvindt met persoonsgegevens die relatief eenvoudig kunnen worden verzameld (Douglas, 2016). Volgens Huey et al. (2025) ligt de verantwoordelijkheid voor het versterken van de digitale weerbaarheid zowel bij de politieorganisatie als bij individuele politieagenten. Dit vraagt om zowel persoonlijke voorzorgsmaatregelen als organisatorische ondersteuning en beleid. Tevens wordt dit onderstreept in de brief van Minister van Justitie en Veiligheid in maart 2025 aan de Tweede Kamer dat de politie blijft investeren in het vergroten van bewustzijn van politiemedewerkers (*Kamerstukken II, 29628, nr. 1318, 2026*)

Rol sociale media platforms. Naast de strafbaarstelling van doxing en preventieve maatregelen binnen de politieorganisatie, moeten sociale mediabedrijven verantwoordelijkheid dragen voor het tegengaan van doxing. Volgens een lid van het College van procureurs-generaal is doxing een maatschappelijk probleem dat niet uitsluitend via het strafrecht kan worden opgelost (OM, 2023). Volgens dit lid hebben sociale mediabedrijven daarom ook een belangrijke rol bij het beperken van strafbare uitingen online (OM, 2023). Oderkerken et al. (2025) stellen dat techbedrijven een sleutelrol hebben bij de aanpak van online geweld, waaronder intimidatie, bedreiging en doxing. Dit sluit aan bij de ontwikkeling dat de politiefunctie niet langer uitsluitend door de politie wordt uitgevoerd. Volgens Bijleveld et al. (2021) wordt deze *non-police policing* sector steeds groter. Omdat persoonsgegevens zich snel tussen verschillende online platforms verspreiden, is publiek-private samenwerking tussen techbedrijven, overheid en maatschappelijke organisaties

noodzakelijk. Duidelijke afspraken maken over monitoring, data-uitwisseling en gezamenlijke normen zijn noodzakelijk om schadelijk gedrag en online geweld effectief over verschillende platforms heen te bestrijden (Oderkerken et al., 2025). Door sneller in te grijpen bij het delen van persoonsgegevens en het verwijderen van schadelijke content, kan de escalatie van online naar offline intimidatie worden beperkt. Dit sluit aan bij eerdere benoemde bevindingen dat sociale media een belangrijke rol spelen in de verspreiding en mobilisatie van doxing (Trottier, 2017; Slavkovik et al., 2015).

7. Kritische reflectie

De probleemanalyse laat zien dat doxing van politieagenten op gespannen voet staat met fundamentele publieke waarden, zoals privacy, veiligheid en het goed functioneren van de democratische rechtsstaat. Tegelijkertijd laat de analyse zien dat het vraagstuk complexer is dan alleen een overtreding van de wet. Daders kunnen doxing beschouwen als een middel om vermeend onrecht zichtbaar te maken of publieke verantwoording af te dwingen (Sykes & Matza, 1957). Hoewel deze motieven vanuit hun perspectief begrijpelijk kunnen lijken, rechtvaardigt dit niet het openbaar maken van persoonsgegevens. Echter zijn de consequenties onvermijdelijk. Niet alleen kunnen politieagenten en hun omgeving geconfronteerd worden met veiligheidsrisico's, ook de uitvoering van de politietaak op het gebied van openbare orde en veiligheid kan onder druk komen te staan. Hierdoor kan tevens het vertrouwen en gezag dat nodig is voor een effectieve uitoefening van de politiefunctie aangetast worden (Politie, 2022).

De strafbaarheidstelling van doxing is niet voldoende om doxing te verminderen. De voorgestelde oplossingsrichtingen richten zich op versterken van digitale weerbaarheid van politieagenten en beperken van verspreiding van persoonsgegevens, maar kennen tegelijkertijd ook beperkingen. Het vergroten van digitale weerbaarheid van politieagenten vraagt blijvende investeringen van de politieorganisatie, ondanks capaciteitsproblemen (Wijkman-van Aalst, 2025) moet tijd vrijgemaakt worden om dit goed te kunnen borgen in de organisatie. Ook kunnen persoonsgegevens door datalekken of informatie door derden worden verspreid (Douglas, 2016). Hierdoor blijft het risico bestaan, ook wanneer politieagenten zorgvuldig omgaan met hun online aanwezigheid.

Tegelijkertijd is de aanpak van doxing complex. Zoals eerder aangegeven hebben ook private partijen taken overgenomen om een aandeel te hebben bij de aanpak van criminaliteit. Hierdoor wordt het steeds lastiger om vast te stellen welke partij primair verantwoordelijk is voor het voorkomen en bestrijden van doxing. Dit wordt door Bijleveld et al. (2021) ook wel het *veiligheidscomplex* genoemd. Daarom vraagt de aanpak van doxing om samenwerking en duidelijke afspraken tussen politie, overheid en sociale mediaplatforms.

Literatuurlijst

Agnew, R., & Peters, A. A. R. (1986). The techniques of neutralization: An analysis of predisposing and situational factors. *Criminal Justice and Behavior*, 13(1), 81-97. <https://doi.org/10.1177/0093854886013001005>

Analistennetwerk Nationale Veiligheid. (2022). Rijksbrede risicoanalyse nationale veiligheid. Rijksinstituut voor Volksgezondheid en Milieu. Geraadpleegd op 25 april 2026, van <https://www.rivm.nl/nationale-veiligheid/actuele-analyses/rijksbrede-risicoanalyse-nationale-veiligheid-2022>

Baarda, B., Bakker, E., Fischer, T., Julsing, M., Kostelijk, E., & van der Velden, T. (2021). *Basisboek kwalitatief onderzoek* (5e druk). Noordhoff Uitgevers.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, 3(3), 193–209. https://doi.org/10.1207/s15327957pspr0303_3

Beetham, D. (1991). *The legitimation of power*. Macmillan Education. Via [https://psi412.cankaya.edu.tr/uploads/files/Beetham%20-%20The%20Legitimation%20of%20Power%20\(1991\).pdf](https://psi412.cankaya.edu.tr/uploads/files/Beetham%20-%20The%20Legitimation%20of%20Power%20(1991).pdf)

Bijleveld, C., Salet, R., Damstra, A., & Stéfanovic, D. (2021). Politiefunctie in een veranderende omgeving. Wetenschappelijke Raad voor het Regeringsbeleid. Geraadpleegd op 15 mei 2026, van <https://www.wrr.nl/documenten/2021/11/03/politiefunctie-in-een-veranderende-omgeving>

Capellan, J. A., Lautenschlager, R., & Silva, J. R. (2020). Deconstructing the Ferguson effect: A multilevel mediation analysis of public scrutiny, De-policing and Crime. *Journal of Crime and Justice*, 43(2), 125–144. <https://doi.org/10.1080/0735648X.2019.1652921>

Corkum, M., & Shead, N. W. (2025). Online moral disengagement: An examination of the relationships between electronic communication, cognitive empathy, and antisocial behavior on the internet. *Psychological Reports*, 128(6), 4169-4192. <https://doi.org/10.1177/00332941231216415>

Douglas, D.M. (2016). Doxing: a conceptual analysis. *Ethics Information Technology*, 18(3), 199–210. <https://doi.org/10.1007/s10676-016-9406-0>

Europees Verdrag voor de Rechten van de Mens. (1950, 1 november). Raad van Europa. Geraadpleegd op 16 mei 2026, van https://www.echr.coe.int/documents/d/echr/convention_nld

Grondwet. (2023, 22 februari). Artikel 10. Geraadpleegd op 16 mei 2026, van <https://wetten.overheid.nl/BWBR0001840/2023-02-22/0>

Hansora, P., Shah, M., Parikh, M., Ranoliya, J., Chauhan, M., & Bharvad, B. (2025). From cyberbullying to doxing: Privacy, law, and challenges in online harms. 2025 5th International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN) [Congres] (pp. 1769-1774). Institute of Electrical and Electronics Engineers. Geraadpleegd op 24 april 2026, van <https://doi.org/10.1109/ICECMSN68058.2025.11382958>

Huey, L., Ferguson, L., & Towns, Z. (2025). Cops need doxxed: Releasing personal information of police officers as a tool of political harassment. *Crime & Delinquency*, 71(3), 714-739. <https://doi.org/10.1177/00111287241271069>

Kamerstukken II, 29628, nr. 1318. (2026, 20 maart). Overheid.nl. Geraadpleegd op 13 mei 2026, van <https://zoek.officielebekendmakingen.nl/kst-29628-1318.pdf>

MacAllister, J. (2017). The doxing dilemma: Seeking a remedy for the malicious publication of personal information, *Fordham Law Review*, 85(5), 2451-2483. Geraadpleegd op 26 april 2026, van <https://ir.lawnet.fordham.edu/flr/vol85/iss5/21/>

McKie, R.E. (2019). Climate change counter movement neutralization techniques: A typology to examine the climate change counter movement. *Sociological Inquiry*, 89(2), 288-316. <https://doi.org/10.1111/soin.12246>

McCormack, R., & Chowdhury, R. M. M. I. (2024). Moral disengagement and neutralization techniques as explanations of unethical behavior. *Journal of Consumer Affairs*, 58(2), 630-662. <https://doi.org/10.1111/joca.12575>

Ministerie van Justitie en Veiligheid. (2023). Versterking van de politiefunctie [White paper]. Geraadpleegd op 16 april 2026, van <https://www.rijksoverheid.nl/documenten/rapporten/2023/12/07/tk-bijlage-1-white-paper-politiefunctie>

Moore, R., & McMullan, E. C. (2009). Neutralizations and rationalizations of digital piracy: A qualitative analysis of university students. *International Journal of Cyber*

Criminology, 3(1), 441-451. Geraadpleegd op 20 mei 2026, van <https://www.cybercrimejournal.com/pdf/mooreijcc2009.pdf>

Mourtgos, S. M., & I. T. Adams. (2019). The rhetoric of de-policing: Evaluating open-ended survey responses from police officers with machine learning-based structural topic modeling. *Journal of Criminal Justice*, 64(5), 61–73. <https://doi.org/10.1016/j.jcrimjus.2019.101627>

NCTV. (2020). Dreigingsbeeld terrorisme 53. Geraadpleegd op 26 februari 2026, van <https://www.nctv.nl/documenten/2020/10/15/dreigingsbeeld-terrorisme-nederland-53>

Oderkerken, M., De Weger, E., Yenga, M., & Woertink, D. (2025). Online geweld tussen burgers. Verwey-Jonker Instituut. Geraadpleegd op 20 mei 2026, van <https://www.verwey-jonker.nl/publicatie/online-geweld-tussen-burgers/>

OM. (2023). Doxing vanaf 1 januari 2024 strafbaar. Geraadpleegd op 1 mei 2026, van <https://www.om.nl/actueel/nieuws/2023/12/19/doxing-vanaf-1-januari-2024-strafbaar>

OpenAI. (2026). ChatGPT (Versie 5.5) [Generatieve AI]. <https://openai.com/nl-NL/index/chatgpt/>

Parlangeli, O., Marchigiani, E., Bracci, M., Duguid, A. M., Palmitesta, P., & Marti, P. (2019). Offensive acts and helping behavior on the internet: An analysis of the relationships between moral disengagement, empathy and use of social media in a sample of Italian students. *Journal of Prevention, Assessment & Rehabilitation*, 63(3), 469–477. <https://doi.org/10.3233/WOR-192935>

Politie. (2022). De Nederlandse politie, vertrouwen en reputatie. Geraadpleegd op 11 juni 2026, van <https://www.politie.nl/binaries/content/assets/politie/nieuws/2022/december/4c744dcc-8af5-4d3d-b5e9-bcc8b679884b.pdf>

Politie. (2026a, 1 mei). Meer agressie en geweld tegen politie. Geraadpleegd op 10 juni 2026, van <https://www.politie.nl/nieuws/2026/mei/1/00-meer-agressie-en-geweld-tegen-politie.html>

Politie. (2026b, 20 mei). Aanhouding in onderzoek naar doxing rond protesten Apeldoorn. Geraadpleegd op 4 juni 2026, van

<https://www.politie.nl/nieuws/2026/mei/20/02-apeldoorn-aanhouding-in-onderzoek-naar-doxing-rond-protesten-apeldoorn.html>

Politie. (z.d.). Kerntaken politie. Geraadpleegd op 16 april 2026, van <https://www.politie.nl/informatie/kerntaken-politie.html>

Politiewet 2012. (2013, 1 januari). Overheid.nl. Geraadpleegd op 4 juni 2026, van <https://wetten.overheid.nl/BWBR0031788/2026-01-23/0>

Raad voor het Openbaar Bestuur. (2020). Een sterkere rechtsstaat. Verbinden en beschermen in een pluriforme samenleving. Geraadpleegd op 31 maart 2026, van <https://www.raadopenbaarbestuur.nl/documenten/2020/04/15/een-sterkere-rechtsstaat>

Rosenfeld, R., & Wallman, J. 2019. Did de-policing cause the increase in homicide rates?. *Criminology & Public Policy*, 18 (1), 51–75. <https://doi.org/10.1111/1745-9133.12414>

RTL Nieuws. (2025, 5 februari). Korpschef bedroefd over onderduiken Utrechtse agent: 'Alle perken te buiten'. Geraadpleegd op 1 maart 2026, van <https://www.rtl.nl/nieuws/binnenland/artikel/5563913/korpschef-bedroefd-over-onderduiken-utrechtse-agent-alle-perken>

Rutgers, M. R. (2011). Het pantheon van de publieke waarden. (Oratiereeks). Universiteit van Amsterdam. Geraadpleegd op 5 april 2026, van <https://dare.uva.nl/search?identifier=40947061-1865-4f66-bc05-fe460227c3af>

Shjarback, J. A., Pyrooz, D. C., Wolfe, S. E., & Decker, S. H. (2017). De-policing and crime in the wake of Ferguson: Racialized changes in the quantity and quality of policing among Missouri police departments. *Journal of Criminal Justice*, 50(3), 42–52. <https://doi.org/10.1016/j.jcrimjus.2017.04.003>

Slavkovik, M., Dennis, L.A., & Fisher, M. (2015). An abstract formal basis for digital crowds. *Distributed Parallel Databases*, 33(1), 3–31. <https://doi.org/10.1007/s10619-014-7161-y>

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can individuals' neutralization techniques be overcome? A field experiment on password policy. *Computers and Security*, 88(1), 101617. <https://doi.org/10.1016/j.cose.2019.101617>

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, 7(3), 321–326. <https://doi.org/10.1089/1094931041291295>

- Suler, J. (2005). Contemporary media forum. *International Journal of Applied Psychoanalytic Studies*, 2(2), 184-188. <https://doi.org/10.1002/aps.42>
- Sykes, G.M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, 22(6), 664-670. <https://doi.org/10.2307/2089195>
- Trottier, D. (2017). Digital vigilantism as weaponisation of visibility. *Philosophy & Technology*, 30(1), 55-72. <https://doi.org/10.1007/s13347-016-0216-4>
- Van Huijstee, M., Nieuwenhuizen, W., Sanders, M., Masson, E., & Van Boheemen, P. (2021). Online ontspoord: Een verkenning van schadelijk en immoreel gedrag op het internet in Nederland. Rathenau Instituut. Geraadpleegd op 28 april 2026, van https://www.rathenau.nl/sites/default/files/2021-07/Rathenau_Instituut_Rapport_Online_ontspoord.pdf
- Von Piekartz, H. (2020, 15 oktober). NCTV: boosheid en ongenoegen over coronamaatregelen leiden vaker tot radicalisering. *De Volkskrant*.
- Von Piekartz, H., & Bahara, H. (2021, 26 maart). Doxing: hoe online dreigementen hun weg vinden naar de fysieke wereld. *De Volkskrant*.
- Wang, L., & Ngai, S. S. (2020). The effects of anonymity, invisibility, asynchrony, and moral disengagement on cyberbullying perpetration among school-aged children in China. *Children and Youth Services Review*, 119(3), 105613. <https://doi.org/10.1016/j.childyouth.2020.105613>
- Wetboek van Strafrecht. (2024, 1 januari). Overheid.nl. Geraadpleegd op 5 juni 2026, van <https://wetten.overheid.nl/BWBR0001854/2026-01-01/0#BoekTweede>
- Wijkman-van Aalst, T. (2025, 9 februari). Nederland heeft te weinig agenten en dat begint gevolgen te hebben. *Nu.nl*. Geraadpleegd op 11 juni 2026, van <https://www.nu.nl/algemeen/6345106/nederland-heeft-te-weinig-agenten-en-dat-begint-gevolgen-te-hebben.html>
- Wolfe, S. E., & Nix, J. (2016). The alleged ferguson effect and police willingness to engage in community partnership. *Law and Human Behavior*, 40(1), 1–10. <https://doi.org/10.1037/lhb0000164>

Het radicaliseren van jongeren in online omgevingen

Dieunée Knoll

Master Veiligheid en Digitalisering, Hogeschool Saxion

1. Inleiding

De toenemende digitalisering van de samenleving heeft invloed op de manier waarop jongeren zich ontwikkelen, informatie tot zich nemen en contact hebben met anderen (NCTV, 2025). Online omgevingen, zoals sociale media, chatgroepen, fora en gamingplatforms, vormen daardoor een steeds belangrijker onderdeel van hun leefwereld. Deze omgevingen bieden kansen voor communicatie en identiteitsvorming, maar brengen ook risico's met zich mee. Jongeren kunnen via online omgevingen in aanraking komen met eenzijdige informatie, desinformatie en extremistische denkbeelden, wat kan bijdragen aan het ontstaan van radicalisering (Whittaker, 2022, p. 28).

Deze probleemanalyse richt zich daarom op de rol van online omgevingen binnen het proces van radicaliseren onder jongeren van 14 tot en met 23 jaar. In deze levensfase zijn jongeren intensief online actief en bevinden zij zich in een fase van identiteitsontwikkeling, waardoor zij extra vatbaar kunnen zijn voor beïnvloeding (Nederlands Jeugdinstituut, 2025).

De centrale vraag van de probleemanalyse luidt waarom het radicaliseringsproces van jongeren, onder invloed van online omgevingen, een risico vormt voor de democratische rechtsstaat. De analyse behandelt achtereenvolgens het verloop van het proces van radicaliseren, de rol van online- en offline factoren en de gevolgen voor de democratische rechtsstaat.

In het kader van de probleemanalyse is gebruikgemaakt van generatieve AI (GenAI) ter ondersteuning van het schrijfproces. Er is gebruikgemaakt van de tool ChatGPT, ontwikkeld door OpenAI. De tool is uitsluitend ingezet als ondersteunend hulpmiddel voor taaltechnische taken. Het is gebruikt om synoniemen te vinden en om een spellingscontrole uit te voeren, zodat de tekst taalkundig correct is. GenAI is niet gebruikt voor het analyseren van inhoudelijke gegevens, het interpreteren van literatuur of het trekken van conclusies (OpenAI, 2026).

2. Probleemstelling

In dit hoofdstuk is de aanleiding, doelstelling, scope en afbakening en de hoofd- en deelvragen beschreven.

2.1 Aanleiding

De afgelopen jaren groeit de maatschappelijke- en veiligheidszorg over de rol van online omgevingen binnen het radicaliseringsproces van jongeren. Radicalisering

wordt gedefinieerd als een proces waarbij personen of groepen in toenemende mate opvattingen ontwikkelen die sterk afwijken van de gangbare normen en de democratische rechtsorde kunnen ondermijnen. In sommige gevallen groeit daarbij de bereidheid om extreme ideeën om te zetten in handelen of geweld (NCTV, 2025). Volgens rapportages van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) spelen digitale platforms een steeds grotere rol bij het verspreiden van extremistische ideologieën en het versterken van online polarisatie (NCTV, 2025). Ook de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) signaleert dat jongeren relatief eenvoudig in aanraking komen met extremistische content via algoritmische aanbevelingen, gesloten online gemeenschappen en internationale netwerken (AIVD, 2025). De online omgeving wordt hierbij gedefinieerd als een digitale of virtuele ruimte op het internet waar gebruikers samenkomen om te communiceren, informatie uit te wisselen, te leren of zich te vermaken. Voorbeelden hiervan zijn sociale media, chatgroepen, fora en gamingplatforms (Visser et al., 2024).

Radicaliseren in online omgevingen komt daarbij relatief vaak voor onder jongeren in de leeftijd van 14 tot en met 23 jaar. In deze levensfase zijn jongeren actief bezig met identiteitsvorming en het zoeken naar erkenning, sociale aansluiting en zingeving. Tegelijkertijd maken zij intensief gebruik van online platforms, waarop zij in aanraking kunnen komen met uiteenlopende ideeën, overtuigingen en online gemeenschappen. De online omgeving biedt jongeren een laagdrempelige mogelijkheid om te experimenteren met identiteit en opvattingen, terwijl opvoeders vaak beperkt zicht hebben op deze online leefwereld. De combinatie van identiteitsontwikkeling, sociale beïnvloeding en digitale dynamiek maakt radicalisering onder jongeren tot een complex en groeiend veiligheidsvraagstuk (Nederlands Jeugdinstituut, 2025).

Radicalisering in online omgevingen vormt daarbij niet alleen een individueel of sociaal probleem, maar kan ook gevolgen hebben voor de democratische rechtsstaat. Wanneer jongeren extremistische overtuigingen ontwikkelen die democratische principes, zoals vrijheid, gelijkheid en rechtszekerheid, afwijzen, kunnen publieke waarden en maatschappelijke stabiliteit onder druk komen te staan. Daarbij is het belangrijk te benadrukken dat radicalisering zich niet uitsluitend online afspeelt. Hoewel in de praktijk regelmatig wordt gesproken over 'online radicalisering', betreft dit conceptueel geen afzonderlijk proces. Radicalisering moet worden begrepen als één samenhangend proces waarin online- en offlinefactoren elkaar voortdurend beïnvloeden (Whittaker, 2022). De online omgeving fungeert hierbij vooral als een versterkende en faciliterende context, waarin mechanismen zoals algoritmische aanbevelingen, echo chambers en online groepsvorming het radicaliseringsproces kunnen versnellen en verdiepen (NCTV, 2025).

Juist doordat online- en offlinefactoren nauw met elkaar verweven zijn, is het relevant om te onderzoeken op welke wijze online omgevingen bijdragen aan het

radicaliseringsproces van jongeren van 14 tot en met 23 jaar en welke risico's dit kan opleveren voor de democratische rechtsstaat.

2.2 Doelstelling

Het doel van de probleemanalyse is om inzicht te verkrijgen in waarom radicalisering onder jongeren van 14 tot en met 23 jaar in online omgevingen een risico vormt voor de democratische rechtsstaat en om op basis daarvan onderbouwde oplossingsrichtingen te formuleren.

2.3 Scope en afbakening

De probleemanalyse richt zich op het radicaliseren onder jongeren van 14 tot en met 23 jaar in Nederland. De focus ligt op de rol van online factoren binnen dit proces, waarbij offline factoren worden meegenomen als ondersteunende context. De analyse richt zich op radicalisering in algemene zin en maakt geen onderscheid naar specifieke ideologieën. Vanuit een interdisciplinaire benadering zijn inzichten uit criminologie, sociale psychologie en veiligheidskunde gecombineerd.

2.4 Hoofd- en deelvragen

De hoofdvraag luidt als volgt: *‘Waarom vormt het proces van radicaliseren van jongeren van 14 tot en met 23 jaar, onder invloed van online omgevingen, een risico voor de democratische rechtsstaat?’*

De deelvragen luiden als volgt:

1. ‘Hoe verloopt het proces van radicaliseren onder jongeren van 14 tot en met 23 jaar in online omgevingen?’
2. ‘Welke online- en offline factoren dragen bij aan het proces van radicaliseren onder jongeren van 14 tot en met 23 jaar?’
3. ‘Op welke manier kan radicalisering onder jongeren van 14 tot en met 23 jaar in online omgevingen de democratische rechtsstaat onder druk zetten?’

3. Onderzoeksmethoden

In dit hoofdstuk zijn de onderzoeksmethoden, validiteit en betrouwbaarheid beschreven.

3.1 Methoden

DEELVRAGEN	ONDERZOEKSMETHODEN
1, 2 EN 3	Literatuurstudie: • Wetenschappelijke onderzoeken en artikelen. • Onderzoeken van overheidsinstanties. • Onderzoeken van jeugd gerelateerde kennisinstituten.

Voor de beantwoording van de deelvragen is literatuurstudie uitgevoerd. Hierbij is gebruikgemaakt van wetenschappelijke artikelen, overheidsrapportages en publicaties van relevante kennisinstituten. De literatuur is verzameld via databanken, zoals Google Scholar en de Saxion-bibliotheek (HBO Kennisbank, Academic Search, Encyclopedia of Social Work), waarbij zoektermen zijn afgeleid van kernbegrippen zoals online radicalisering jongeren, echo chambers, filterbubbels, polarisatie jongeren en risk factors radicalization.

De selectie van bronnen vond plaats op basis van drie criteria: relevantie voor de onderzoeksvraag, actualiteit en wetenschappelijke kwaliteit. Hierbij is prioriteit gegeven aan peer-reviewed artikelen en rapportages van overheidsinstanties, zoals de NCTV en de AIVD.

3.2 Validiteit en betrouwbaarheid

Om de validiteit van de probleemanalyse te waarborgen, is bewust gekozen voor betrouwbare en relevante bronnen. Zo is gebruikgemaakt van peer-reviewed wetenschappelijke artikelen, rapporten van overheidsinstanties en publicaties van jeugdinstituten die actueel en onderbouwd zijn. Door bronnen te combineren uit verschillende vakgebieden, zoals criminologie, sociale psychologie, bestuurskunde en recht, is een zo volledig mogelijk beeld van radicaliseren geschetst en is een eenzijdige benadering voorkomen.

De betrouwbaarheid is vergroot door een zoekstrategie toe te passen via Google Scholar en de Saxion-bibliotheek. Hierbij zijn gerichte zoektermen gebruikt en is literatuur beoordeeld op inhoud en context. Hierdoor zijn de bevindingen beter controleerbaar en navolgbaar.

De analyse is gebaseerd op geselecteerde en bestudeerde literatuur, waardoor de academische integriteit van het onderzoek behouden blijft.

4. Probleemanalyse

In dit hoofdstuk zijn de deelvragen beantwoord. Allereerst is het proces van radicaliseren binnen online omgevingen beschreven. Vervolgens is ingegaan op de online- en offlinefactoren die van invloed zijn op dit proces. Tot slot zijn de mogelijke gevolgen van radicalisering voor de democratische rechtsstaat beschreven.

4.1 Het verloop van radicaliseren in online omgevingen

In deze paragraaf is de volgende vraag beantwoord: 'Hoe verloopt het proces van radicaliseren onder jongeren van 14 tot en met 23 jaar in online omgevingen?'

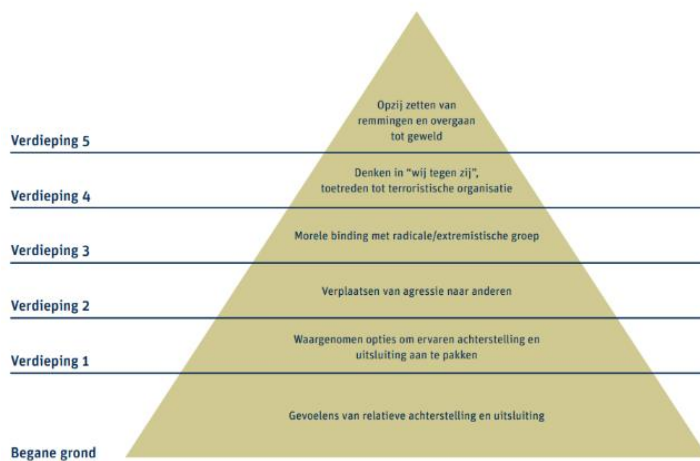
Het proces van radicaliseren onder jongeren van 14 tot en met 23 jaar is een complex fenomeen dat niet volgens een eenduidig patroon verloopt. Radicaliseren wordt beïnvloed door een combinatie van persoonlijke kenmerken, sociale contexten en de online omgeving waarin jongeren zich bevinden. Factoren zoals leeftijd,

identiteitsontwikkeling, groepsdruk en gevoelens van sociale vervreemding spelen een rol in de vatbaarheid van jongeren voor radicale ideologieën. Radicalisering gebeurt vaak subtiel en onopgemerkt, waardoor vroegtijdige signalering en interventie uitdagend zijn. Elk individu doorloopt dit proces op een unieke manier, waarbij persoonlijke ervaringen en online blootstelling een belangrijke rol spelen in het versnellen of afremmen van radicaliseringsmechanismen (Van de Ven, z.d.).

Een eerste fase van radicalisering in online omgevingen betreft doorgaans de initiële blootstelling aan extremistische of radicale content. Jongeren worden via sociale media, online gamingplatforms en diverse websites geconfronteerd met berichten die inspelen op gevoelens van onrechtvaardigheid, onbehagen of identiteitsvraagstukken. Algoritmes van platforms en zogenoemde 'echokamers' versterken dit proces door jongeren herhaaldelijk vergelijkbare content aan te bieden, waardoor bepaalde wereldbeelden genormaliseerd raken. In deze fase zijn jongeren nog voornamelijk ontvangers van informatie, maar beginnen zij geleidelijk een alternatieve interpretatie van maatschappelijke kwesties te ontwikkelen die kan afwijken van gangbare normen en waarden. Deze fase sluit aan bij de onderste treden van het trappenhuismodel van Fathali Moghaddam (figuur 1), waarin gevoelens van onrechtvaardigheid, frustratie en vervreemding de basis vormen voor verdere radicalisering (Van den Berg, 2022).

Na de initiële blootstelling kan het proces zich verdiepen door interactie met gelijkgestemden of recruiters binnen besloten online groepen. In deze context wordt de inhoud extremer gepresenteerd en neemt de sociale druk toe, waardoor jongeren een sterk 'wij-zij'-denken ontwikkelen. Dit groepsdenken leidt tot het eigen maken van normen en waarden van de radicale gemeenschap en het afwijzen of minimaliseren van kritische stemmen van buiten de groep. Sociale identificatie binnen deze online netwerken speelt een centrale rol bij het versterken van radicale overtuigingen en kan leiden tot isolatie van eerdere sociale netwerken in de offline omgeving. Binnen het trappenhuismodel (figuur 1) bevindt deze fase zich op de middelste treden, waarin jongeren zich steeds sterker identificeren met de radicale groep en alternatieve perspectieven afwijzen (Van den Berg, 2022).

Een latere fase van radicalisering wordt gekenmerkt door de rechtvaardiging en normalisering van geweld. Jongeren nemen extremistische ideeën over en kunnen geweld gaan zien als een normale of gerechtvaardigde manier om maatschappelijke problemen op te lossen. Gedragsveranderingen worden zichtbaar in verhoogde online activiteit, gebruik van symboliek en memes met radicale of gewelddadige associaties en een terugtrekking uit contacten met andersdenkenden. De combinatie van online exposure, sociale druk binnen netwerken en psychologische kwetsbaarheden vergroot de kans dat jongeren daadwerkelijk overgaan tot actie in lijn met radicale overtuigingen. Deze fase sluit aan bij de bovenste treden van het trappenhuismodel (figuur 1), waarin extremistische overtuigingen verankerd raken en geweld steeds meer als legitiem middel wordt beschouwd (Van den Berg, 2022).



Opmerking. Overgenomen uit *Wat kun je doen aan polarisatie en radicalisering?* (p.22) door Van den Berg, G. 2022, Nederlands Jeugdinstituut. Copyright 2022, Van den Berg.

Het digitale tijdperk speelt een belangrijke rol in de dynamiek van radicalisering. Nepnieuws, desinformatie en complottheorieën vormen een onderdeel van het online systeem en kunnen jongeren kunstmatig in een bepaalde richting sturen. Algoritmische aanbevelingen en sociale mediafijken zorgen ervoor dat jongeren steeds extremere content te zien krijgen, terwijl humor, ironie en memes extremistische boodschappen normaliseren. Dit mechanisme maakt het moeilijker voor jongeren om kritische afstand te bewaren en kan leiden tot een parallelle denkwereld die losstaat van de offline realiteit (Custers, 2019).

Niet iedereen doorloopt alle stappen, maar online factoren kunnen dit proces versnellen en versterken. Radicalisering in online omgevingen ontstaat daarmee uit een samenspel van individuele kwetsbaarheden en digitale invloeden, waarbij online platforms een centrale rol spelen in zowel blootstelling als verdere escalatie (Van den Berg, 2022).

4.2 Online- en offline factoren

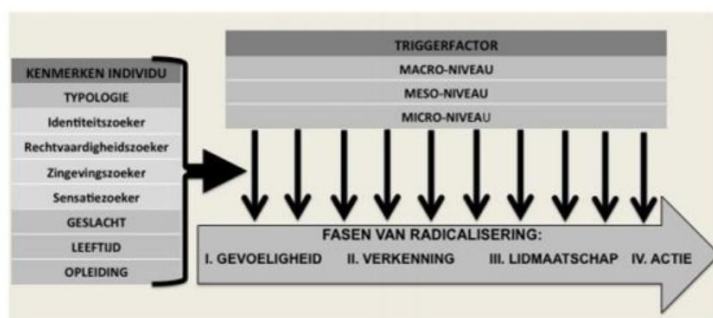
In deze paragraaf is de volgende vraag beantwoord: 'Welke online- en offline factoren dragen bij aan het proces van radicaliseren onder jongeren van 14 tot en met 23 jaar?' Het proces van radicaliseren onder jongeren wordt beïnvloed door een samenspel van factoren op individueel, sociaal en maatschappelijk niveau, waarbij online- en offlinecontexten elkaar voortdurend versterken. Dit proces is dynamisch en contextafhankelijk en kent geen eenduidige oorzaak (Van den Berg, 2022).

Op individueel niveau (microniveau) speelt de ontwikkelingsfase van jongeren een belangrijke rol (Figuur 2). Jongeren bevinden zich in een periode van identiteitsvorming, waarin zij zoeken naar erkenning, zingeving en sociale aansluiting. Factoren zoals onzekerheid, lage eigenwaarde, gevoelens van uitsluiting en ingrijpende levensgebeurtenissen kunnen de vatbaarheid voor radicale denkbeelden vergroten (R. Feddes et al., 2025). Volgens de theorie van relatieve deprivatie kunnen

ervaren ongelijkheid en onrechtvaardigheid leiden tot frustratie, wat jongeren ontvankelijk maakt voor ideologieën die hier een verklaring voor bieden (Van den Bos & Loseman, 2012).

Op sociaal niveau (mesoniveau) zijn groepsprocessen en sociale interacties bepalend (Figuur 2). Jongeren ontleen betekenis en identiteit aan de groepen waartoe zij behoren. Wanneer aansluiting bij reguliere sociale netwerken ontbreekt, kunnen alternatieve en radicale groepen aantrekkelijk worden. Binnen zowel offline als online gemeenschappen kunnen normen en waarden worden gevormd en versterkt. In online contexten wordt dit proces geïntensiveerd door echokamers, waarin gelijkgestemde opvattingen worden bevestigd en afwijkende perspectieven worden uitgesloten. Hierdoor neemt polarisatie toe en wordt het wij-zij-denken versterkt (R. Feddes et al., 2025).

Op maatschappelijk niveau (macroniveau) spelen bredere structurele factoren een rol, zoals discriminatie, kansenongelijkheid en maatschappelijke spanningen (Figuur 2). Ook internationale conflicten en mediaberichtgeving kunnen bijdragen aan gevoelens van onrechtvaardigheid en vervreemding. Deze factoren kunnen fungeren als voedingsbodem voor radicalisering, doordat zij bestaande frustraties en onzekerheden versterken (R. Feddes et al., 2025).



Opmerking. Overgenomen uit *Online zorgwekkende radicalisering* door Van wonderen, R 2024, Richtlijnen Jeudhulp en Jeudbescherming. Copyright 2024. Van wonderen. R.

De online omgeving werkt als een krachtige versterkende en versnellende factor in radicalisering. Jongeren hebben via digitale platforms laagdrempelig toegang tot radicale ideologieën, propaganda en desinformatie. Door algoritmes worden zij bovendien stapsgewijs blootgesteld aan steeds extremere content (de 'socialmediafuik'), vaak zonder dat zij zich hiervan bewust zijn (Van Wonderen et al., 2024).

Daarnaast ontstaan gemakkelijk echokamers en filterbubbels waarin vooral gelijkgestemden elkaar versterken en tegengeluiden ontbreken. Extremistische content wordt bovendien vaak verpakt in memes en humor, waardoor deze genormaliseerd raakt. Ook maakt de online omgeving anoniem contact en rekrutering mogelijk, waarbij wordt ingespeeld op persoonlijke kwetsbaarheden van jongeren (Van Wonderen et al., 2024).

Door de continue stroom aan informatie online kan radicalisering zich snel ontwikkelen. Tegelijkertijd blijven offline factoren, zoals gezin en school, bepalend voor hoe jongeren met deze invloeden omgaan. Radicalisering ontstaat daarmee uit een samenspel van online- en offlinefactoren, waarbij de online omgeving een steeds belangrijkere rol speelt (Van Wonderen et al., 2024).

Samenvattend kan worden gesteld dat radicalisering onder jongeren van 14 tot en met 23 jaar wordt beïnvloed door een combinatie van individuele, sociale, maatschappelijke en online factoren. Vooral online omgevingen spelen hierin een versterkende rol. Het is juist deze combinatie van factoren en niet één afzonderlijke oorzaak die bepaalt of en hoe een jongere radicaliseert.

4.3 De gevolgen voor de democratische rechtsstaat

In deze paragraaf is de volgende vraag beantwoord: 'Op welke manier kan radicalisering onder jongeren van 14 tot en met 23 jaar in online omgevingen de democratische rechtsstaat onder druk zetten?'

De democratische rechtsstaat vormt de basis van de Nederlandse samenleving en combineert democratische besluitvorming met juridische waarborgen. Een democratische rechtsstaat kenmerkt zich door een staatsinrichting waarin de overheid gebonden is aan het recht en waarin burgers worden beschermd door grondrechten en vrijheden, zowel tegen medeburgers als tegen machtsmisbruik van de overheid. Daarnaast is er sprake van machtscheiding (*trias politica*) en onafhankelijke rechtspraak, waardoor willekeur en onbegrensde machtsuitoefening worden beperkt. De macht ligt daarmee bij het volk, maar wordt tegelijkertijd begrensd door wetten, grondrechten en juridische controlemechanismen die zorgen voor rechtszekerheid en bescherming van burgers (Raad voor het Openbaar Bestuur, 2020).

Binnen deze democratische rechtsstaat staan publieke waarden centraal. Publieke waarden kunnen worden gedefinieerd als duurzame opvattingen over de inrichting en het functioneren van de samenleving, die als wenselijk worden beschouwd voor het voortbestaan van de samenleving en het welzijn van haar leden. Hieronder vallen onder meer waarden zoals vrijheid, gelijkheid, rechtvaardigheid, legitimiteit, rechtmatigheid, transparantie, integriteit en veiligheid. Deze waarden vormen het fundament voor sociale cohesie en het vertrouwen in publieke instituties. Wanneer deze waarden worden ondermijnd, raakt dit niet alleen individuele burgers, maar ook het vertrouwen in het functioneren van instituties en de samenleving als geheel (Rutgers, 2011).

Radicalisering in online omgevingen kan de democratische rechtsstaat op verschillende manieren onder druk zetten, doordat publieke waarden worden aangetast. Allereerst kan het leiden tot de afwijzing van kernwaarden zoals gelijkheid, tolerantie en vrijheid. Jongeren die extremistische overtuigingen overnemen, kunnen groepen uitsluiten of als minderwaardig beschouwen, wat kan leiden tot discriminatie en sociale uitsluiting (Emmelkamp et al., 2020).

Daarnaast versterkt radicalisering in online omgevingen polarisatie. Digitale platforms stimuleren via algoritmes voornamelijk gelijkgestemde content, waardoor echo chambers ontstaan. Hierdoor worden tegenstellingen tussen groepen vergroot en neemt het wij-zij-denken toe. Dit ondermijnt sociale cohesie en bemoeilijkt dialoog en compromis, terwijl juist deze elementen essentieel zijn binnen een democratisch systeem (Universiteit Utrecht, 2025).

Ook kan radicalisering in online omgevingen het vertrouwen in democratische instituties aantasten. Binnen online netwerken wordt regelmatig desinformatie verspreid, bijvoorbeeld in de vorm van complottheorieën over de overheid of het rechtssysteem. Wanneer jongeren deze informatie als waar beschouwen, kan dit leiden tot wantrouwen richting instituties zoals de overheid, politie en rechtspraak. Hierdoor komt de legitimiteit van deze instituties, en daarmee een belangrijke pijler van de democratische rechtsstaat, onder druk te staan (Van Wonderen et al., 2024). Tot slot kan radicalisering in online omgevingen bijdragen aan de normalisering van extremistische overtuigingen en in sommige gevallen geweld. Door herhaalde blootstelling aan radicale content kunnen extremistische ideeën steeds normaler worden ervaren, waardoor de drempel voor het ondersteunen of uitvoeren van extremistisch gedrag afneemt. In ernstige gevallen kan dit leiden tot geweldsincidenten of terrorisme, wat een directe bedreiging vormt voor de veiligheid van burgers (Emmelkamp et al., 2020).

Samenvattend vormt radicalisering in online omgevingen een risico voor de democratische rechtsstaat. Het tast publieke waarden aan, vergroot polarisatie, ondermijnt vertrouwen in instituties en kan leiden tot veiligheidsdreigingen. Hierdoor komt niet alleen de stabiliteit van de samenleving onder druk te staan, maar ook het functioneren van het democratische systeem als geheel.

5. Conclusie

Radicalisering onder jongeren van 14 tot en met 23 jaar in online omgevingen vormt een risico voor de democratische rechtsstaat doordat het publieke waarden zoals vrijheid, gelijkheid, tolerantie en rechtsstatelijkheid onder druk zet. Online omgevingen versterken radicaliseringsprocessen via algoritmes, echo chambers en online groepsvorming, waardoor jongeren eenzijdige informatie ontvangen en sneller in aanraking komen met extremistische overtuigingen.

Dit kan leiden tot de afwijzing van democratische kernwaarden, het versterken van wij-zij-denken en toenemende maatschappelijke polarisatie. Hierdoor komt de sociale cohesie onder druk te staan, terwijl juist sociale verbondenheid en wederzijds begrip essentieel zijn binnen een democratische rechtsstaat. Daarnaast kan de verspreiding van desinformatie en complottheorieën leiden tot wantrouwen richting instituties zoals de overheid, politie en rechtspraak. Dit tast de legitimiteit van democratische instituties aan.

Vanuit een kritisch perspectief blijkt dat radicalisering niet alleen een veiligheidsvraagstuk is, maar ook een sociaal-maatschappelijk en normatief

vraagstuk. Het raakt direct aan de balans tussen veiligheid, vrijheid en grondrechten. Radicalisering laat daarmee zien hoe kwetsbaar publieke waarden en democratische principes kunnen zijn binnen een samenleving waarin online- en offline werelden steeds meer met elkaar verweven raken.

6. Oplossingsrichting

6.1 Oplossingsrichting

Het tegengaan van radicalisering onder jongeren van 14 tot en met 23 jaar in online omgevingen vereist interventies die aansluiten op de onderliggende factoren van het radicaliseringsproces. Uit de probleemanalyse blijkt dat met name algoritmische versterking, sociale groepsvorming en individuele kwetsbaarheden een belangrijke rol spelen. Daarnaast kan radicalisering leiden tot polarisatie, afnemend vertrouwen in instituties en het ondermijnen van de democratische rechtsstaat.

Een eerste oplossingsrichting is het bevorderen van democratisch burgerschap en online mediawijsheid binnen het onderwijs. Jongeren dienen meer kennis te ontwikkelen over democratische waarden, grondrechten, vrijheid van meningsuiting en respect voor diversiteit. Daarnaast moeten zij leren omgaan met desinformatie, framing, complottheorieën en online beïnvloedingstechnieken. Door kritisch denken en digitale weerbaarheid te versterken, neemt de kans af dat jongeren meegaan in extremistische narratieven en groeit hun begrip voor pluralisme en maatschappelijke verantwoordelijkheid (Van Halderen et al., 2022).

Daarnaast is het belangrijk om vroegtijdige signalering van radicalisering in online omgevingen te verbeteren. Hierbij gaat het om het herkennen van digitale signalen, zoals deelname aan echo chambers, het delen van extremistische content en het gebruik van radicale symboliek. Professionals binnen onderwijs, jongerenwerk en veiligheid dienen daarom niet alleen algemene kennis over radicalisering te ontwikkelen, maar ook specifiek getraind te worden in het herkennen van online signalen. Dit vergroot de kans op tijdige interventie, voordat extremistische overtuigingen sterker verankerd raken en democratische waarden verder onder druk komen te staan (Hamid & Ariza, 2022).

Verder blijkt uit de analyse dat sociale binding een belangrijke rol speelt binnen het radicaliseringsproces. Jongeren zoeken erkenning, identiteit en groepsgevoel, waardoor radicale online gemeenschappen aantrekkelijk kunnen worden. Daarom is het belangrijk om veilige online- en offline dialoogruides te creëren waarin maatschappelijke spanningen, frustraties en gevoelens van onrecht bespreekbaar worden gemaakt. Daarnaast kunnen jongerenwerk, onderwijsprogramma's en maatschappelijke initiatieven bijdragen aan inclusie, sociale participatie en het verminderen van gevoelens van uitsluiting en polarisatie (Nederlands Jeugdinstituut, 2026).

Tot slot vraagt de complexiteit van radicalisering in online omgevingen om een gerichte publiek-private samenwerking. Politie, gemeenten, onderwijsinstellingen, jeugdinstituten, ouders en technologiebedrijven moeten actief samenwerken in het

delen van kennis, signalen en interventies. Technologiebedrijven kunnen bijdragen door extremistische content sneller te signaleren en betrouwbare informatie actief te stimuleren. Daarnaast kunnen positieve online tegenverhalen en rolmodellen bijdragen aan het versterken van democratische waarden en maatschappelijke verbinding. Alleen door een integrale aanpak kunnen preventieve en repressieve maatregelen beter worden afgestemd op de dynamiek van online omgevingen en de bescherming van de democratische rechtsstaat worden versterkt (NCTV, 2025).

6.2 Kritische beschouwing

Het tegengaan van radicalisering in online omgevingen is complex, omdat het raakt aan belangrijke publieke waarden zoals vrijheid, veiligheid, privacy en gelijkheid. Aan de ene kant is het noodzakelijk om radicalisering tegen te gaan en de samenleving te beschermen tegen extremisme en geweld. Aan de andere kant moeten grondrechten, zoals vrijheid van meningsuiting en privacy, gewaarborgd blijven. Maatregelen zoals online monitoring of het verwijderen van content kunnen bijdragen aan veiligheid, maar kunnen tegelijkertijd spanning veroorzaken met democratische vrijheden (Jurriën Hamer & Lemmens, 2022).

Daarnaast blijkt uit de literatuur dat radicalisering niet uitsluitend een online probleem is. Offline factoren, zoals sociale uitsluiting, identiteitsproblematiek, gevoelens van onrechtvaardigheid en maatschappelijke spanningen, spelen eveneens een belangrijke rol binnen het proces van radicaliseren. Dit betekent dat oplossingen die uitsluitend gericht zijn op online platforms onvoldoende aansluiten bij de onderliggende oorzaken van radicalisering (Van Wonderen et al., 2024).

Ook spelen de verschillende belangen van betrokken partijen een rol. Overheden en politie richten zich vooral op veiligheid en risicobeperking, terwijl technologiebedrijven vaak belang hebben bij gebruikersactiviteit en interactie. Hierdoor kunnen algoritmes onbedoeld bijdragen aan het versterken van extremistische content. Jongeren zelf hechten juist veel waarde aan autonomie en vrijheid, waardoor maatregelen als controlerend of stigmatiserend kunnen worden ervaren (Bodo & Trauthig, 2022).

Bovendien brengt het tegengaan van radicalisering het risico met zich mee op overmatige controle en surveillance van online gedrag. Wanneer online monitoring te ver gaat, kan dit botsen met grondrechten en juist wantrouwen richting instituties versterken. Een eenzijdige focus op repressie of controle kan gevoelens van uitsluiting bovendien vergroten, terwijl deze gevoelens juist een voedingsbodem kunnen vormen voor radicalisering (Bodo & Trauthig, 2022).

Daarom lijken preventieve oplossingen, gericht op inclusie, digitale weerbaarheid, kritisch denken en positieve groepsvorming, het beste aan te sluiten bij zowel de oorzaken van radicalisering als de waarden van de democratische rechtsstaat. Hierbij is het belangrijk dat samenwerking tussen overheid, onderwijs, jongerenwerk en technologiebedrijven transparant, proportioneel en zorgvuldig wordt ingericht.

Samenvattend vraagt het vraagstuk van radicalisering in online omgevingen om een zorgvuldige balans tussen veiligheid en vrijheid. Oplossingen moeten niet alleen effectief zijn in het tegengaan van radicalisering, maar ook passen binnen de publieke waarden en democratische principes die juist beschermd moeten worden.

Literatuurlijst

AIVD. (2025, 3 april). AIVD ziet toename dreiging van online radicaliserende minderjarigen. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Geraadpleegd op 21 maart 2026, van <https://www.aivd.nl/actueel/nieuws/2025/04/03/aivd-ziet-toename-dreiging-van-online-radicaliserende-minderjarigen>

Bodo, L., & Trauthig, K. (2022). Emergent technologies and extremists: The DWeb as a new internet reality? Global Network on Extremism & Technology. Van <https://gnet-research.org/wp-content/uploads/2022/07/GNET-Report-Emergent-Technologies-Extremists-Web.pdf>

Custers, B. (2019). Nepnieuws, filterbubbels en echokamers. Leiden University. <https://scholarlypublications.universiteitleiden.nl/access/item%3A2977068/view>

Emmelkamp, J., Asscher, J. J., Wissink, I. B., & Stams, G. J. J. M. (2020). Risk factors for (violent) radicalization in juveniles: A multilevel meta-analysis. *Aggression and Violent Behavior*, 55, Article 101489. <https://doi.org/10.1016/j.avb.2020.101489>

Feddes, A. R., Szekeres, H., Kunst, B., & Doosje, B. (2025). Radicalisering en psychosociale problematiek: Beter begrijpen, beter ingrijpen. WODC / Universiteit van Amsterdam. Van <https://repository.wodc.nl/bitstream/handle/20.500.12832/3465/rapport-radicalisering-en-psychosociale-problematiek-beter-begrijpen-beter-ingrijpen.pdf>

Hamid, N., & Ariza, C. (2022). Offline versus online radicalisation: Which is the bigger threat? Global Network on Extremism & Technology. Van <https://gnet-research.org/wp-content/uploads/2022/02/GNET-Report-Offline-Versus-Online-Radicalisation.pdf>

Hamer, J., & Lemmens, A. (2022). Algoritmes afwegen: Verkenning naar maatregelen ter bescherming van mensenrechten bij profilering in de uitvoering. Rathenau Instituut. Van https://www.rathenau.nl/sites/default/files/2022-05/Algoritmes_afwegen_Rapport_Rathenau_Instituut.pdf

NCTV. (2025, 17 juni). Toenemende online radicalisering van jongeren. Ministerie van Justitie en Veiligheid. Geraadpleegd op 21 maart 2026, van <https://www.nctv.nl/actueel/nieuws/2025/06/17/nctv-toenemende-online-radicalisering-van-jongeren>

Nederlands Jeugdinstituut. (z.d.). Hybride straatgeweld: Verbondenheid van fysieke en online leefwereld. Geraadpleegd op 11 april 2026, van <https://www.nji.nl/kennis/jeugdcriminaliteit/hybride-straatgeweld-verbondenheid-van-fysieke-en-online-leefwereld>

Nederlands Jeugdinstituut. (2025, 9 april). Online radicalisering bij jongeren. Geraadpleegd op 26 maart 2026, van <https://www.nji.nl/kennis/radicalisering/online-radicalisering-bij-jongeren>

Nederlands Jeugdinstituut. (2026). Wat kan ik preventief doen tegen radicalisering? Geraadpleegd op 29 april 2026, van <https://www.nji.nl/kennis/radicalisering/wat-kan-ik-preventief-doen-tegen-radicalisering>

OpenAI. (2026). ChatGPT (12 mei versie) [Large language model]. <https://chat.openai.com/>

Raad voor het Openbaar Bestuur. (2020). Een sterkere rechtsstaat: Verbinden en beschermen in een pluriforme samenleving. <https://www.raadopenbaarbestuur.nl/documenten/publicaties/2020/04/15/een-sterkere-rechtsstaat>

Rutgers, M. R. (2011). Het pantheon van de publieke waarden [Oratie, Universiteit van Amsterdam]. https://pure.uva.nl/ws/files/2216703/108322_343438.pdf

Universiteit Utrecht. (2025, 26 juni). Echokamers, konijnenholen en propaganda: Hoe beïnvloedt het internet radicalisering onder jongeren? Geraadpleegd op 20 april 2026, van <https://ter-info.nl/echokamers-konijnenholen-en-propaganda-hoe-beïnvloedt-het-internet-radicalisering-onder-jongeren/>

Van de Ven, H. (z.d.). Hoe verloopt het proces van radicalisering? Nederlands Jeugdinstituut. Geraadpleegd op 20 april 2026, van <https://www.nji.nl/kennis/radicalisering/hoe-verloopt-het-proces-van-radicalisering>

Van den Berg, G. (2022). Wat kun je doen aan polarisatie en radicalisering? Nederlands Jeugdinstituut. Van <https://www.nji.nl/system/files/2022-02/Wat-kun-je-doen-aan-polarisatie-en-radicalisering.pdf>

Van den Bos, K., & Loseman, A. (2012). Radicalisering onder jongeren. Tijdschrift voor Groepsdynamica, 1, 11-19.
https://www.groepspsychotherapie.nl/hvvp/_sitefiles/file/tijdschriftartikelen/2012/2012_1Radicalisering-onder-jongeren.pdf

Van Halderen, R. C., Tjoelker, R., Walberg, A. M., & Spithoven, R. (2024). (Ir)reëel gevaar: Een verkennend onderzoek naar de lokale preventie van bedreiging en intimidatie door complotdenkers. Hogeschool Saxion.
https://www.researchgate.net/publication/384288999_Irreeel_gevaar_Een_verkennend_onderzoek_naar_de_lokale_preventie_van_bedreiging_en_intimidatie_door_complotdenkers

Van Wonderen, R., Burggraaff, D., Sieckelinck, S., Dijkman, A., & Day, M. (2024). Online zorgwekkende radicalisering. Richtlijnen Jeugdhulp en Jeugdbescherming. Van <https://www.richtlijnenjeugdhulp.nl/radicalisering/verantwoording-en-bronnen>

Visser, M., Oosterveer, D., & Den Besten, D. (2024). Basisboek online marketing (5e ed). Noordhoff.

Whittaker, J. (2022). Rethinking online radicalization. Perspectives on Terrorism, 16(4), 27–40. <https://www.jstor.org/stable/27158150>



CYBER
WEERBAAR
NL