CYBER WEERBAAR NL

Een SPRONG naar cyberweerbaarheid

Onderzoeksagenda

Rutger Leukfeldt, Remco Spithoven, Jurjen Jansen & Carlyn van Amersfoort (red.)

Boom

Over de onderzoeksagenda

Online weerbaarheid wordt steeds belangrijker in de maatschappij en daarmee wordt ook de vraag naar kennis over dit thema urgenter en actueler. De Cyberweerbaar NL onderzoeksagenda dient als leidraad voor toekomstig praktijkgericht onderzoek op het gebied van cyberweerbaarheid en identificeert de belangrijkste vraagstukken en uitdagingen binnen dit thema. De focus ligt daarbij niet zozeer op de technologische aspecten, maar juist op de menselijke en organisatorische kanten van cyberweerbaarheid: welke gedrags- en houdingsaspecten beïnvloeden cyberweerbaarheid en hoe kunnen organisaties deze aspecten ten behoeve van cyberweerbaarheid verbeteren? Deze onderzoeksagenda bespreekt meerdere thema's: slachtofferschap, daderschap, gedrag en gedragsverandering, en versterkingsmaatregelen voor cyberweerbaarheid in en door publieke en private organisaties.

Over Cyberweerbaar NL

Het expertisenetwerk Cyberweerbaar NL is een consortium van Nederlandse kennisinstellingen en publieke en private organisaties, en richt zich op het cyberweerbaar maken van de Nederlandse samenleving. Binnen dit netwerk wordt de kennis over cyberweerbaarheid ontwikkeld en uitgewisseld en worden huidige en toekomstige uitdagingen met elkaar gedeeld. Zo wordt er gezamenlijk gebouwd aan een duurzaam expertisenetwerk van onderzoekers en kennismakelaars in de beroepspraktijk waarbij continue vraagarticulatie en disseminatie van kennis over cyberweerbaarheid plaatsvindt. Zie voor meer informatie https://cyberweerbaarnl.nl.

ISBN 978-90-4730-257-5

9 789047 302575 >

www.boom.nl/criminologie

EEN SPRONG NAAR CYBERWEERBAARHEID

EEN SPRONG NAAR CYBERWEERBAARHEID: ONDERZOEKSAGENDA

Onder redactie van:

Rutger Leukfeldt, Remco Spithoven, Jurjen Jansen &
Carlyn van Amersfoort

Boom

Omslagontwerp: Yorinde Zomer-Bouwhuis
Illustraties binnenwerk: Marielle van der Salm
Opmaak binnenwerk: Textcetera, Den Haag

ISBN 978-90-4730-257-5
ISBN 978-94-0011-528-6 (e-book)
NUR 741

www.boom.nl
www.boom.nl/criminologie

VOORWOORD

De onderzoeksagenda die voor u ligt, is een initiatief van het expertisenetwerk Cyberweerbaar NL. Dit netwerk richt zich op het cyberweerbaar maken van Nederland. De focus ligt daarbij niet zozeer op de techniek, maar juist op de mens: welke gedrags- en houdingsaspecten beïnvloeden cyberweerbaarheid en hoe kunnen organisaties deze aspecten ten behoeve van cyberweerbaarheid verbeteren?

In totaal schreven er 27 auteurs mee die verbonden zijn aan vier hogescholen. Het expertisenetwerk Cyberweerbaar NL is namelijk een consortium van Nederlandse kennisinstellingen en publieke en private organisaties. Drie hogescholen met stevige trackrecords op het thema cyberweerbaarheid – De Haagse Hogeschool, Hogeschool Saxion en NHL Stenden Hogeschool – zijn de initiatiefnemers en vormen de kerngroep van het expertisenetwerk Cyberweerbaar NL. Deze drie hogescholen zoeken nadrukkelijk de samenwerking met andere kennisinstellingen die actief zijn op het gebied van praktijkgericht onderzoek naar cyberweerbaarheid. Verder bestaat het netwerk uit lokale, regionale en landelijke partners zoals gemeenten, de politie, MKB Nederland, Vereniging van Nederlandse Gemeenten (VNG), Cyberveilig Nederland (CVNL), PVO, CCV, Security Delta (HSD) en Avans Hogeschool. Iedere deelnemer aan het expertisenetwerk koppelt een zogenaamde kennismakelaar uit de praktijk aan onderzoekers uit de kerngroep. Zo wordt mogelijk gemaakt dat de nieuwste kennis over cyberweerbaarheid wordt uitgewisseld en dat huidige en toekomstige uitdagingen met elkaar worden gedeeld. Zo bouwen we gezamenlijk aan een duurzaam expertisenetwerk van onderzoekers en kennismakelaars in de beroepspraktijk, waarbij continue vraagarticulatie en

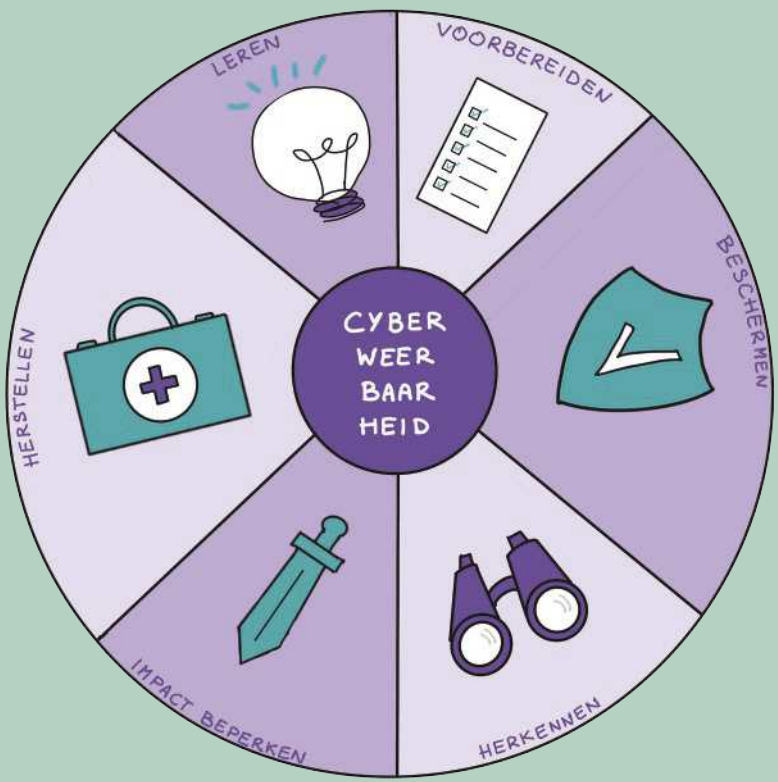
verspreiding van kennis op het gebied van cyberweerbaarheid plaatsvindt.

De onderzoeksagenda die voor u ligt, is opgesteld door de kernlectoren en onderzoekers van het expertisenetwerk Cyberweerbaar NL. Uiteraard zijn we al langere tijd met diverse partners aan de slag om relevant praktijkgericht onderzoek uit te voeren, maar deze agenda helpt bij het geven van richting aan toekomstig onderzoek. Daarbij maken we strategische keuzes in de gezamenlijke uitwerking van de thema's van deze onderzoeksagenda en maken we de beweging van ad hoc samenwerkingen naar meerjarig geagendeerd onderzoek.

Den Haag, Apeldoorn, Leeuwarden, april 2025
Rutger Leukfeldt, Remco Spithoven, Jurjen Jansen,
Carlyn van Amersfoort

INHOUD

1


LEREN
VOORBEREIDEN
BESCHERMEN
HERKENNEN
IMPACT BEPERKEN
HERSTELLEN
CYBER
WEER
BAAR
HEID

INLEIDING

Rutger Leukfeldt, Carlyn van Amersfoort, Remco Spithoven, Jurjen Jansen

1.1 OVER CYBERWEERBAAR NL EN DE ONDERZOEKSAGENDA

Online criminaliteit is al jaren onderwerp van onderzoek. Toch wordt dit onderzoek door professionals ervaren als gefragmenteerd en te weinig aangesloten op de praktijk. Het expertisenetwerk Cyberweerbaar NL wil bestaande inzichten bundelen en samen met praktijkpartners nieuwe, hoogwaardige kennis ontwikkelen. Van welke thema's weten we al het nodige en van welke thema's nog nagenoeg niets? Op welke onderwerpen hebben we in Nederland al expertise en wat zijn de grootste uitdagingen de komende jaren? Deze onderzoeksagenda laat zien op welke thema's de kennisinstellingen binnen Cyberweerbaar NL zich richten. De onderzoeksvragen die in ieder thema zijn geformuleerd dienen als een concrete aanzet om het cyberweerbaarheidsdomein verder te brengen. Dit betreft zeker geen uitputtende lijst. Samen met alle praktijkpartners gaan we aan de slag om gezamenlijk te bepalen welke thema's we de komende jaren verder uitdiepen en welke onderzoeksvragen daarbij prioriteit moeten krijgen. Deze onderzoeksagenda is daarmee een vertrekpunt.

Deze onderzoeksagenda gaat in op vijf hoofdthema's. Hoofdstuk 2 bespreekt de slachtofferkant van online criminaliteit, zoals de omvang en de risicofactoren. Hoofdstuk 3 behandelt gedrag en gedragsverandering, bijvoorbeeld effectieve risicocommunicatie. Hoofdstuk 4 gaat in op het versterken van de cyberweerbaarheid aan de publieke kant. Hoofdstuk 5 bespreekt het versterken van de cyberweerbaarheid aan de

private kant, zoals *incident response* bij het mkb. Als laatste behandelt hoofdstuk 6 de daders van online criminaliteit, waaronder de ontwikkelpaden van cybercriminelen en cybercrime-as-a-service. Hoewel we hebben getracht overlap te voorkomen, kan het zijn dat een enkel onderwerp vanuit verschillende perspectieven aan bod komt. Voordat we overgaan tot de onderzoeksthema's, gaan we eerst dieper in op wat wij verstaan onder cyberweerbaarheid (par. 1.2), online criminaliteit (par. 1.3) en effectieve aanpakken en interventies (par. 1.4).

1.2 OVER CYBERWEERBAARHEID

In de nationale cybersecuritystrategie 2022-2028 (NCSC, 2022, p. 9) wordt cyberweerbaarheid gedefinieerd als:

> 'het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken'.

In de (internationale) literatuur wordt cyberweerbaarheid op verschillende wijzen gedefinieerd. Eén die aansluit op de bovenstaande definitie en daarbij de doelstelling van cyberweerbaarheid verduidelijkt, is die van Dupont et al. (2023, p. 3, gebaseerd op Björk et al. [2015] en Linkov & Kott [2019]):

> '[T]he ability to prepare, absorb, recover, and adapt to adverse effects caused by cyberattacks […], with the ultimate aim for the organization to continuously deliver the intended functions or services.'

1.3 OVER ONLINE CRIMINALITEIT

Voor criminaliteit waarbij technologie van wezenlijk belang is voor de uitvoering ervan bestaan verschillende benamingen

en categorieën. In het huidige criminologische onderzoek naar online criminaliteit worden in de regel twee categorieën gebruikt. De gangbare Engelse terminologie van deze categorieën is *cyber dependent crime* en *cyber enabled crime* (McGuire & Dowling, 2013; Beerthuizen et al., 2020). In het Nederlands kan dit vertaald worden als 'cybercriminaliteit' en 'gedigitaliseerde criminaliteit'. Beide categorieën en hun mengvormen vallen onder het paraplubegrip 'online criminaliteit'.

Delicten die vallen onder de noemer cybercriminaliteit kunnen worden gezien als 'nieuwe' vormen van criminaliteit. Immers, ICT is in dit geval niet alleen een middel om het delict te plegen, maar ook het doelwit. Dergelijke delicten waren in het pre-digitale tijdperk simpelweg niet mogelijk, omdat er nog geen ICT-infrastructuur was om aan te vallen. Voorbeelden zijn hacken (het zonder toestemming binnendringen in een geautomatiseerd werk), het gebruik van malware (kwaadaardige software zoals een virus of spyware), ransomware (het versleutelen van digitale informatie of systemen en daar losgeld voor vragen), DDoS-aanvallen (het platleggen van een digitaal systeem door deze te overbelasten) en *defacen* (het zonder toestemming aanpassen van websites).

Delicten die vallen onder de noemer 'gedigitaliseerde criminaliteit' zijn feitelijk delicten die er in het pre-digitale tijdperk ook al waren, maar waarbij ICT nu van wezenlijk belang is voor de uitvoering van die delicten. Een voorbeeld is het uitvoeren van een phishingcampagne, waarbij criminelen via een valse e-mail proberen inloggegevens van mensen te ontfutselen om zo controle te krijgen over de online bankieromgeving van slachtoffers. Vervolgens is het doel om geld via zogenaamde geldezels over te sluizen van de rekening van een slachtoffer naar rekeningen van de criminelen. Een vrij klassiek motief, financieel gewin, en een nieuwe vorm van een heel oud delict, namelijk oplichting of diefstal.

Onder gedigitaliseerde criminaliteit kan een veelheid van delicten vallen. Grofweg worden in de criminologische literatuur drie subcategorieën onderscheiden:

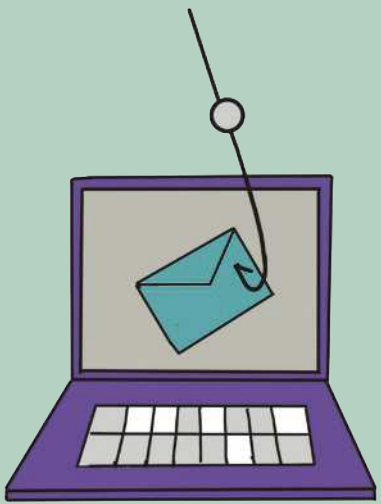
financieel-economische delicten, interpersoonlijke delicten en zedendelicten. Bij financieel-economische cyberdelicten is het doel van de daders financieel gewin. Voorbeelden hiervan zijn phishing, identiteitsfraude, WhatsAppfraude, koop- en verkoopfraude, diefstal, voorschotfraude, heling, CEO-fraude en datingfraude. Interpersoonlijke cyberdelicten zijn digitale vormen van strafbare gedragsdelicten waarbij de persoonlijke levenssfeer wordt aangetast. De meest voorkomende vormen zijn laster en chantage, gevolgd door stalking en bedreiging met geweld. Sinds de opkomst van het internet vinden zedendelicten ook online plaats. Voorbeelden hiervan zijn grooming en het verspreiden van kinderporno. Daarnaast zijn er de zogenaamde IBSA-delicten (*Image Based Sexual Abuse*), zoals het zonder toestemming verspreiden van naaktfoto's en -filmpjes (ook wel *shame sexting* genoemd) of hiermee dreigen (*sextortion*) (Powell et al., 2019). Zowel het dreigen met als het daadwerkelijk verspreiden van dergelijk seksueel beeldmateriaal zonder toestemming is strafbaar.

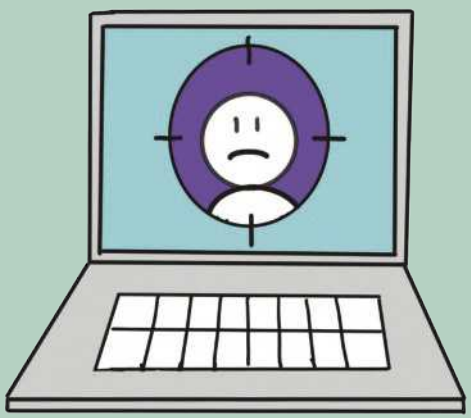
1.4 OVER EFFECTIEVE AANPAKKEN EN INTERVENTIES

De cyberweerbaarheid van eindgebruikers, organisaties en de samenleving vraagt om effectieve aanpakken en interventies. Het is daarom van belang om in kaart te brengen welke effecten en resultaten interventies behalen (Ooyen-Houben & Leeuw, 2010). Dankzij de toegenomen aandacht voor de thema's cyberweerbaarheid, cybersecurity en online criminaliteit zien we dat er veel interventies worden uitgevoerd. Maar een evaluatie van de effecten van deze interventies en aanpakken ontbreekt veelal. Ook zijn de interventies niet altijd ontwikkeld op basis van vooronderzoek onder de doelgroep en ontbreekt vaak een theoretische onderbouwing, oftewel interventies en aanpakken zijn vaak niet evidence-based (Bluhm et al., 2024). Leukfeldt (2024) roept daarom op om bij het versterken van de cyberweerbaarheid scherp oog te hebben voor (I) de onderbouwing en (II) het meten van de effecten van interventies om ervoor te zorgen dat we de

juiste vraagstukken op een onderbouwde manier aanpakken. Hier gaan we in hoofdstuk 3 verder op in voor gedrag en gedragsverandering, maar dat geldt natuurlijk evengoed voor interventies die zich richten op daders, slachtoffers en versterking van de cyberweerbaarheid in het algemeen.

2





SLACHTOFFER-SCHAP

Rutger Leukfeldt, Jildau Borwell, Susanne van 't Hof-de Goede, Sifra Matthijsse, Remco Spithoven

2.1 AARD EN OMVANG SLACHTOFFERSCHAP ONDER BURGERS

De digitalisering van onze samenleving heeft grote gevolgen voor criminaliteit en slachtofferschap. We zien een dalende trend bij slachtofferschap van traditionele vormen van criminaliteit, maar een toename van slachtofferschap van online criminaliteit. Recente cijfers van het CBS (2024) laten zien dat:

- in 2023 20% van de Nederlanders van vijftien jaar en ouder slachtoffer is geweest van één of meer (traditionele, offline) gewelds-, vermogens- of vandalismedelicten, waarbij het totaalaantal slachtoffers sinds 2005 met 53% is gedaald;
- in 2023 16% van de Nederlanders van vijftien jaar en ouder slachtoffer is geweest van een of meerdere vormen van online criminaliteit; een aandeel dat iets lager ligt dan in 2021 (17%), maar hoger ligt dan in 2017 (11%) en 2012 (12%) (CBS, 2024).

Nederlanders werden volgens het CBS in 2023 het vaakst slachtoffer van een vorm van online oplichting en fraude (9%), gevolgd door hacking (6%) en online bedreiging en intimidatie (3%). Hierbij moet worden opgemerkt dat het CBS lang niet alle vormen van online criminaliteit meet. Zo komt slachtofferschap van malware veelvuldig voor (Domenie et al., 2013; Beerthuizen et al., 2020; Matthijsse et al., 2024), maar ontbreken cijfers over andere vormen van online criminaliteit,

zoals datingfraude (Beerthuizen et al., 2020). Bovendien laten cijfers op basis van zelfrapportage een onvolledig beeld zien, omdat mensen niet altijd weten dat ze slachtoffer zijn, zoals bij diefstal van persoonsgegevens. Ook kunnen respondenten zich niet herkennen in het label 'slachtoffer', omdat dit voor hen een te negatieve lading heeft. Op basis van het voorgaande wordt verwacht dat slachtofferschap van online criminaliteit in werkelijkheid nog hoger is dan de cijfers laten zien.

Politiecijfers laten echter een ander beeld zien, namelijk slechts zo'n 14.000 registraties van online criminaliteit in Nederland in 2022. Onderzoek van Ruiter en collega's (2023) laat zien dat ongeveer 13% van de slachtoffers melding maakt en gemiddeld slechts 8% van de slachtoffers aangifte doet bij de politie. Er zijn verschillende redenen voor het grote verschil tussen deze cijfers en de prevalentie gebaseerd op zelfrapportage. Ten eerste is onder slachtoffers van online criminaliteit sprake van een lage aangiftebereidheid, nog lager dan bij traditionele, offline delicten (Van de Weijer et al., 2018; Van de Weijer & Leukfeldt, 2020). Ten tweede registreert de politie online criminaliteit slechts beperkt. In een recent onderzoek naar de in- en doorstroom van online criminaliteit in de strafrechtketen werd met *predictive text-mining*-modellen gevonden dat de meeste vormen van online criminaliteit in minder dan 1% (met een maximum van 4% voor alle gedigitaliseerde criminaliteit tezamen) van de registraties voorkwamen (Ruiter et al., 2023).

> Toekomstig onderzoek zou zich moeten richten op vragen zoals: Hoe kan slachtofferschap van online criminaliteit nauwkeuriger worden gemeten, rekening houdend met het gebrek aan en de beperkingen van surveyonderzoek en registratiedata? Hoeveel burgers in Nederland worden jaarlijks daadwerkelijk slachtoffer van online criminaliteit, inclusief niet-geregistreerde gevallen? En op welke doelgroepen en vormen van online criminaliteit zouden professionals zich moeten richten wat betreft beleid en aanpak ten aanzien van slachtofferschap?

2.2 AARD EN OMVANG VAN SLACHTOFFERSCHAP ONDER BEDRIJVEN

Organisaties lopen het risico om het doelwit te worden van cybercriminelen. Vaak lezen we in nieuwsberichten over organisaties die getroffen zijn door ransomware of over banken die te maken hebben met een DDoS-aanval, waardoor hun online diensten niet beschikbaar zijn.

Het aantal bedrijven dat in de Cybersecuritymonitor van het CBS in 2022 een ICT-veiligheidsincident door een aanval van buitenaf rapporteerde, varieerde van 20% onder grote bedrijven (> 250 medewerkers) tot 5% onder bedrijven met 2-10 medewerkers (CBS, 2023). Hiernaast rapporteerde respectievelijk bijna 50% en 12% een ICT-veiligheidsincident met een interne oorzaak. Ongeveer de helft van alle incidenten heeft tot kosten geleid voor de bedrijven. Sinds 2016 laat het aantal incidenten een dalende trend zien. Het aantal meldingen van datalekken bij de Autoriteit Persoonsgegevens is stabiel tot licht dalend (CBS, 2023).

Vooral midden- en kleine bedrijven (mkb) – veruit het grootste deel van de bedrijven in Nederland en Europa – zijn kwetsbaar voor de gevolgen van digitale aanvallen, omdat zij vergeleken met de grotere organisaties achterlopen op het gebied van cybersecurity. In 2014 liet het eerste grootschalige onderzoek naar slachtofferschap van online criminaliteit in het mkb zien dat 28% van de onderzochte bedrijven slachtoffer was geworden van online criminaliteit, waarbij malware, aankoopfraude, phishing en hacken het meest werden gerapporteerd (Veenstra et al., 2015). In 2019 bleek zo'n 20% van de deelnemende mkb'ers het afgelopen jaar slachtoffer te zijn geworden van online criminaliteit met schade als gevolg (Notté et al., 2019). Het vaakst werd hierbij slachtofferschap van cybercriminaliteit gerapporteerd (18%), waarvan malware (31%) en ransomware (17%) het meest genoemd werden. Een kleinere groep werd slachtoffer van gedigitaliseerde criminaliteit (9%), waarbij phishing met financiële schade tot gevolg (10%) het meest gerapporteerd werd.

Ook werden bedrijven slachtoffer van beide soorten online criminaliteit.

Een delict dat sterk in opkomst lijkt te zijn geweest onder Nederlandse bedrijven is ransomware. Gemiddeld ervaarde 0,7% van de Nederlandse ondernemingen met twee of meer medewerkers een ransomware-aanval in 2021. Dit percentage neemt toe naarmate ondernemingen groter zijn, namelijk van zo'n 0,5% van de bedrijven met 2 tot 10 medewerkers tot 4% van de ondernemingen met meer dan 250 medewerkers (CBS, 2023). Van de ransomware-slachtoffers betaalde 11% het losgeld, stapte 13% naar de politie en schakelde 39% hulp in van een cybersecuritybedrijf. Uit onderzoek vanuit de cybersecuritysector blijkt dat dergelijke incidenten en crises ook na lange tijd nog een stevige impact kunnen hebben op de medewerkers die erbij betrokken zijn geweest (Northwave, 2022).

Recent is er ook internationaal vergelijkend onderzoek gedaan naar slachtofferschap van online criminaliteit in het mkb. In de Eurobarometer (2022) zijn resultaten gepubliceerd over 12.863 Europese mkb'ers, waarvan 528 uit Nederland. Nederlandse mkb'ers werden significant vaker dan andere Europese mkb'ers slachtoffer van online criminaliteit in 2021 (37% versus 28% van alle Europese mkb'ers) en rapporteerden iets minder vaak schade (50% versus 58% van alle Europese mkb'ers). De delicten die het vaakst gerapporteerd werden, waren malware (resp. 17% en 14% van alle Europese mkb'ers) en phishing (resp. 21% en 11% van alle Europese mkb'ers). Vier op de tien Nederlandse mkb'ers hebben het incident nergens gemeld, vergeleken met 44% van de Europese mkb'ers. De ondernemers die het slachtofferschap wel hebben gemeld, deden dit het vaakst bij de verkoper of dienstverlener van bijvoorbeeld het bedrijfsonderdeel dat aangevallen werd, de politie en/of de internetprovider. Het ging om respectievelijk 21%, 17% en 11% van de slachtoffers. Dit meldingsgedrag lijkt vergelijkbaar met Europese mkb'ers, respectievelijk 17%, 18% en 12% (Eurobarometer, 2022).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Wat is de daadwerkelijke omvang van het slachtofferschap van online criminaliteit onder Nederlandse organisaties, inclusief niet-geregistreerde gevallen? Wat is de impact van het slachtofferschap van online criminaliteit onder Nederlandse organisaties, hun werknemers en hun omgeving? Welke ontwikkelingen in omvang en impact zijn er te voorspellen ten aanzien van het slachtofferschap van online criminaliteit onder Nederlandse organisaties?

2.3 IMPACT EN BEHOEFTEN SLACHTOFFERS

De impact van online criminaliteit op slachtoffers wordt vaak onderschat (Van 't Hoff-de Goede & Leukfeldt, 2024; Leukfeldt et al., 2018, 2019b). Onderzoek laat echter zien dat de ervaren impact van online criminaliteit grotendeels overeenkomt met die van traditionele delicten (Bluhm et al., 2022; Borwell et al., 2021, 2022; Leukfeldt et al., 2018; Notté et al., 2021; Richards & Cross, 2018; Leukfeldt et al., 2019). Naast financiële gevolgen[1] zijn er vaak ook psychologische en emotionele gevolgen. Slachtoffers ervaren bijvoorbeeld verlies van vertrouwen, schuldgevoelens, schaamte, woede, frustratie, stress, angst, onveiligheidsgevoelens, machteloosheid, verdriet, teleurstelling en in sommige gevallen suïcidale neigingen (Van 't Hoff-de Goede & Leukfeldt, 2021; Leukfeldt et al., 2018, 2019b).

Bepaalde unieke kenmerken van online delicten kunnen zelfs leiden tot een grotere impact dan die van traditionele criminaliteit. Zo kan er sprake zijn van permanent en terugkerend slachtofferschap, bijvoorbeeld omdat beelden online blijven en weer kunnen opduiken, zoals bij sextortion of wraakporno (Leukfeldt et al., 2018, 2019b; Yeung et al., 2014). Daarnaast kunnen slachtoffers online voortdurend worden benaderd, zoals bij stalking en bedreiging (Fox, 2016; Malsch

1 Indirecte financiële gevolgen zijn bijvoorbeeld het verlies van werk en de tijd die het kost om aangifte te doen en/of pogingen van het slachtoffer om de dader te stoppen.

et al., 2015; Maple et al., 2011; Sheridan & Grant, 2007; Short et al. & Maple, 2014). Door de onzichtbaarheid van de dader voelen sommige slachtoffers zich nergens veilig (Leukfeldt et al., 2018).

Bovendien komt bij slachtofferschap van online delicten vaak *victim blaming* voor (Cross, 2018; Leukfeldt et al., 2018, 2019b). Naast schaamte en zelfverwijt ervaren slachtoffers afkeuring van de hulpverleningsinstanties en hun sociale omgeving. Dit kan te maken hebben met de relatieve onbekendheid met de impact van online criminaliteit. Ook kan meespelen dat slachtoffers vaak onbedoeld een actieve rol speelden in het delict, bijvoorbeeld door zelf inloggegevens of beelden te versturen, waardoor de neiging is om de schuld bij het slachtoffer te leggen in plaats van bij de dader (Borwell et al., 2021).

Als gevolg van het delict blijken slachtoffers van online criminaliteit grotendeels vergelijkbare behoeften te hebben als slachtoffers van traditionele criminaliteit op emotioneel, praktisch en informationeel vlak (Leukfeldt et al., 2018). Veelal hebben zij behoefte aan eerste opvang, zorg, steun, erkenning en veroordeling van de dader. Echter, de afhandeling van online delicten bij de politie verloopt vaak moeizaam. Veelal wordt geen dader gevonden, omdat bijvoorbeeld de ernst niet wordt onderkend of de opsporing te complex lijkt te zijn (Bijleveld et al., 2021; Button et al., 2022; Leukfeldt et al., 2018).

Momenteel is nog weinig bekend over de impact en behoeften van slachtoffers van online criminaliteit over de tijd heen, en over het optreden van langetermijngevolgen. Hier is longitudinaal onderzoek voor nodig. Daarnaast is nog weinig bekend over mogelijke verklaringen voor de impact en slachtofferbehoeften na online criminaliteit. Zo is er relatief weinig theoretische onderbouwing voor de impact van slachtofferschap na online criminaliteit en behoeften van slachtoffers vanuit traditionele of nieuwe theorieën (Agustina, 2015; Borwell et al., 2021, 2022; Longo, 2018; Van der Wagen & Pieters, 2018). Als laatste is er zeer beperkt inzicht in de gevolgen van de verwevenheid van traditionele

en online criminaliteit voor slachtoffers (Van 't Hoff-de Goede & Janssen, 2024; Fox, 2016; Roks et al., 2021).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe ontwikkelen impact en behoeften van slachtoffers van online criminaliteit zich over de tijd heen? Welke factoren beïnvloeden het ontstaan en de ernst van de impact en behoeften van slachtoffers van online criminaliteit? In hoeverre kunnen traditionele en nieuwe theoretische benaderingen bijdragen aan het begrijpen van de impact en behoeften van slachtoffers van online criminaliteit? Welke gevolgen hebben de verwevenheid tussen traditionele en online criminaliteit voor slachtoffers? En in hoeverre beïnvloeden nieuwe aanvalsvormen, zoals AI-gegenereerde en AI-gestuurde aanvallen het slachtofferschap?

2.4 RISICOFACTOREN VOOR SLACHTOFFERSCHAP ONDER BURGERS

Er zijn flink wat studies gedaan naar risicofactoren voor slachtofferschap van online criminaliteit (Van 't Hoff-de Goede & Leukfeldt, 2024), maar er zijn nog maar weinig aantoonbare voorspellers van slachtofferschap gevonden. Dit komt onder andere doordat in studies verschillende vormen van online criminaliteit centraal staan of door methodologische keuzes en inherente tekortkomingen.

Onderzoekers hebben zich eerst gericht op achtergrondkenmerken van slachtoffers. Zo werd lang gedacht dat hoe meer burgers online zijn, hoe meer risico zij lopen op slachtofferschap van cybercriminaliteit (Cheng et al., 2020; Domenie et al., 2013; Guerra & Ingram, 2020; Holt et al., 2020b; Van Wilsem, 2013a, 2013b). Recente longitudinale studies wijzen erop dat deze relatie mogelijk niet causaal is en dat de toename van slachtofferschap door andere factoren wordt verklaard (Guerra & Ingram, 2020; Van 't Hoff-de Goede et al., 2023; Van de Weijer, 2019). Ook worden jongeren weliswaar gemiddeld genomen vaker slachtoffer van online criminaliteit

dan ouderen, maar er wordt verwacht dat ook deze relatie samenhangt met andere factoren.

Meer recent proberen onderzoekers slachtofferschap te verklaren vanuit online gedrag, zoals onveilig omgaan met wachtwoorden en hyperlinks in e-mails. Veel mensen gedragen zich online slechts in beperkte mate veilig (Cain et al., 2018; Diaz et al., 2020; Van 't Hoff-de Goede et al., 2019; Jansen & Leukfeldt, 2015; Li et al., 2020). Onderzoek naar de gevolgen van onveilig online gedrag staat nog in de kinderschoenen. Dit komt deels doordat deze studies veelal gebaseerd zijn op zelfgerapporteerd online gedrag. Wat mensen zeggen dat zij online doen, is echter niet altijd hetzelfde als wat zij daadwerkelijk online doen (Van 't Hoff-de Goede et al., 2019; Parry et al., 2021; Sharif et al., 2018; Wilcockson et al., 2018). Om deze reden is onderzoek nodig dat daadwerkelijk online gedrag meet en internetgebruikers door de tijd heen volgt. Enkele beschikbare studies wijzen erop dat veel bestanden downloaden en veel verschillende websites en netwerken bezoeken de kans op slachtofferschap van malware en phishing verhoogt (Lévesque et al., 2018; Ovelgönne et al., 2017; Sharif et al., 2018). Een longitudinale studie waarin daadwerkelijk online gedrag werd gemeten, vond echter geen verband met het risico op slachtofferschap van online criminaliteit in het jaar erna (Van 't Hoff-de Goede et al., 2023). Er is dan ook meer onderzoek nodig naar de relatie tussen online gedrag en het risico op slachtofferschap van online criminaliteit.

Studies naar de relatie tussen zelfcontrole en slachtofferschap van online criminaliteit wijzen er consistent op dat individuen met een lage zelfcontrole kwetsbaarder zijn voor online criminaliteit en meer risico lopen op slachtofferschap (Holt et al., 2020b; Mesch & Dodel, 2018; Mikkola et al., 2020; Partin et al., 2021). Het is echter tot op heden onduidelijk of de link tussen zelfcontrole en slachtofferschap van online criminaliteit een directe causale relatie betreft, of bijvoorbeeld via (bepaald) gedrag loopt. Dat dit tot op heden niet duidelijk is, komt onder andere doordat bovengenoemde factoren

zelden gelijktijdig en longitudinaal worden bestudeerd (Van 't Hoff-de Goede et al., 2023).

Tot slot is eerder slachtofferschap een belangrijke risicofactor voor toekomstig slachtofferschap van online criminaliteit (Van 't Hoff-de Goede et al., 2023; Näsi et al., 2021). Er zijn nog steeds geen bewezen verklaringen voor waarom deze personen een verhoogd risico lopen op herhaald slachtofferschap van online criminaliteit. Ook het onderzoek op dit gebied staat nog in de kinderschoenen. Tevens is meer onderzoek nodig om te komen tot onderbouwde achtergrondkenmerken als eventuele risicofactoren.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Welke potentiële risicofactoren kunnen worden geïdentificeerd op basis van theorie en praktijk en in hoeverre zijn deze factoren gerelateerd aan slachtofferschap van online criminaliteit? Hoe ontwikkelen relaties tussen risicofactoren en slachtofferschap zich over de tijd? In hoeverre hangt de relatie tussen een lage zelfcontrole en slachtofferschap van online criminaliteit samen met andere gerelateerde factoren? Hoe kunnen mensen met een lage zelfcontrole beter worden bereikt en geholpen door preventieve maatregelen? Hoe kan daadwerkelijk online gedrag en de relatie met slachtofferschap van online criminaliteit nauwkeuriger gemeten en onderzocht worden? En welke risicofactoren dragen bij aan herhaald slachtofferschap van online criminaliteit?

2.5 AANGIFTEBEREIDHEID

Hoewel veel individuen en organisaties slachtoffer zijn van online criminaliteit, komt dit niet tot uiting in de aangiftecijfers. Slachtoffers van online criminaliteit zijn minder bereid om aangifte te doen bij de politie dan slachtoffers van traditionele criminaliteit (Graham et al., 2020; Van de Weijer et al., 2019). Dit geldt voor zowel individuen (tussen de 10% en 21%) als organisaties (tussen de 7% en 18%) (Akkermans et al., 2023; De Kimpe, 2020; Domenie et al., 2013; European

Commission, 2022; Van de Weijer et al., 2020; Veenstra et al., 2015; Wanamaker, 2019). Bovendien benadert een deel van de slachtoffers andere instanties of personen voor informatie of hulp, zoals vrienden of familie, een financiële instelling of een cybersecuritybedrijf (Akkermans et al., 2023; Van de Weijer et al., 2020; Voce & Morgan, 2023). Het is van belang dat slachtoffers aangifte doen bij de politie, aangezien aangiftes invloed hebben op de mate waarin het strafrechtelijk systeem effectief is in de aanpak van online criminaliteit, het afschrikken van (potentiële) daders en het voorkomen van slachtofferschap (Goudriaan, 2006; Greenberg & Ruback, 1992; Skogan, 1984). Dit betekent dan wel dat er ook (actief) gehandeld moet worden op deze aangiften.

In de afgelopen decennia is veel onderzoek verricht naar aangiftebereidheid na slachtofferschap van traditionele vormen van criminaliteit. Onderzoek naar de meldingsbereidheid van online criminaliteit is daarentegen schaars. De redenen waarom slachtoffers ervoor kiezen om geen melding te doen bij de politie zijn divers. Slachtoffers vinden het incident niet serieus genoeg, ze hebben het zelf of met behulp van een andere partij opgelost, of ze denken dat de politie niets voor hen kan betekenen (Akkermans et al., 2023; Cybbar & CSD, 2023; Matthijsse et al., 2024; Van de Weijer et al., 2020, 2021; Veenstra et al., 2015; Voce & Morgan, 2023; Wanamaker, 2019). Daarentegen zijn belangrijke redenen om online criminaliteit wel te melden dat slachtoffers willen dat de dader gepakt wordt of om te voorkomen dat het henzelf of een ander (nogmaals) overkomt (Matthijsse et al., 2024; Van de Weijer et al., 2021; Voce & Morgan, 2023). Er is nog weinig bekend over de invloed van demografische of organisatiekenmerken (De Kimpe, 2020; Kemp et al., 2023; Van de Weijer et al., 2021). Bovendien blijkt uit eerder onderzoek dat er een grote discrepantie bestaat tussen de intentie om te melden en het daadwerkelijke meldgedrag (European Commission, 2022; Matthijsse et al., 2024; Van de Weijer et al., 2020).

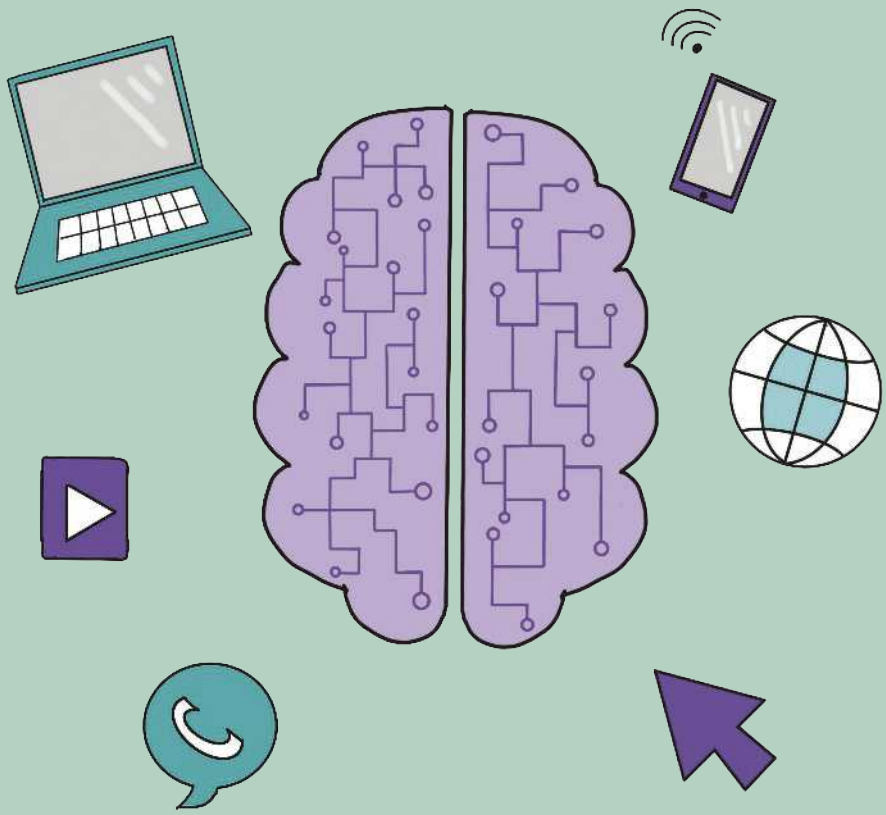
Al met al is meer inzicht nodig in de factoren, motivaties en barrières die gerelateerd zijn aan de beslissing om online criminaliteit te melden bij de politie, waarbij onderscheid

gemaakt wordt tussen de verschillende typen slachtoffers en verschijningsvormen van online criminaliteit. Daarnaast zou toekomstig onderzoek zich kunnen richten op andere formele en informele partijen die slachtoffers bijstaan, en de mate waarin deze partijen effectief zijn in het ondersteunen van slachtoffers en het bestrijden van online criminaliteit. Dit kan aanknopingspunten bieden voor het verhogen van de meldingsbereidheid en/of het verbeteren van de ondersteuning van slachtoffers van online criminaliteit.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: In hoeverre zijn slachtoffers van online criminaliteit bereid om slachtofferschap te melden, bij welke formele en informele partijen doen zij dit en waarom? Wat zijn de belangrijkste redenen voor het wel of niet melden van slachtofferschap van online criminaliteit? In hoeverre zijn demografische, delict- en psychologische kenmerken gerelateerd aan de beslissing om slachtofferschap van online criminaliteit te melden? Welke invloed heeft de meldplicht uit de Cyberbeveiligingswet (Cbw) op de meldingsbereidheid van organisaties die wel en niet onder de NIS2-richtlijn[1] vallen? Wat betekent een verhoogd aantal meldingen voor de formele en informele partijen?

1 Network and Information Security (NIS2) richtlijn

3



GEDRAG EN GEDRAGS-VERANDERING

Remco Spithoven, Kimberly Bluhm, Sander Ebbers, Susanne van 't Hoff-de Goede, Ynze van Houten, Jurjen Jansen, Milou Kievik, Rick van der Kleij, Rutger Leukfeldt, Ellen Misana-ter Huurne, Marcel Spruit, Bruno Verweijen

3.1 VEILIG ONLINE GEDRAG

Voor het verklaren van (on)veilig gedrag zijn in de literatuur verschillende theorieën en modellen ontwikkeld. Enkele voorbeelden zijn de *Protection Motivation Theory* (Rogers, 1975; 1983; Rogers & Prentice-Dunn, 1997); *Theory of Planned Behavior* (Ajzen, 1991); *Health Belief Model* (Maiman & Becker, 1974); *Extended Parallel Processing Model* (Witte, 1992; 1996) en het *Risk Information Seeking & Processing Model* (Griffin et al., 1994, 1998, 1999) en meer recentelijk het *COM-B-model* (Michie et al., 2011). Meer hierover staat in paragraaf 3.3. Hoewel deze modellen oorspronkelijk niet voor het cyberweerbaarheidsdomein zijn ontwikkeld, worden ze daar steeds vaker toegepast (bijv. Jansen, 2018; Van der Kleij et al., 2020a, 2020b).

De *Protection Motivation Theory* gaat uit van de motivatie van elk individu om zich tegen risico's en gevaar te beschermen en biedt handvatten voor het begrijpen van veranderingen in houdingen ten opzichte van risico's. Centraal staan de inschatting van gevaar (*threat appraisal*) en de inschatting van de uitkomsten van de eigen omgang daarmee (*coping appraisal*). Onderdeel van deze mix zijn verklarende

elementen als de waargenomen (a) kwetsbaarheid (kans); (b) ernst (impact); (c) responseffectiviteit; (d) zelfeffectiviteit, en (e) barrières of obstakels voor het ondernemen van actie (*response costs*).

De overige genoemde theorieën voegen elk eigen aspecten aan de mix van verklarende variabelen toe. Zo voegt de *Theory of Planned Behavior* (TPB) (Ajzen, 1991) het aspect van (f) subjectieve normen toe. Dit betreft de mate waarin zelfbeschermend gedrag in een sociale context als gewenst of vanzelfsprekend wordt beschouwd. Het *Health Belief Model* (Maiman & Becker, 1974) richt zich, net zoals TPB, op de invloed van de (g) gedragsintentie op het uiteindelijke gedrag. Het *Extended Parallel Processing Model* (Witte, 1992, 1996) legt de nadruk op de (h) emotionele reactie die ontstaat als gevolg van de afwegingen. Hoe intenser de emotionele reactie is, hoe meer mensen geneigd zijn actie te ondernemen. Het *Risk Information Seeking & Processing Model* (Griffin et al., 1994, 1998, 1999) focust zich op (i) de omvang van het risico en de kans op (j) herhaling van een gevaar.

Tevens zijn enkele remmende factoren in kaart gebracht. Zo is er sprake van (k) een zogenaamde *optimistic bias*, waarbij mensen geneigd zijn om het risico vooral toe te schrijven aan anderen dan henzelf. Dit fenomeen is in de literatuur over risicoperceptie bekend onder verschillende namen, maar is vastgesteld voor *'(...) over a thousand studies and for a diverse array of undesirable events, including diseases, natural disasters, and a host of other events ranging from unwanted pregnancies and home radon contamination to the end of romantic relationships'* (Shepperd et al., 2013, p. 232) en komt neer op een ontkenning van risico's voor zichzelf (Spithoven, 2017). Voor veilig digitaal gedrag specifiek is een remmende werking van (l) cyber *fatigue* vastgesteld (vrij vertaald: cybermoeheid). Dit betreft de bevinding dat de overvloed aan cybersecurity-gerelateerde informatie, gedragsadviezen en gevraagde acties van het individu om de cyberveiligheid in stand te houden door de ontvangers als overweldigend en vermoeiend kan worden ervaren (Reeves et al., 2021).

Er is meer onderzoek nodig naar de verklaringen van daadwerkelijk (on)veilig online gedrag. Zo heeft eerder onderzoek aangetoond dat de aanname dat mensen met veel kennis van online veiligheid zich ook veiliger online gedragen niet klopt (Cain et al., 2018; Van 't Hoff-de Goede et al., 2019). De inzet van awarenesscampagnes en -trainingen zou zodoende wel kunnen bijdragen aan de kennis van internetgebruikers over veilig online gedrag, maar vervolgens niet hun daadwerkelijke gedrag veranderen.

> Er is dan ook meer onderzoek nodig naar manieren waarop veilig online gedrag kan worden bewerkstelligd onder internetgebruikers. Het is van belang om zowel de positieve als negatieve verklaringen van digitaal veilig gedrag te begrijpen: Welke oorzaken liggen ten grondslag aan (on)veilig digitaal gedrag van mensen? Welke factoren stimuleren digitaal veilig gedrag van mensen? En welke factoren belemmeren digitaal veilig gedrag van mensen en hoe zijn deze factoren te beïnvloeden? Welke interventies zijn geschikt om mensen zich veilig te laten gedragen en hoe effectief zijn deze interventies?

3.2 BEWUSTZIJN EN RISICOPERCEPTIE

In de verklaring voor (on)veilig gedrag van mensen met betrekking tot digitale gegevens en systemen speelt de individuele motivatie een centrale rol. De motivatie voor (on)veilig gedrag is op zijn beurt weer afhankelijk van de risicoperceptie en de risicoattitude. De risicoperceptie, de risicoattitude en de motivatie voor gedrag kunnen, bijvoorbeeld in een organisatie, ook worden beïnvloed door groepsprocessen. Er is veel geschreven over hoe zelfbeschermend gedrag tot stand komt (o.a. Jansen, 2018; Spithoven, 2020; Spithoven et al., 2022; Spruit et al., 2024). Zelfbeschermend gedrag wordt samenvattend gestuurd door de gedragsintentie. Lang niet altijd wordt deze intentie ook omgezet in daadwerkelijk gedrag. Daarbij zien we dat deze kans volgens de theorie toeneemt als men (I) ervaart controle te hebben over een risico en bijbehorend

beschermend gedrag; (II) men een hoge risicoperceptie heeft waarbij zowel kansen als gevolgen hoog worden ingeschat en er (III) een sociale norm heerst dat het normaal of zelfs vanzelfsprekend is je tegen het risico te beschermen (Leukfeldt et al., 2020).

Eén van de aspecten die gedrag kunnen beïnvloeden is de angst om slachtoffer te worden van online criminaliteit. In de literatuur hierover wordt onderscheid gemaakt tussen een disfunctionele en een functionele zorg over slachtofferschap, waarbij disfunctionele zorg leidt tot een negatieve invloed op de kwaliteit van leven en *niet* aanzet tot het aanpassen van het eigen gedrag en functionele zorg over slachtofferschap leidt tot waakzaamheid en voorzorgen (zie Jackson & Gray, 2010; Fattah, 1993; Hale, 1996; Warr, 2000; Ditton & Innes, 2005). In de psychologische literatuur wordt gesproken over een vergelijkbaar onderscheid, namelijk *emotion-focused* en *problem-focused coping*. In paragraaf 3.3 gaan we hier uitgebreider op in.

> Relevante onderzoeksvragen zijn: Hoe beleven mensen digitale dreigingen en relevante kwetsbaarheden? Welke gevolgen verwachten mensen van slachtofferschap? Hoe schatten zij digitale risico's in? In hoeverre is er sprake van een functionele zorg over slachtofferschap en hoe kan deze worden gestimuleerd? In hoeverre vertonen mensen gedrag om effectief met digitale risico's om te gaan?

3.3 RISICOCOMMUNICATIE EN GEDRAGSVERANDERING

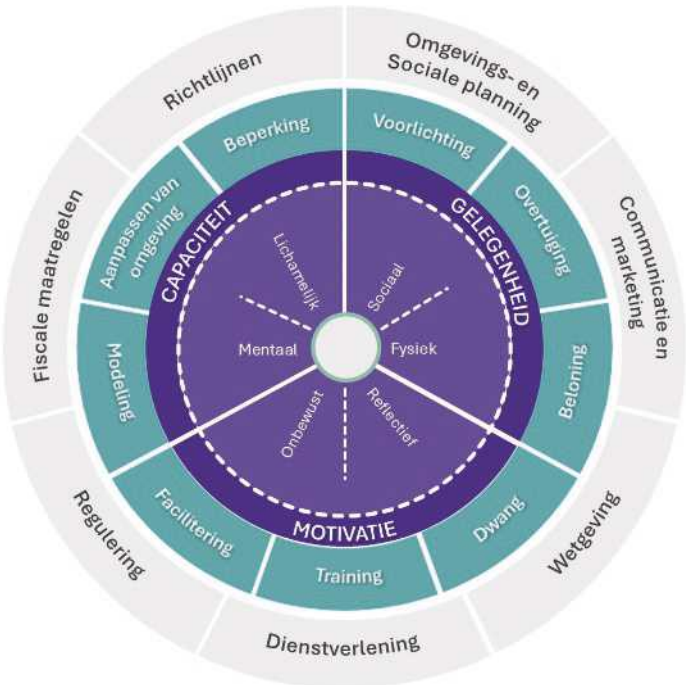
Uit eerder onderzoek is gebleken, dat effectieve risicocommunicatie en voorlichting een bijdrage leveren aan de capaciteit van mensen om zichzelf of hun organisatie te beschermen tegen de mogelijke risico's en effecten van cybercrime (Sheng et al., 2010). Risicocommunicatie is in essentie bedoeld om individuen te ondersteunen om zo geïnformeerde beslissingen te nemen ten aanzien van de risico's waarmee zij worden geconfronteerd (Wade et al., 1992). Risicocommuni-

catie is idealiter maatwerk. Voor een optimaal effect moet de communicatie worden gebaseerd op de beleving en percepties van de doelgroep (Ter Huurne, 2008). Daarnaast is het van belang om voor iedere doelgroep de communicatiestrategie te laten aansluiten op hun voorkeuren, kenmerken, percepties en huidige gedragingen (Kievik, 2017).

Juist bij het bevorderen van preventief gedrag speelt risicocommunicatie een rol die verder gaat dan louter informeren. Het doel is immers om individuen in staat te stellen en te stimuleren om zichzelf daadwerkelijk (beter) te beschermen. Hiervoor is een aantal aspecten belangrijk. Mensen moeten: (I) *weten* (risicobewustzijn); (II) *willen* (perceptie eigen verantwoordelijkheid); (III) *kunnen* (zelfeffectiviteit en waargenomen gedragscontrole) en (IV) *doen* (gedrag). In de wetenschappelijke en praktijkgerichte discipline van de risicocommunicatie zijn aanvullende inzichten opgedaan over hoe gedragsverandering ten aanzien van risico's tot stand komt. In de basis kunnen mensen op twee manieren reageren op informatie over mogelijke risico's, namelijk *problem-focused coping* of *emotion-focused coping* (Lazarus & Folkman, 1984).

Bij problem-focused coping is het doel om het 'probleem', in dit geval het risico of de dreiging van cybercrime, te minimaliseren. In de eerdergenoemde *Extended Parallel Processing* (EPPM; Witte, 1992) en de *Protectie Motivatie Theorie* (PMT; Rogers & Prentice-Dunn, 1997) wordt dit het '*danger control process*' genoemd. Dit is het gedrag dat men door middel van campagnes beoogt te bereiken; mensen gaan hun gedrag aanpassen op basis van de gegeven gedragsadviezen met als doel zichzelf te beschermen tegen het gevaar. Deze communicatie speelt in op de waargenomen gedragscontrole. Bij waargenomen gedragscontrole gaat het om de mate waarin men zichzelf in staat acht het gewenste gedrag ook echt te kunnen uitvoeren, waarbij het zowel gaat over zelfvertrouwen en eigen vaardigheden (intern) als ervaren gebruiksvriendelijkheid (extern). Daarnaast betreft het de beleving van de mate waarin dit gedrag zal bijdragen aan het minimaliseren van het gevaar of de mogelijke gevolgen daarvan.

Binnen Cyberweerbaar NL maken wij met het oog op gedragsverandering gebruik van het *Behaviour Change Wheel*, wat een doorontwikkeling op het *Capability Opportunity Motivation Behaviour*-model (COM-B) voor effectieve gedragsverandering is (Michie et al., 2011) en maar liefst negentien evidence-based inzichten over gedragsverandering samenbrengt (Figuur 2). Elke interventie start met het begrijpen van het gedrag dat men beoogt te veranderen. Mogelijke, aanvullende interventies bij risicocommunicatie zijn, afhankelijk van de achtergronden van het gedrag en de doelen van de interventie: voorlichten, overtuigen, belonen, dwingen, trainen, faciliteren, voorschrijven, aanpassen van de omgeving en beperken. Daarbij zijn ook combinaties mogelijk.



Figuur 1. Nederlandse vertaling van het *Behaviour Change Wheel* (o.b.v. Michie et al., 2018)

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Welke factoren zijn van invloed op *problem-focused coping* door eindgebruikers ten aanzien van digitale risico's? Welke factoren zijn van invloed op *emotion-focused coping* door eindgebruikers ten aanzien van digitale risico's? Hoe kunnen eindgebruikers met op maat gemaakte risicocommunicatie hun veilig digitaal gedrag verbeteren (*problem-focused coping*)? Hoe kunnen gedragsinterventies risicocommunicatie over online veilig gedrag versterken om mensen tot gedragsverandering te laten komen?

3.4 EFFECTIVITEIT VAN BESTAANDE INTERVENTIES

Om de cyberweerbaarheid van eindgebruikers te verhogen, worden diverse interventies ontwikkeld en uitgevoerd (voor overzichten zie onder andere VAR [2022] en CCV [2023]). Het is van belang om in kaart te brengen welke effecten en resultaten interventies behalen (Ooyen-Houben & Leeuw, 2010). De literatuur suggereert hierbij dat drie onderdelen mogelijk invloed hebben op de effectiviteit van interventies (Durlak & DuPre, 2008; Ooyen-Houben & Leeuw, 2010): het bereik (ofwel: bereikt de interventie de beoogde doelgroep), de programma-integriteit (ofwel: is de interventie uitgevoerd zoals aanvankelijk beoogd) en de dosering (ofwel: wordt de interventie met voldoende intensiteit en compleet uitgevoerd).

Om een interventie als effectief te beschouwen, dient het aanvankelijk opgestelde doel te zijn behaald en moet de interventie een positieve gedragsverandering teweeg hebben gebracht (Sondorp et al., 2019). Om bovenstaande onderdelen meetbaar te maken, zijn concrete variabelen en doelstellingen noodzakelijk (Davies, 2006).

Ondanks de aandacht voor het thema en het ontwikkelen van interventies, is het onduidelijk in hoeverre interventies gericht op cyberweerbaarheid de aanvankelijk opgestelde doelen behalen en in hoeverre deze interventies (op lange termijn) effectief zijn. We zien dat interventies worden

uitgevoerd, maar een (effect)evaluatie ontbreekt veelal. Ook zijn de interventies niet altijd ontwikkeld op basis van vooronderzoek onder de doelgroep en ontbreekt vaak een theoretische onderbouwing, oftewel ze zijn vaak niet evidence-based. Tevens vraagt elke doelgroep om een op maat gemaakte aanpak die begint bij het achterhalen en verklaren van het risicobewustzijn en het preventieve gedrag. Ook in het design van de interventies worden bovenstaande onderdelen niet altijd op een meetbare manier meegenomen, bijvoorbeeld door doelen op te stellen die geen concrete aantallen bevatten over de te bereiken doelgroep. Hierdoor is het achteraf niet mogelijk om te toetsen in hoeverre de doelgroep daadwerkelijk wordt bereikt (Bluhm et al., 2024). In het verlengde hiervan is het niet enkel van belang om te meten in hoeverre interventies effectief zijn, maar ook welke onderdelen in een interventie deze effectiviteit teweegbrengen (Omlo et al., 2013). Het is bekend dat de effecten van interventies na verloop van tijd afnemen. Op basis van deze bevindingen kunnen toekomstige interventies worden vormgegeven.

Het toepassen van methodieken, zoals *Intervention Mapping* (Eldridge et al., 2016) en het eerdergenoemde *Behaviour Change Wheel* (Michie et al., 2011), bevordert dat onderzoeksgegevens en theorie systematisch worden toegepast, en er niet direct van probleem naar vermeende oplossing wordt gesprongen. Het leidt tot een goede beschrijving van de interventie, welke theorie van gedrag is gebruikt, hoe dit is verwerkt in de interventie, en hoe de interventie vervolgens is uitgevoerd. Het vergroot de kans op de ontwikkeling van interventies die effectief zijn en waarvan de mogelijke werkzame elementen bekend zijn.

Het vaststellen van de effectiviteit van een interventie kan het meest grondig worden aangepakt met een onderzoeksontwerp, genoemd *randomised controlled trial* (Barends et al., 2014), waarbij gebruik wordt gemaakt van een controlegroep en een experimentele groep, met *random* toewijzing van deelnemers, en voor- en nametingen. De experimentele groep krijgt de interventie wel aangeboden en de

controlegroep niet. Door te kijken naar verschillen tussen de voor- en nameting kan worden aangetoond dat een interventie echt effectief is. In de praktijk is een RCT niet altijd mogelijk of zelfs ethisch onwenselijk. In afgezwakte vorm worden bijvoorbeeld de controlegroep en/of de voormeting weggelaten.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe effectief zijn bestaande interventies gericht op cyberweerbaarheid? Wat zijn (per doelgroep/delict-combinaties) effectieve bestanddelen in interventies gericht op cyberweerbaarheid? Welke factoren dragen bij aan de langdurige effectiviteit van interventies? Wat weerhoudt partijen van het gebruik van gedegen methodieken voor de ontwikkeling van interventies, en hoe kunnen deze belemmeringen worden weggenomen? Wat is in de context van cyberweerbaarheid een acceptabele methode om de effectiviteit van een interventie vast te stellen? Op welke wijze kunnen we betrouwbare gedragsgegevens over daadwerkelijk veilig online gedrag en beschermende maatregelen genereren, naast of in plaats van gerapporteerd gedrag, waarbij ethiek en veiligheid worden gewaarborgd? Welke belemmeringen ervaren organisaties om interventies op effect te evalueren? Welke oplossingen kunnen hiervoor worden aangedragen? En hoe kan ervoor worden gezorgd dat effectmetingen van verschillende interventies tot vergelijkbaarheid leiden?

3.5 LEREND VERMOGEN VAN ORGANISATIES

(On)veilig gedrag speelt ook op het niveau van organisaties. Wanneer organisaties slachtoffer worden van een cyberincident, krijgen ze te maken met financiële gevolgen, dataverlies en mogelijke reputatieschade. Verschillende barrières weerhouden organisaties ervan om hun cyberweerbaarheid te verbeteren. Sommige ondernemers en medewerkers geloven niet dat cyberdreigingen een risico voor hen vormen, terwijl anderen de mogelijke impact van deze incidenten

onderschatten, niet weten welke stappen ze kunnen nemen om zich ertegen te beschermen of blind vertrouwen op hun IT-leverancier. Naast een gebrek aan cyberbewustzijn en -kennis onder ondernemers constateert Deloitte (2024) dat ondernemers het moeilijk vinden te bepalen hoeveel en waarin zij moeten investeren. Het aanbod van hulpmiddelen is onoverzichtelijk, onbegrijpelijk, onsamenhangend en sluit vaak niet aan bij de behoefte. Tevens weten veel ondernemers niet aan welke hulpmiddelen ze behoefte hebben.

Naast het cyberbewustzijn en digitaal veilig gedrag van ondernemers en medewerkers heeft ook de context waarbinnen dit gedrag plaatsvindt invloed op de cyberweerbaarheid van organisaties. Er spelen verschillende krachten binnen organisaties die het realiseren van digitaal veilig gedrag vergemakkelijken of bemoeilijken. Hierbij gaat het naast het verdelen van verantwoordelijkheden, het verkennen van de risico's voor de eigen organisatie en het nemen van technische, organisatorische en gedragsmatige maatregelen ook om het als organisatie leren de cyberweerbaarheid (continu) te verbeteren. Het goede nieuws is dat door het nemen van beschermende maatregelen veel incidenten kunnen worden voorkomen of een verminderde impact kunnen hebben (Hof et al., 2024). Zo kent het Digital Trust Center (DTC) de vijf basisprincipes voor veilig digitaal ondernemen die ondernemers kunnen toepassen om hun cyberweerbaarheid te vergroten, bijvoorbeeld het in kaart brengen van risico's en het beschermen van systemen, apparaten en applicaties (Digital Trust Center, z.d.).

Een andere belangrijke strategie om cyberweerbaarheid te vergroten is het leren van cyberincidenten, bijvoorbeeld door het vergroten van risicobewustzijn, het implementeren van maatregelen en het verbeteren van veerkracht (Patterson et al., 2023; Verweijen, 2022). Er is relatief weinig onderzoek gedaan naar hoe organisaties leren van cyberincidenten (Patterson et al., 2023). Zo is weinig bekend over de verschillende strategieën die organisaties kunnen toepassen om te leren. Incidentonderzoeken worden vaak ad hoc uitgevoerd en geven geen diepgaande analyse van achterliggende

oorzaken (Ahmad et al., 2012, 2015). Onderzoek laat tevens zien dat er weinig integratie is van verschillende perspectieven en inzichten in het leren van incidenten, waardoor incidenten relatief eenzijdig geïnterpreteerd worden (Ahmad et al., 2015). Verweijen (2022) laat zien dat incidentonderzoeken vaak één van de volgende drie verschillende kennisperspectieven toepassen: een technisch informatiebeveiligingsperspectief, een IT-managementperspectief en een crisismanagementperspectief. Deze perspectieven worden echter zelden gecombineerd. Dit bevestigt conclusies uit eerder onderzoek dat er een kloof bestaat tussen verschillende vakgebieden en afdelingen in organisaties (Sadok et al., 2020). Het huidige onderzoek geeft dus weinig bewijs voor volwaardig en breed organisatorisch leren van incidenten (Patterson et al., 2023).

Het incident-meldgedrag is cruciaal voor bedrijven om meer cyberweerbaar te worden (Patterson et al., 2024), omdat interne incidenten doorgaans fungeren als een wake-upcall voor organisaties, waarbij zwaktes in de beveiliging worden belicht en een kans wordt geboden om te leren en veerkracht te verbeteren. Door te leren van incidenten kunnen organisaties hun verdediging versterken en zich beschermen tegen toekomstige bedreigingen. Het ontvangen van securitymeldingen door medewerkers biedt de organisatie veel kansen op verbetering, maar uit de praktijk blijkt dat medewerkers incidenten niet of niet altijd melden (Briggs et al., 2017).

Volgens Verweijen (2022) kunnen organisaties hun cyberweerbaarheid ook vergroten door te leren van de ervaringen van andere organisaties die slachtoffer zijn geworden van cyberincidenten. Het voordeel van dergelijk *vicarious learning* is dat organisaties niet gebukt gaan onder de negatieve impact van een incident, maar wel lessen kunnen trekken van andere organisaties om hun eigen cyberweerbaarheid te verbeteren. De voorwaarde voor *vicarious learning* is dat slachtoffers hun geleerde lessen over de oorzaken en gevolgen van een cyberincident inzichtelijk maken. Sommige organisaties doen dit door hun evaluatierapporten openbaar te publiceren. Daarnaast wisselen ook diverse sectorale

samenwerkingsverbanden hun geleerde lessen uit. Hollnagel (2011) identificeert vier noodzakelijke vermogens voor organisatorische weerbaarheid: (I) het kunnen anticiperen op toekomstige verstoringen; (II) het monitoren van prestaties en potentiële verstoringen; (III) het adequaat kunnen reageren op verstoringen; en ten slotte (IV) het leren van ervaringen.

Patterson et al. (2023) en Ebert et al. (2023) benadrukken de invloed van culturele factoren om het leren van cyberincidenten te bevorderen, zoals 'het hebben van een open cultuur' of de aanwezigheid van transparantie. Een tweede aspect dat naar voren komt, is de integratie van technische en socioculturele factoren bij het leren van cyberincidenten. Ebert et al. (2023) en Patterson et al. (2023) pleiten voor een geïntegreerde aanpak die zowel technische als socioculturele aspecten behelst om zo een alomvattend begrip van cyberincidenten te bevorderen.

> De volgende onderzoeksvragen zijn relevant: Hoe kunnen organisaties leren van incidenten in de eigen organisatie? Welke rol speelt veiligheidscultuur, ervaring met safety-procedures en volwassenheidsniveau daarin? Hoe kunnen organisaties leren van incidenten van andere organisaties? Hoe worden (*vicarious*) geleerde lessen in organisaties geïmplementeerd in de bredere organisatie om organisatorisch leren te bewerkstelligen? Welke voorwaarden en praktijken zijn noodzakelijk voor het (*vicarious*) organisatorisch leren van cyberincidenten?

3.6 MENSGERICHTE CYBERWEERBAARHEID

Naast een verbreding van de klassieke oriëntatie op informatietechnologie naar een interdisciplinaire benadering, is het van belang om een extra stap te zetten: de focus moet rondom cyberweerbaarheid niet alleen liggen op het voorkomen van incidenten en fouten, maar er moet tevens aandacht worden besteed aan wat er goed gaat in het dagelijks werk om ook daarvan te kunnen leren (Zimmermann

& Renaud, 2019; Pollini et al., 2022; Ebert et al., 2023; Kaur et al., 2021; Morgen et al., 2020). Daarmee verschilt mensgerichte cyberweerbaarheid fundamenteel van de klassieke cybersecuritybenadering (Spithoven et al., 2024, Tabel 1).

Tabel 1. Verschillen tussen de benaderingen van mens-als-probleem en mens-als-oplossing (o.b.v. Zimmermann & Renaud, 2019)

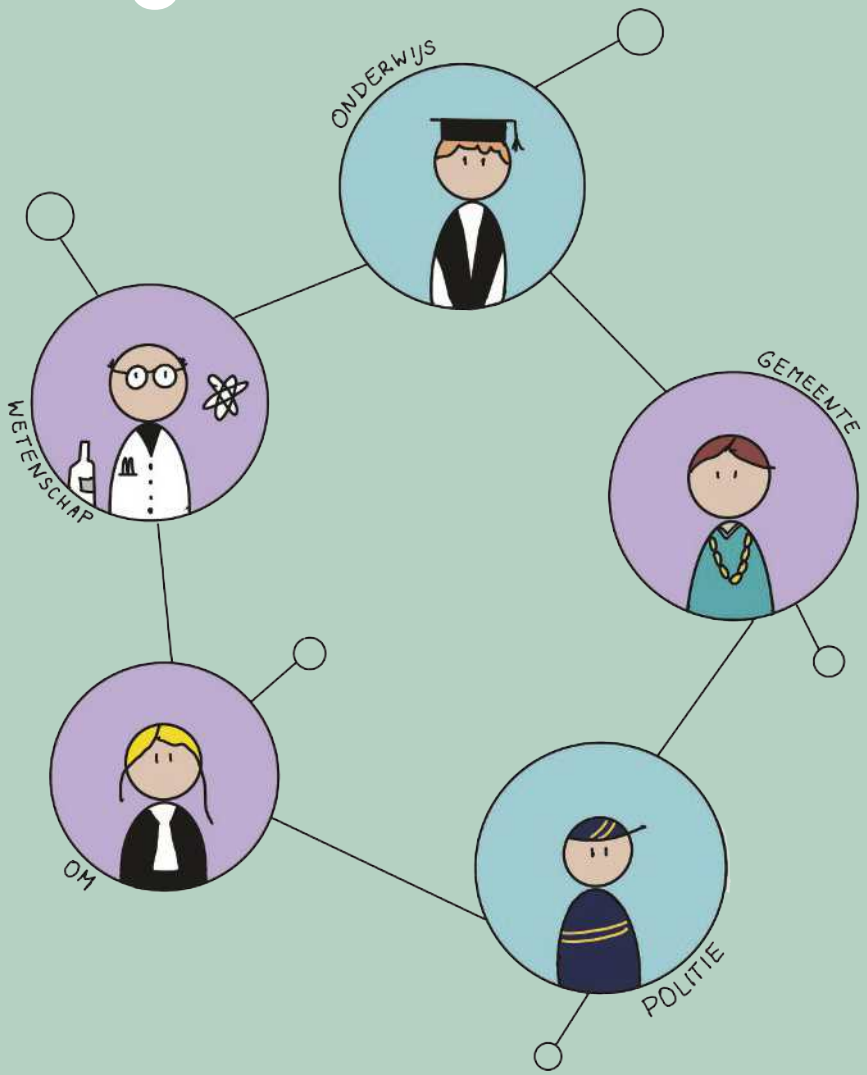
Mens-als-probleem	**Mens-als-oplossing**
Aard: statisch, technisch	*Aard*: dynamisch, interdisciplinair
Doel: zo weinig mogelijk mis laten gaan	*Doel*: zo veel mogelijk goed laten gaan
Probleem: mensen maken fouten	*Probleem*: complexiteit van de omgeving
Principe: reactief, begrenzen	*Principe*: proactief, voeden
Focus: begrijpen wat er mis is gegaan	*Focus*: begrijpen waarom er veel goed gaat
Mensbeeld: mensen maken fouten	*Mensbeeld*: mensen zijn flexibel en leren veel
Rol van de mens: potentieel schadelijk	*Rol van mens*: cruciaal in weerbaarheid
Context: incidenten en ongelukken (< 1%)	*Context*: dagelijks werk en leven (> 99%)

Op deze wijze moet mensgerichte cyberweerbaarheid vooral worden gezien als een *toevoeging* op het klassieke fundament van cybersecurity en niet als een vervanging daarvan. Het blijft immers noodzakelijk om incidenten te voorkomen, daarvan te leren en waar mogelijk de cyberweerbaarheid met technische maatregelen te versterken. Cruciaal daarbij, vanuit het perspectief van de positieve psychologie, is de menselijke bijdrage aan weerbaarheid (proactie en preventie) en veerkracht (repressie en herstel). Hierbij gaat het niet alleen om individueel gedrag, maar ook om individuen die samenwerken en de interactie tussen de mens en technologie in organisatieprocessen.

> Bij deze benadering kan toekomstig onderzoek zich richten op vragen als: Hoe kunnen (netwerken van) organisaties, naast de klassieke focus op de preventie en repressie van incidenten, *ook* leren van wat er goed gaat in het dagelijks werk rond cyberweerbaarheid en wat levert dat op? Hoe kan een multidisciplinaire benadering de cyberweerbaarheid van organisaties versterken? Hoe kunnen menselijke eigenschappen bijdragen aan

het versterken van cyberweerbaarheid? Hoe kunnen organisaties een positieve cultuur en effectieve communicatie bevorderen rondom weerbaar gedrag, leren en innoveren om de cyberweerbaarheid te versterken?

4



VERSTERKINGS-MAATREGELEN VOOR CYBER-WEERBAARHEID: DE PUBLIEKE KANT

Jurjen Jansen, Willem Bantema, Luuk Bekkers, Robin van Halderen, Renske Korenromp, Asier Moneva, Remco Spithoven, Wouter Stol, Renze Tjoelker, Thijs van Valkengoed, Saskia Westers

4.1 PUBLIEK-PRIVATE SAMENWERKING EN KETENS

De overheid zet in op meer publiek-private samenwerkingen in het kader van de brede bestrijding van online criminaliteit (Veiligheidsagenda, 2023). Er bestaan verschillende publiek-private samenwerkingen op dit gebied. Staats en collega's (2021) hebben een literatuuronderzoek gedaan naar succesfactoren en knelpunten bij verschillende publiek-private samenwerkingen in financiële criminaliteit en online criminaliteit, zoals het LMIO, Hack_Right, ECTF en NoMoreDDoS. Uit hun onderzoek blijkt dat er vaak weinig bekend is over de effectiviteit van publiek-private samenwerkingen, omdat er vooral plan- en procesevaluaties en slechts één effectevaluatie zijn uitgevoerd. De effectevaluatie ging over een publiek-private samenwerking bij de Fraudehelpdesk (Staats et al., 2021).

Een voorbeeld van een recent geëvalueerde publiek-private samenwerking is Project Melissa. Dit samenwerkingsverband is gericht op ransomewarebestrijding met als aangesloten partijen de Politie, het Openbaar Ministerie, NCSC, Cyberveilig Nederland en private cybersecurity bedrijven (Brandt, 2024; Van der Berg et al., 2024). Binnen het samenwerkingsverband wordt gezamenlijk operationele en technische informatie uitgewisseld en geanalyseerd om zo in het gefragmenteerde landschap tot een beter overzicht te komen (Brandt, 2024). Een evaluatie heeft de volgende onderliggende succesfactoren van Project Melissa geïdentificeerd: de wederkerigheid van expertise, de gedeelde motivatie, de vertrouwensband, aanjagende sleutelfiguren en een heldere scope. Daarnaast is een aantal risicofactoren aangekaart, namelijk de vrijwillige investeringen, spanningen bij het delen van (gevoelige) informatie, het wegvallen van sleutelfiguren en het stroef werkend informatiedelingssysteem (Van der Berg et al., 2024).

Er liggen kansen voor samenwerkingsverbanden in de lokale aanpak en integrale benadering van online criminaliteit, en op het gebied van alternatieve interventies (Spithoven & Leukfeldt, 2023; Veenstra, 2023). Online criminaliteit is namelijk lokaal verankerd en sterk verweven met traditionele criminaliteit. In de praktijk zijn echter geen of nauwelijks voorbeelden bekend van een lokale integrale casusaanpak in relatie tot online criminaliteit. In Noord-Nederland is daar in RIEC-verband (Regionale Informatie- en Expertisecentra), ervaring mee opgedaan. Gemeenten, politie, de Belastingdienst en de Arbeidsinspectie hebben verschillende interventies ingezet. Door samen te werken wordt het interventiepotentieel vergroot, want partners kunnen hun volledige interventierepertoire aanwenden. Via het RIEC-samenwerkingsverband kan invulling worden gegeven aan de lokale en integrale aanpak van ‘cyber’criminele netwerken (Veenstra, 2023). Daarom wordt geadviseerd om onderzoek te doen naar duurzame (lokale) samenwerkingsverbanden tussen publieke en private partijen om de brede bestrijding van online criminaliteit in te zetten en deze tevens te evalueren op effectiviteit. Verder wordt geadviseerd om

de randvoorwaarden voor een brede bestrijding van online criminaliteit in kaart te brengen en specifiek de juridische grondslag van verschillende alternatieve interventies.

Hoewel cyberweerbaarheid en online criminaliteit zijn geprioriteerd in strategie en beleid (bijv. Ministerie van Veiligheid & Justitie, 2022), zijn er nog belangrijke stappen te zetten. Vooral op lokaal niveau heerst een gebrek aan kennis, motivatie en prioriteit om actief aan de slag te gaan met cyberweerbaarheid (Bekkers et al., 2024b; Ruiter et al., 2023; Schiks et al., 2022). Dit zit samenwerking in de weg. Ook in de opsporing is publiek-publieke samenwerking en publiek-private samenwerking nodig, maar betrokken professionals ervaren hierbij verschillende barrières. Informatiedeling verloopt stroperig, centrale coördinatie ontbreekt, heersende wet- en regelgeving is mogelijk niet toereikend, en private bedrijven zijn vanwege andere belangen niet altijd responsief (Bekkers et al., 2024b; Brown, 2015; De Paoli et al., 2021; Schiks et al., 2022; Van den Eeden et al., 2021). Wat hierbij een belangrijke rol speelt, is dat nog weinig bekend is over het effect van initiatieven op het gebied van cyberweerbaarheid door een gebrek aan nulmetingen en effectevaluaties (bijv. Bekkers et al., 2021; Bluhm et al., 2024; Schiks et al., 2022). We gaan daar in paragraaf 3.4 verder op in.

Daarnaast zien we een tendens van verschillende initiatieven die naast elkaar lopen, in plaats van dat krachten worden gebundeld en met elkaar wordt samengewerkt. Ook is het van belang om zicht te krijgen op welke partijen een rol vervullen in de politiefunctie en hoe daar effectief mee kan worden samengewerkt (Stol et al., 2024). Met de toenemende digitalisering van de samenleving spelen organisaties die grote hoeveelheden gegevens over mensen hebben een belangrijke rol. Publiek-private samenwerkingen in de strijd tegen online criminaliteit kunnen effectief zijn, maar roepen ook vragen op. Het proactief verstrekken van grote datasets door private partijen om online criminaliteit op te sporen, bijvoorbeeld door *super controllers* aan de politie (of andere wetshandhavingsinstanties), roept vragen op over privacy en gegevensbescherming. De publiek-private samenwerking

tussen wetshandhavingsinstanties en *super controllers* kan invloed hebben op de fundamentele rechten van burgers, en moet dus zorgvuldig worden afgewogen (Europese Raad & Raad van de Europese Unie, 2024).

Ook binnen de toeleveringsketen is samenwerking essentieel. Bedrijven maken tegenwoordig deel uit van een keten, en worden daarbij steeds afhankelijker van ICT voor bijvoorbeeld het aankopen, bezorgen en inventariseren van producten of diensten. Dit brengt risico's met zich mee, zoals stepping-stone aanvallen, die enkel kunnen worden ingedekt door een samenwerking tussen de betrokken stakeholders, zowel publiek als privaat (Van Ruijven & Keijser, 2017). Er is echter nog weinig bekend over het concept van cyber-ketenweerbaarheid buiten formele informatiedeling-initiatieven, over hoe cyberweerbaarheid en risico's samenhangen tussen verschillende sectoren, en hoe risico's en afhankelijkheden in de toeleveringsketen inzichtelijk kunnen worden gemaakt (Bekkers et al., 2020, 2021; NCSC, 2022).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: In hoeverre en op welke manier is er sprake van een ketenaanpak tussen verschillende instanties binnen de gemeente, tussen verschillende lokale en regionale overheden in Nederland, en met internationale partijen op het gebied van cyberweerbaarheid? Wat zijn voorbeelden van een succesvolle ketenaanpak van cyberweerbaarheid, wat zijn succesfactoren en geleerde lessen daarbij, en wat zijn de effecten van dergelijke initiatieven? Wat zijn veelvoorkomende barrières bij publiek-private samenwerking en hoe kunnen deze worden opgelost? Wie zijn belangrijke publieke en private ketenpartners in de opsporing van daders van online criminaliteit, wat zijn hun taken en bevoegdheden, en hoe kunnen we samenwerking tussen die partijen beter organiseren? Hoe is het gesteld met cyberweerbaarheid in de toeleveringsketen buiten formele informatiedeling-initiatieven en hoe kunnen we risico's en afhankelijkheden in de toeleveringsketen inzichtelijk maken? Hoe bewerkstelligen we een toekomstbestendige ketenaanpak met partijen die

beschikken over continue up-to-date kennis en vaardigheden? En welke organisatorische en juridische randvoorwaarden zijn noodzakelijk voor een effectieve ketenaanpak?

4.2 BREDE BESTRIJDING

Voor een effectieve aanpak van online criminaliteit is brede bestrijding noodzakelijk. Brede bestrijding is het opsporen, vervolgen, tegenhouden van daders, het beperken van schade en het beschermen van slachtoffers (Bonnes & Divendal, 2024). De overheid benadrukt dat online criminaliteit bestreden moet worden in een netwerk van publieke en private organisaties waar informatie verzameld, geanalyseerd en met afnemers gedeeld wordt (NCTV, 2022).

Een goede informatiepositie is een randvoorwaarde voor de aanpak van online criminaliteit (Ministerie van Justitie en Veiligheid, 2022). De informatiepositie is bijvoorbeeld belangrijk voor het doen van fenomeenonderzoeken die zijn gericht op brede bestrijding van eenheid overstijgende, criminele fenomenen of dadergroepen. Het NCTV (2023) houdt de ontwikkelingen op hoofdlijnen bij en ook private partijen spelen een rol, bijvoorbeeld met analyses aangaande sexting (Van Wijngaarden, 2024). De politie volgt ontwikkelingen op basis van meldingen en aangiften, bijvoorbeeld inzake internetoplichting (Inspectie Veiligheid en Justitie, 2015). Echter, minder dan de helft van de online criminaliteitsvormen die het Centraal Bureau voor de Statistiek (CBS) bekijkt, wordt bij de politie gemeld of aangegeven (Akkermans et al., 2024). Dan zijn er nog online criminaliteitsvormen die het CBS niet in beeld brengt, zoals de handel in afbeeldingen van seksueel kindermisbruik en wapenhandel.

De strafrechtelijke aanpak van online criminaliteit is gericht op vervolging en berechting, wat begint bij opsporing door de politie. Waar preventie zich richt op de toekomst en opsporing op het in kaart brengen van het verleden, richt verstoring of situationele criminaliteitspreventie (SCP) zich primair op het heden (Kirby & Snow, 2017). Verstoring is

het hinderen van het proces van online criminaliteit (Van de Sandt, 2019). SCP is een praktische manier om specifieke misdaadkansen te verminderen door misdaadsituaties te veranderen (Clarke, 1980, 2017). Het stelt 25 technieken voor om de kans op criminaliteit te verkleinen door het risico voor daders te vergroten, de inspanning die nodig is om te overtreden te verhogen, de beloningen van criminaliteit te verminderen, de provocaties die criminaliteit kunnen triggeren te verminderen en excuses voor niet-naleving te elimineren (Cornish & Clarke, 2003). SCP-technieken zijn offline en online gebruikt om misdaadkansen te verminderen (zie Brewer et al., 2019; Guerette & Bowers, 2009; Ho et al., 2022). Er wordt echter betoogd dat niet alle technieken zinvol zijn in online situaties, aangezien de online omgeving unieke kenmerken heeft en niet gebonden is aan geografische beperkingen (Newman & Clarke, 2003). Veel cybersecuritymaatregelen die de cyberweerbaarheid van organisaties verbeteren (bijv. ISO/IEC 27002-beveiligingscontroles, NIST-beveiligingscontroles, Mitre Att&ck Mitigations) en sommige zelfbeschermingsmaatregelen die de cyberweerbaarheid van individuen verbeteren (bijv. antivirusbescherming, firewalls, sterke wachtwoorden) kunnen als SCP-technieken worden beschouwd.

Een ander belangrijk hiaat op dit gebied is dat veel van het werk over de toepassing van SCP op online criminaliteit theoretisch van aard is (Hartel et al., 2010; Willison & Siponen, 2009), en dat het bestaande empirische werk schaars is. Dit betekent dat er weinig bewijs is over welke SCP-technieken effectief zijn voor welke soorten online criminaliteit (Brewer et al., 2019; Hartel et al., 2010; Ho et al., 2022). Het werkveld heeft baat bij het uitvoeren van empirische studies die de effectiviteit van SCP-technieken grondig evalueren. Experimenteel onderzoek helpt bepalen welke technieken werken om de cyberweerbaarheid te vergroten en welke niet.

Brede bestrijding van online criminaliteit kent aanzienlijke juridische obstakels, vooral met betrekking tot opsporingsbevoegdheden en gegevensuitwisseling. Er is geen wettelijke grondslag voor opsporingsbevoegdheden ten behoeve van verstoring, wat betekent dat alternatieve interventies

vaak afhankelijk zijn van lopende opsporingsonderzoeken (Ministerie van Justitie en Veiligheid, 2022; Bonnes & Divendal, 2024). Dit kan de schaal en effectiviteit van deze interventies beperken. Aanvullend is de rol van de rechter-commissaris (RC) in ontwikkeling (Bonnes & Divendal, 2024). De RC is toezichthouder in een opsporingsonderzoek, maar wordt steeds vaker om een machtiging gevraagd bij het verkrijgen van digitale gegevens, waarbij de RC meer gaat sturen op inhoudelijk onderzoek. Bonnes en Divendal (2024) pleiten voor een wettelijke verankering van brede bestrijding.

Daarnaast zijn er uitdagingen met betrekking tot gegevensuitwisseling, zowel binnen publieke organisaties als tussen publieke en private partners, vanwege regelgeving zoals de Wpg, AVG, Wbni en Wbp (Van den Eeden, 2021). Deze beperking in informatie-uitwisseling is één van de knelpunten voor een effectieve publiek-private samenwerking om online criminaliteit tegen te gaan (Staats et al., 2021). Op dit moment deelt de politie op innovatieve wijze versleutelde gegevens om online misbruik van inloggegevens tegen te gaan en te voldoen aan wet- en regelgeving. Met het project 'No More Leaks' verstrekt de politie inloggegevens 'gehasht' aan partijen met veel online accounthouders, zodat zij hun gebruikers kunnen waarschuwen (Politie, z.d.). Dit is een innovatieve manier om online criminaliteit te verstoren en te voldoen aan de wet- en regelgeving.

Kop (2012) verwijst naar een meerzijdige aanpak 'van opsporing naar criminaliteitsbeheersing'. Gezien de mogelijkheden, het gedeelde belang en het eigenaarschap die burgers en vooral particuliere organisaties hebben om bij te dragen aan cybercrimebeheersing (Passchier, 2021; Stol et al., 2024), ligt publiek-private samenwerking voor de hand, zoals met Internet Service Providers (ISP) (Stol et al., 2007), de bancaire sector (Jansen, 2018) of zelfs 'big tech'. In elke situatie dient wel de balans tussen rechtshandhaving en rechtsbescherming te worden bewaakt. Kortom, het speelveld wordt langs twee wegen veelvormiger; meer strategieën dan enkel opsporing en meer partijen met belangrijke informatieposities of beïnvloedingsmogelijkheden. De vraag is welke strategieën en

samenwerkingen effectief zijn bij welke vormen van online criminaliteit, én welke ethische, juridische en zelfs machtspolitieke kwesties (Passchier, 2021) daarbij een rol spelen.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Welke interventies (wat, door wie, hoe) ter bestrijding van online criminaliteit zijn er en welk effect hebben ze? Welke ethische, juridische en machtspolitieke kwesties spelen daarbij een rol? Wat zijn de belangrijkste knelpunten in het strafrechtssysteem aangaande online criminaliteit en hoe kunnen deze worden opgelost? Welke conceptuele basis voor situationele misdaadpreventie wordt gedeeld door de verschillende wetenschappelijke disciplines die streven naar het verminderen van kansen voor online criminaliteit? Hoe kunnen we deze gedeelde conceptuele basis synthetiseren tot een gemeenschappelijk raamwerk? En wat werkt effectief in situationele online criminaliteitspreventie? Onder welke (juridische) voorwaarden kunnen strafvorderlijke bevoegdheden worden ingezet voor de brede bestrijding (alternatieve interventies) van online criminaliteit? En op welke wijze kan brede bestrijding van online criminaliteit (beter) gereguleerd worden?

4.3 HET ONTWIKKELEN EN EVALUEREN VAN ALTERNATIEVE INTERVENTIES

In de Veiligheidsagenda 2023-2026 stelt het ministerie van Justitie en Veiligheid (2022) nationale beleidsdoelstellingen vast voor de politie en het Openbaar Ministerie, die onder andere het aantal verdachten en onderzoeken specificeren op het gebied van online criminaliteit. De minister heeft als doel gesteld om ook alternatieve interventies in te zetten, waarvan 25% bij zaken met verdachten en 50% bij fenomeenonderzoeken. Alternatieve interventies zijn maatregelen die naast of in plaats van strafrechtelijke vervolging worden ingezet. Dit omvat onder andere preventie, verstoring, schadebeperking en notificatie van slachtoffers (Van den Eeden et al., 2021). Voorbeelden van dergelijke alternatieve

interventies zijn het ontoegankelijk maken van frauduleuze socialmedia-accounts of webshops, het verstoren van criminele verdienmodellen met private partners (zie par. 4.4), het weerbaarder maken van jongeren (De Groot et al., 2022; Spithoven & Van Tuijl, 2024) en het blokkeren middels een blacklist (Jansen et al., 2019; Stol et al., 2009).

Specifieke alternatieve interventies die door de politie in Nederland worden ingezet, zijn advertenties op social media, Re_B00tCMP, Cease & Desist, Hack_Right en Operation Amplification. Het evalueren van bestaande alternatieve interventies is van groot belang. Er zijn verschillende evaluatiestudies afgerond (Andriessen et al., 2024; Schiks et al., 2021a, 2021b). Aanvullende plan-, proces- en effectevaluaties van alternatieve interventies zijn essentieel in de brede bestrijding van online criminaliteit.

Naast het evalueren van bestaande interventies is het aldus van belang om aanvullende alternatieve interventies te ontwikkelen. Uit het Cybercrimebeeld Nederland 2024 blijkt dat een zorgwekkend aandeel cybercrimeverdachten jonger dan 25 jaar is (Openbaar Ministerie & Politie, 2024). Eerder is geconcludeerd dat er 'witte vlekken' zijn in het interventielandschap van jeugd en online criminaliteit (CCV, 2023). In andere woorden, er zijn aandachtsgebieden waar nog onvoldoende interventies voor ontwikkeld zijn. Het CCV maakt onderscheid tussen preventie op verschillende niveaus en gericht op verschillende doelgroepen. Daarnaast wordt er onderscheid gemaakt in primaire (gericht op de brede populatie), secundaire (gericht op risicogroepen) en tertiaire (gericht op het voorkomen van recidive) preventie. Daarnaast wordt onderscheid gemaakt tussen dadergerichte, slachtoffergerichte en situationele preventie, waarbij vooral de laatste categorie weinig vertegenwoordigd is. Op basis van deze indeling zijn zes witte vlekken naar voren gekomen in het interventielandschap. Een voorbeeld van een witte vlek is het ontbreken van een primaire interventie gericht op ouders van slachtoffers en daders (CCV, 2023).

> Het advies is om onderzoek te doen naar alternatieve interventies op het gebied van deze witte vlekken aan de hand van de volgende onderzoeksvragen: Hoe kunnen bestaande interventies worden aangepast om vervolgens te worden ingezet op de witte vlekken in het interventielandschap? Welke andere alternatieve interventies kunnen een bijdrage leveren aan de brede bestrijding van online criminaliteit? Welke situationele preventie-interventies (bijv. technische maatregelen zoals twee-factor-authenticatie) zijn mogelijk om online criminaliteit te verstoren? Welke primaire interventies kunnen gericht worden op ouders van slachtoffers en van daders van online criminaliteit? Welke secundaire interventies zijn geschikt voor kwetsbare daders, slachtoffers en opportunistische daders van online criminaliteit? En welke tertiaire interventies kunnen recidive en herhaald slachtofferschap van online criminaliteit voorkomen?

4.4 GEMEENTELIJKE ROLLEN BIJ DE AANPAK VAN CYBERCRIME EN DIGITALE VEILIGHEID

De 'Agenda Digitale Veiligheid 2020-2024' van de Vereniging van Nederlandse Gemeenten (VNG, 2020) noemt drie gemeentelijke taakgebieden op het gebied van cyberweerbaarheid en digitale veiligheid: (1) informatiebeveiliging (eigen huis op orde), (2) digitale incidenten en crises en (3) digitale criminaliteit. Inmiddels wordt zichtbaar dat steeds meer gemeenten aan de slag gaan met het vergroten van bewustzijn onder inwoners en bedrijven binnen de gemeente om slachtofferschap van online criminaliteit te voorkomen en daarin een regierol innemen.

Onderzoek van Twickler en collega's (2024) bespreekt een mogelijke rol voor de gemeente die verder gaat dan alleen de regierol en daarnaast een aanvullend instrumentarium kan bieden om bedrijven, indien nodig, te dwingen hun digitale veiligheid te vergroten. Het gaat nog weinig over de inzet van bestuursrechtelijke bevoegdheden zoals bij de aanpak van online aangejaagde ordeverstoringen (zie hierna). Ervan uitgaande dat online criminaliteit kan leiden

tot openbare-ordeverstoringen biedt deze route mogelijkheden voor nader onderzoek. Een voorbeeld van de impact van online criminaliteit op de openbare veiligheid betreft de casus van het Looijkartel in Hilversum ('Wie schiet deze lelijkerd', 2023). Een aanknopingspunt kan gevonden worden in de bestuursrechtelijke aanpak van kinderporno (Steur et al., 2019). Bestuursdwang kan een effectieve aanvulling zijn op bestaande strafrechtelijke maatregelen en zelfregulering door specifiek partijen aan te pakken die niet adequaat reageren op verwijderverzoeken. Bestuursdwang beperkt zich tot partijen die binnen het Nederlands grondgebied opereren. Ook zijn er technische belemmeringen, vooral wanneer er gebruik wordt gemaakt van virtuele servers of wanneer servers meerdere klanten of diensten hosten.

Een andere rol die gemeenten spelen, doet zich voor in de aanpak van een zogenaamde cybercrisis (Ebbers et al., 2021). Een cybercrisis is doorgaans een crisis waarvan de oorzaak in de digitale wereld ligt, maar waarvan de ontregeling in de analoge wereld plaatsvindt, bijvoorbeeld wateroverlast en uitval van elektriciteit. Een verkennend onderzoek van Van der Varst en collega's (2022) benadrukt dat burgemeesters en voorzitters van veiligheidsregio's momenteel geen specifieke bevoegdheden hebben om direct in te grijpen bij cyberincidenten, tenzij deze de openbare veiligheid bedreigen. In de praktijk richt de bestuurlijke aanpak zich meer op cyberwaakzaamheid en het beheersen van de gevolgen van cyberincidenten via bestaande openbare-ordebevoegdheden. Een ontregeling kan zich echter ook online manifesteren. Het spannende aan deze gemeentelijke taak is dat het onduidelijk is hoe gemeentelijk optreden eruitziet als de crisis zich volledig online afspeelt en (nog) geen fysieke gevolgen heeft.

Stol en Bantema (2019, 2020) voegden, naast de drie taakgebieden die de VNG (2020) onderscheidt, twee gemeentelijke taakgebieden toe, namelijk de aanpak van online aangejaagde ordeverstoringen en de mogelijkheid voor gemeenten om eisen te stellen aan de digitale veiligheid van vergunningplichtige activiteiten. In verschillende publicaties is aandacht

voor onder andere bestuursrechtelijke mogelijkheden om als burgemeester/gemeente online aangejaagde ordeverstoringen aan te pakken (Bantema & Twickler, 2023; Bantema et al., 2018, 2020, 2022; Buitenhuis, 2022; Vuik & Bantema, 2021). Het stellen van eisen aan digitale veiligheid bij activiteiten waarvoor vergunningen vereist zijn, is een nieuwe experimentele route waar gemeenten mogelijk een rol kunnen spelen en die gaat verder dan de regierol waar bewustzijn centraal staat. De gemeente stelt bij vergunningverlening eisen aan de digitale veiligheid en zorgt voor toezicht op de naleving. Te denken valt aan de digitale veiligheid van evenementen en van andere bedrijfsmatige activiteiten binnen de gemeente. Deze invalshoek is vernieuwend en nog amper onderzocht.

Er blijken juridische mogelijkheden te zijn om lokaal op te treden via bijvoorbeeld de Algemene Plaatselijke Verordening (APV) in het geval van evenementenvergunningen en via de Omgevingswet als het gaat om aantoonbare gevolgen voor de fysieke leefomgeving (Twickler et al., 2024). Lokale regels mogen niet indruisen tegen Europese regels en zo is het afwachten hoe lokale mogelijkheden zich verhouden tot Europese richtlijnen zoals de NIS2. Met name bij de digitale veiligheid van evenementen zijn er nu al veel mogelijkheden om lokaal regels te stellen. Experts bevelen aan om (inter)nationale standaarden te hanteren, bijvoorbeeld de AVG, NIS2 en ISO-normeringen, zodat er geen verschillen ontstaan tussen gemeenten en de daar gevestigde bedrijven.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe is de verantwoordelijkheid en hoe zijn de rollen verdeeld rondom de aanpak van digitale veiligheid van evenementen? Wat zijn mogelijke cyberrisico's van evenementen en wat zijn de concrete gevolgen voor de openbare orde en veiligheid? Hoe verhouden lokale, nationale en Europese regels zich tot elkaar en hoeveel ruimte biedt dit voor lokale bestuurlijke handhaving op dit terrein? Welke bedrijven hebben een groter risico op nadelige effecten voor de fysieke leefomgeving bij digitale onveiligheid en welke evenementen voor de openbare orde en veiligheid? Welke vormen van cybercrime kunnen de openbare

orde raken? Welke bestuursrechtelijke mogelijkheden zijn er voor de aanpak van die specifieke vormen van cybercrime?

4.5 DIGITAAL SAMENLEVEN: BESCHERMEN VAN DE DEMOCRATISCHE RECHTSSTAAT

De hiervoor beschreven thema's publiek-private samenwerking, gemeentelijke rollen bij de aanpak van cybercrime en digitale veiligheid en het ontwikkelen van alternatieve interventies (rondom preventie), hangen samen met de rol die publieke organisaties hebben bij de aanpak van online schadelijke gedragingen die druk zetten op publieke waarden en de democratische rechtsstaat. Illustratief voor deze gedragingen zijn het online discrimineren van etnische of seksuele minderheden, doxing van politici, ambtenaren of journalisten, en het verspreiden van desinformatie over het beleid of de intenties van de overheid. Het zijn gedragingen die geduid kunnen worden als vormen van online informatiemanipulatie, digitaal vigilantisme en online haat (Van Huijstee et al., 2021), en als specifieke uitingen van cybercrime of 'cyberdeviance' (Phillips et al., 2022).

Het betreft gedragingen die potentieel een bedreiging vormen voor de politieke en sociale stabiliteit in Nederland, door bijvoorbeeld het functioneren van het openbaar bestuur te hinderen of aan te zetten tot polarisatie. De ernst is goed zichtbaar in scenario's waarin het online verspreiden van complottheorieën, namenlijsten van politici en instructies over het opzetten van volkstribunalen, resulteert in fysiek geweld tegen politici en vijandelijkheid tussen personen die de acties wel of niet omarmen (Analistennetwerk Nationale Veiligheid, 2023).

Gemeenten, politie en andere publieke organisaties zijn zoekende hoe zij om moeten gaan met de bedoelde online schadelijke gedragingen. Het is een complexe opgave om invulling te geven aan de 'politiefunctie' op dit thema. Het verlangt een genuanceerde en gebalanceerde benadering, waarbij samenwerking beschouwd kan worden als

vertrekpunt. Het is van belang dat gemeenten hun regierol op het gebied van veiligheid en openbare orde vertalen naar de online omgeving. Daarnaast moet beleid rondom digitalisering expliciet aandacht besteden aan menselijk gedrag, naast de neveneffecten van technologie, zoals discriminerende algoritmen. Online monitoring zou geen centrale rol moeten spelen in de aanpak van schadelijk online gedrag. Bovendien moeten het onderwijs, de bibliotheeksector en het maatschappelijk werk bijdragen aan het verbeteren van de vaardigheden van mensen om deel te nemen aan onze digitaliserende samenleving (Van Halderen et al., 2024).

> De (lokale) beroepspraktijk kan worden ondersteund met praktijkgericht onderzoek dat gericht is op vragen als: Hoe ziet het landschap van relevante publieke en private partijen eruit? Welke rollen en verantwoordelijkheden kunnen deze partijen op zich nemen bij de aanpak van online schadelijk gedrag? Welke kennisbehoeften hebben zij? En wat zijn passende interventies? Ten grondslag daaraan ligt een goed begrip van de genoemde online schadelijke gedragingen door het zoeken naar antwoorden op vragen zoals: Wat is de aard en omvang van de problematiek? Welke variabelen dragen bij aan de online schadelijke gedragingen? En in welke mate en op welke wijze werken de online schadelijke gedragingen door in de offline omgeving?

4.6 DIGITALE TRANSFORMATIE EN LEIDERSCHAP

De vierde industriële revolutie, ook wel de digitale revolutie, wordt gedreven door eenvoudiger, sneller en veelvuldiger gebruik van wereldwijde netwerken, kleinere en betere sensoren, machine learning en kunstmatige intelligentie, en dit alles voor beperkte kosten (Schwab, 2017). Hierdoor komt de mogelijkheid om technologie in te zetten overal in de maatschappij voor, ten behoeve van de maatschappij, maar tevens met kwaadwillend oogmerk.

Technologische inzet kan onder andere werkzaamheden effectiever, efficiënter en van hogere kwaliteit laten

plaatsvinden, bijdragen aan kennismanagement en vakontwikkeling, en zorgen voor een vergroting van de intelligencepositie. Nieuwe technologie zorgt echter ook voor nieuwe veiligheidsrisico's, aangezien zij enerzijds inherent kwetsbaarheden zal bezitten en anderzijds zorgen technologische ontwikkelingen voor nieuwe, betere en snellere criminogene mogelijkheden (Wall, 2024).

Nederland hoort bij de internationale koplopers van onder andere de gebieden van digitalisering, technologieadaptatie en digitale vaardigheden. Daarnaast is echter ook duidelijk dat het gebruikersperspectief beperkt wordt meegewogen (Demirel et al., 2023). Kijkend naar de vervanging van traditionele dienstverlening door gedigitaliseerde dienstverlening, is van belang om te beseffen dat één op de vijf Nederlanders digitaal niet kan meekomen (CBS, 2023). Deze groep mensen loopt hierbij extra risico, aangezien zij digitaal moeten laveren in de samenleving, zonder daarbij over de juiste vaardigheden te beschikken.

De overheid, bedrijven en instanties investeren in de digitale vaardigheden van de gebruikers in een poging veiligheidsrisico's te verlagen (Rijksoverheid, 2022). De vraag is of dergelijke programma's wel voldoende effect hebben om de risico's te mitigeren. Onderzoek binnen cybersecurity toont aan dat hier vaak geen sprake van is (Bada et al., 2019). Digitalisering vraagt van de samenleving op alle vlakken leiderschap, een gedegen en gedragen aanpak, waar een duidelijke visie aan ten grondslag ligt. Er is sprake van een groot verschil tussen papieren beleid en de digitale werkelijkheid. De overheid heeft namelijk grote moeite om tijdig en binnen budget ICT-projecten tot wasdom te brengen. Daarnaast is ook sprake van een beperkte inhoudelijke inbreng van het leiderschap (Hartholt, 2023; Kroes et al., 2023).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Welke sleutelfactoren zijn er te benoemen voor een veilige digitale transformatie in de keten en beïnvloedingssfeer van maatschappelijke deelnemers tot en met uiteindelijke rechtspraak? Welke competenties worden er van leiders gevraagd om van

digitale transformatie in de publieke sector en niet-technologisch georiënteerde organisaties een (veilig) succes te maken? Welke technologische ontwikkelingen binnen de digitale transformatie kunnen bijdragen aan veiliger, up-to-date en betrokken vakmanschap? Met welke factoren dient rekening gehouden te worden bij digitalisering in de samenleving en eigen organisatie met betrekking tot veiligheid en vakmanschap? En op welke wijze kan leiderschap bijdragen aan de juiste ethische, morele en privacy-minded digitale transformatie?

4.7 CYBERWEERBAARHEID IN HET ONDERWIJS

De toenemende blootstelling van jongeren aan online criminaliteit in de digitale samenleving vraagt om een gerichte aanpak binnen het onderwijs om hun cyberweerbaarheid te versterken (Livingstone et al., 2011). Ondanks de recente ontwikkeling van nieuwe (concept)kerndoelen (SLO) voor digitale geletterdheid, blijft de aandacht voor online criminaliteit in het primair en voortgezet onderwijs (PO/VO) beperkt (SLO, 2024). Deze kerndoelen bieden kansen voor integratie van onderwerpen zoals online criminaliteit, maar de brede opzet ervan maakt het uitdagend om gerichte en effectieve lessen te ontwikkelen die direct bijdragen aan de versterking van de cyberweerbaarheid van leerlingen (Hollis & Tsaousi, 2018).

Online criminaliteit raakt kinderen (tot twaalf jaar) en jongeren (twaalf tot achttien jaar) in hun dagelijks leven en scholen spelen (naast ouders/verzorgers) een cruciale rol in het voorbereiden van leerlingen op de digitale wereld. Dit omvat niet alleen het leren gebruiken van technologie, maar ook het wapenen tegen de gevaren ervan (International Telecommunication Union, 2020). Het belang van cyberweerbaarheid wordt steeds meer erkend, wat heeft geleid tot de ontwikkeling van educatieve initiatieven zoals HackShield, Mijn Cyberrijbewijs en De Kiesraad (Willemse, 2021). Deze programma's bieden waardevolle lesmaterialen en tools om

leerlingen bewust te maken van digitale dreigingen en hen te leren hoe zij zichzelf kunnen beschermen.

Het is essentieel dat docenten beter voorbereid worden om cyberweerbaarheid te integreren in hun curriculum. Huidige lespakketten zoals HackShield en Mijn Cyberrijbewijs worden onvoldoende benut door scholen, ondanks hun beschikbaarheid (Willemse, 2021). Dit roept vragen op over de belemmeringen die scholen en docenten ervaren bij het gebruik van deze middelen. De belemmeringen kunnen variëren van gebrek aan kennis en vaardigheden over online criminaliteit tot organisatorische en tijdsgebonden obstakels bij het integreren van deze onderwerpen in hun lespraktijk (Tsaousi et al., 2022).

Om de cyberweerbaarheid van leerlingen effectief te vergroten, is het van belang om de kennis en vaardigheden van docenten te versterken. Dit kan door middel van gerichte professionalisering en ondersteuning bij het gebruik van bestaande lesprogramma's (Tsaousi et al., 2022). Scholen moeten zich niet alleen richten op het aanleren van technologie, maar ook op het ontwikkelen van vaardigheden om cyberdreigingen te herkennen en ermee om te gaan (International Telecommunication Union, 2020).

Er is behoefte aan een duidelijke visie en beleid rond digitale geletterdheid en cyberweerbaarheid binnen scholen. Door samenwerking tussen schoolbesturen en docenten kan er een integrale aanpak worden ontwikkeld die gericht is op het structureel borgen van online criminaliteit in de curricula (SLO, 2024). Deze aanpak moet afgestemd zijn op de nieuwe (concept)kerndoelen voor digitale geletterdheid om ervoor te zorgen dat er jaarlijks aandacht aan wordt besteed (Hollis & Tsaousi, 2018).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Welke obstakels ervaren docenten bij de implementatie van cyberweerbaarheid in hun onderwijs? Hoe kan de samenwerking tussen scholen, beleidsmakers en ontwikkelaars van lesprogramma's worden versterkt? Wat zijn effectieve strategieën om de betrokkenheid van leerlingen bij cyberweerbaarheid te

vergroten? Aan welke standaardeisen, rekening houdend met type onderwijs en niveau, zouden lesprogramma's moeten voldoen? En hoe kunnen bestaande lesprogramma's beter worden benut om een cultuur van digitale veiligheid binnen scholen te bevorderen?

4.8 CYBERWEERBAARHEID VAN MENSEN MET EEN LICHT VERSTANDELIJKE BEPERKING (LVB)

Onderzoek naar de cyberweerbaarheid van specifieke groepen zoals laaggeletterden, vluchtelingen en mensen met een licht verstandelijke beperking (LVB) is van groot belang vanwege hun verhoogde kwetsbaarheid in de digitale wereld. Binnen Cyberweerbaar NL wordt er met name onderzoek gedaan naar de cyberweerbaarheid van mensen met een LVB. Deze groep loopt zowel het risico slachtoffer te worden van online criminaliteit als te worden geronseld door criminelen voor illegale activiteiten (Landelijk Kenniscentrum LVB, z.d.).

Mensen met een LVB hebben vaak moeite met het begrijpen van complexe digitale omgevingen en herkennen daardoor minder snel cyberdreigingen zoals phishing, online fraude of manipulatieve berichten. Hierdoor kunnen ze gemakkelijk worden misleid en slachtoffer worden van bijvoorbeeld identiteitsdiefstal of andere vormen van uitbuiting, wat grote financiële, juridische, psychische en emotionele schade tot gevolg kan hebben. Daarnaast zien we dat criminelen soms bewust misbruik maken van de zwakke digitale weerbaarheid van deze groep door hen te ronselen voor illegale praktijken. Een voorbeeld hiervan is het inzetten van mensen met een LVB als geldezels, waarbij hun bankrekeningen worden gebruikt voor het witwassen van geld (Van Balkom, 2022). De gevolgen hiervan zijn vaak ernstig: de betrokkenen worden strafrechtelijk vervolgd, terwijl ze zich vaak niet volledig bewust zijn van de implicaties van hun handelingen.

Cybersecuritymaatregelen zijn vaak niet afgestemd op de specifieke behoeften van kwetsbare groepen. Onderzoek naar deze doelgroep helpt bij het creëren van een meer

inclusieve digitale samenleving, waarin ook mensen met een LVB zich veilig kunnen bewegen zonder angst voor misbruik of manipulatie. Door praktijkgericht en interdisciplinair onderzoek wil het kennisnetwerk effectieve interventies ontwikkelen om mensen met een LVB meer weerbaar te maken tegen cyberdreigingen. Dit kan bijvoorbeeld door het aanbieden van laagdrempelige educatieprogramma's, maar ook door interventies voor de begeleiders van mensen met een LVB, waarbij duidelijke richtlijnen voor digitale veiligheid en systemen die vroegtijdig signalen van misbruik herkennen centraal staan.

> Relevante onderzoeksvragen zijn: Hoe en in welke mate worden mensen met een LVB slachtoffer van cybercrime en betrokken bij illegale activiteiten? Welke vormen van slachtoffer-/daderschap komen het meest voor? Zien we verschillen in demografische variabelen? In hoeverre is het noodzakelijk om online begrenzingen in te stellen voor mensen met een LVB, kunnen risicogroepen worden geïdentificeerd? Op welke wijze kunnen begeleiders/ouders/opvoeders van mensen met een LVB bijdragen aan het cyberweerbaarder maken van deze groep? Hoe kunnen we via (gedrags)interventies mensen met een LVB cyberweerbaarder maken? Hoe bescherm je mensen met een LVB zonder hun autonomie/privacy te schenden?

5

VERSTERKINGS-MAATREGELEN VOOR CYBER-WEERBAARHEID: DE PRIVATE KANT

Jurjen Jansen, Kimberly Bluhm, Sander Ebbers, Ynze van Houten, Rick van der Kleij, Stephen McCombie, Peter Roelofsma, Bruno Verweijen

5.1 CYBERWEERBARE ORGANISATIES: BALANS TUSSEN VOORBEREIDING EN IMPROVISATIE

Cyberweerbaarheid is van vitaal belang geworden voor organisaties om zichzelf te beschermen tegen cyberdreigingen. Met de toenemende onderlinge verbondenheid van digitale systemen nemen de risico's van cyberaanvallen, datalekken en andere beveiligingsincidenten toe. De overheid vindt dat er moet worden ingezet op het verhogen van de cyberweerbaarheid van bedrijven (zie bijv. Strategie digitale economie uit 2022 [Ministerie van Economische Zaken en Klimaat, 2022]; Nederlandse Cybersecuritystrategie 2022-2028 [Nationaal Coördinator Terrorismebestrijding en Veiligheid, 2022]; KIA veiligheid 2024-2027 [KIA, 2023]) en het verkleinen van de groeiende cyberweerbaarheidskloof (CSR meerjarenstrategie 2022-2025 [CSR, 2022]). En ook de Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023-2029 (Rijksoverheid, 2023) stelt dat een hogere weerbaarheid en paraatheid van

overheid, bedrijven en maatschappelijke organisaties nodig is. In dit hoofdstuk ligt de focus met name op informatietechnologie (IT) en minder op de operationele technologie (OT). Dit is een witte vlek in deze agenda, aangezien bij OT ook belangrijke cyberrisico's voorkomen. Komende jaren willen wij binnen Cyberweerbaar NL het OT-domein meer gaan verkennen.

Effectief risico-, incident- en crisismanagement vormt de kern van strategieën voor cyberweerbaarheid. Deze managementpraktijken richten zich op het voorkomen, detecteren, reageren op en herstellen en leren van cyberdreigingen en -incidenten. Organisaties moeten proactief risico's inschatten, protocollen voor *incident response* opstellen en zich voorbereiden op mogelijke crises. Zo kunnen ze hun vermogen vergroten om de bedrijfscontinuïteit te handhaven en gevoelige informatie te beschermen. In dit hoofdstuk zoomen we in op het organisatieniveau. De vraag die hierbij centraal staat is: hoe kunnen organisaties hun cyberweerbaarheid structureel verhogen?

In tegenstelling tot cybersecurity, die vooral een preventieve doelstelling heeft, benadrukt cyberweerbaarheid dat volledige preventie onmogelijk is en dat organisaties doortastend moeten kunnen handelen als ze getroffen worden door een cyberaanval (Dupont, 2019). Daarmee leunt cyberweerbaarheid in grote mate op het vermogen van organisaties om zich voor te bereiden op cyberaanvallen. Uit openbare evaluatieonderzoeken naar cyberincidenten blijkt echter dat veel van de getroffen organisaties zich slechts beperkt hadden voorbereid op cyberaanvallen, maar toch in staat waren om effectief te reageren op cyberincidenten (Verweijen, 2022). Vaak hadden zij namelijk wel crisisstructuren en processen voor andersoortige incidenten, maar moesten deze aangepast worden aan de cybercrisis. Zo moet bijvoorbeeld specifieke expertise betrokken worden en zijn er unieke dilemma's op het gebied van crisiscommunicatie. Deze improvisatiepraktijken hebben veel weg van wat antropoloog Claude Levi-Strauss '*bricolage*' noemde, ofwel '*doing things with whatever is at hand*' (Levi-Strauss, 1966, p. 17 in

Duymedjian & Ruling, 2010). Hoewel dergelijk improvisatievermogen dus een belangrijke rol heeft gespeeld in *incident response*, wordt hier weinig aandacht aan besteed in de evaluatieonderzoeken en de aanbevelingen die daaruit voortvloeien (Verweijen, 2022). Met name twee zaken vallen op:

1. Het toegepaste improvisatievermogen is maar beperkt onderzocht. Er zijn weinig lessen geïdentificeerd over voorwaardelijke factoren en praktijken waardoor organisaties effectief konden improviseren.
2. Ondanks de erkenning van de noodzaak van improvisatie bij cyberincidenten, komt dit weinig terug in aanbevelingen. Zelfs in cases waar goed geïmproviseerd is, zijn aanbevelingen voornamelijk gericht op preparatie door uitgebreidere crisisplanvorming en scenario's. Daarmee lijkt veerkracht geoperationaliseerd te worden als een capaciteit die gerealiseerd wordt met formele documenten in plaats van improvisatie (Verweijen, 2022, p. 103).

Tegelijkertijd is improvisatievermogen risicovol: in situaties van grote complexiteit en onzekerheid zoals een incident kan improvisatie ook mislukken, en de situatie mogelijk verergeren (Hollnagel, 2014).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe vindt improvisatie in *incident response* plaats bij organisaties die getroffen zijn door een cyberincident? Welke voorwaarden, drempels en succesfactoren zijn van invloed op improvisatievermogen in *incident response*? En hoe verhouden improvisatievermogen en preparatieve activiteiten zich tot elkaar en hoe beïnvloeden ze elkaar?

5.2 MENSGERICHT ONTWERPEN VAN BEVEILIGINGSMAATREGELEN

Beveiligingsmaatregelen helpen om het risico voor de activa van de organisatie, zoals klantgegevens en informatiesystemen, te verminderen of te beperken. Beveiligingsmaatregelen op de werkvloer zijn echter alleen effectief als ze correct worden gebruikt (Whitten & Tygar, 1999) en leiden daarom niet automatisch tot verbeterde beveiliging (Sasse & Flechais, 2005; Furnell, 2005), vooral wanneer ze betrekking hebben op de eindgebruikers van de IT- en OT-systemen die beschermd moeten worden. Maatregelen die de eindgebruiker betreffen, zoals wachtwoordbeheer, zijn gericht op het beïnvloeden van gedrag van medewerkers. Door bewust bezig te zijn met cyberveiligheid, bijvoorbeeld het steeds invoeren van een sterk wachtwoord, worden medewerkers meer vaardig in het verkleinen van cyberrisico's voor de organisatie.

Bekeken vanuit een menselijk perspectief hebben beveiligingsmaatregelen vaak serieuze tekortkomingen (Furnell, 2005), waardoor mensen problemen hebben om beveiligingsmaatregelen correct te gebruiken (Sasse & Flechais, 2005; Seiler-Hwang et al., 2019). Whitten en Tygar (1999) toonden bijvoorbeeld aan dat mensen met een goed niveau van technische kennis, zelfs na instructie en oefening, er niet in slaagden om beveiligingsmaatregelen correct te gebruiken. Vaak erkennen de maatregelen die deze problemen veroorzaken niet de menselijke eigenschappen, zoals beperkingen van het werkgeheugen (Farrington, 2011), of het feit dat mensen geen rationele entiteiten zijn (zoals computers) die uitsluitend op basis van kennis handelen (Sligo & Jameson, 2000). Het is zelfs denkbaar dat eindgebruikers opzettelijk maatregelen uitschakelen of omzeilen als die hen hinderen bij hun werk. Dit verschijnsel kan worden gezien als een voorbeeld van waarschuwingsmoeheid (Bliss, 1993). Die term wordt gebruikt om situaties te beschrijven waarin eindgebruikers die herhaaldelijk worden blootgesteld aan waarschuwingsberichten over een beveiligingsrisico dat vervolgens niet optreedt, cynisch, apathisch en 'moe' worden van het horen

van waarschuwingen. Ze kunnen ongevoelig worden voor het risico en zichzelf daardoor nog meer in gevaar brengen of het systeem saboteren dat verantwoordelijk is voor de waarschuwingsberichten. Op deze manier kunnen zelfs de meest (technisch) veilige systemen onveilig worden (Feth & Polst, 2019).

Het falen van cybersecuritymaatregelen kan ook worden toegeschreven aan een conflict tussen twee onverenigbare doelen, namelijk het op tijd voltooien van het werk of het veilig houden ervan (Stroebe et al., 2013). Het efficiënt uitvoeren van taken die gebruikers helpen hun doelen te bereiken krijgt prioriteit. Beveiligingsmaatregelen maken de uitvoering van de taken die gebruikers op de lange termijn helpen om hun doelen te bereiken mogelijk, maar zijn niet essentieel om deze doelen te bereiken (Sasse & Flechais, 2005). Daarom kunnen mensen beveiligingsmaatregelen als een hindernis zien. In een onderzoek van Weigan (2021) vond bijna de helft van de kantoormedewerkers dat beveiligingsmaatregelen tot veel tijdverspilling leiden. Meer dan de helft maakte zich meer zorgen over het halen van deadlines dan over het blootstellen van de organisatie aan een datalek. Bijna een derde van hen had zelfs geprobeerd beveiligingsmaatregelen te omzeilen.

Een verklaring voor de bovengenoemde tekortkomingen kan de beperkte aandacht voor gebruiksvriendelijkheidsfactoren in het ontwerpproces zijn. Kennis van menselijke factoren maakt vaak geen deel uit van de vaardigheden van de teamleden van softwareontwikkelingsteams (Van der Kleij et al., 2024). Het toepassen van mensgerichte benaderingen vroeg in het ontwerpproces van beveiligingsmaatregelen kan het probleem van onbruikbare beveiligingsmaatregelen aanpakken. Zo worden gebruikers in staat gesteld om zich veiliger te gedragen en mogelijke schade door onveilig gedrag te voorkomen (Van der Kleij, 2022). De ontwerpopgave om mensgerichte cybersecuritymaatregelen te realiseren vereist een interactie waarbij mensen, processen en technologie elkaar aanvullen in plaats van elkaar in de weg zitten.

> Toekomstige onderzoeksvragen kunnen zijn: Hoe kunnen beveiligingsmaatregelen zo worden ontworpen dat de gebruiker, geconfronteerd met deze maatregelen, eerder geneigd is om zich veilig te gedragen? Hoe kunnen mensgerichte ontwerpkenmerken en technieken worden geïntegreerd in een gebruikersgerichte ontwerpbenadering voor bruikbare cybersecurity?

5.3 DETECTIE EN RESPONS BIJ CYBERDREIGINGEN

Detectie maakt het mogelijk om binnen een netwerk of systeem malafide software, gebruikers enzovoort vroegtijdig te identificeren om zo tijdig te reageren en eventuele schade te voorkomen of te beperken (NCSC, 2024a). Dankzij detectie kunnen organisaties een inzichtelijk beeld krijgen van dreigingen, waardoor gepaste maatregelen kunnen worden getroffen. Een mogelijke eerste stap voor een organisatie bij het starten van detectie is de afname van diensten, zoals een antivirussoftware en monitoringsdienst bij de externe IT-dienstverlener of om de interne ICT-beheerder over deze onderwerpen bij te laten scholen (NCSC, 2024b).

Cyber Threat Intelligence (CTI) is het verzamelen, verrijken en analyseren van informatie over digitale dreigingen, wat organisaties helpt bij het beoordelen van risico's en het nemen van beveiligingsmaatregelen (NCSC, 2021). CTI richt zich primair op technologische aspecten, zoals softwarekwetsbaarheden en aanvalspogingen op servers. Echter, deze focus leidt ertoe dat CTI niet altijd aansluit bij de strategische doelen van de organisatie (Ainslie et al., 2023; Cremer et al., 2022). Het delen van dreigingsinformatie binnen en buiten organisaties stuit regelmatig op hindernissen, vooral omdat technische details niet altijd worden begrepen of gewaardeerd door besluitvormers op C-niveau of het management. Dit kan resulteren in een onvolledig gecommuniceerd dreigingsbeeld en een onderschatting van risico's, waardoor de kans op cyberincidenten toeneemt (Ainslie et al., 2023; Ask et al., 2021).

Elke situatie die zou kunnen leiden tot een cyberincident wordt een *near-miss* of bijna-incident genoemd (Jones et al., 1999). In de veiligheidskunde krijgt dit thema veelvuldig aandacht, omdat *near-misses* als voorspellers of indicatoren van daadwerkelijke incidenten worden gezien. Daarnaast geven *near-misses* inzicht in de dagelijkse praktijk van organisaties (Ebert et al., 2023; Zimmermann & Renaud, 2019). *Near-misses* die gerapporteerd worden zorgen ervoor dat een organisatie preventief maatregelen kan nemen om erger te voorkomen (Gnoni et al., 2022; Jones et al., 1999; Vrbnjak et al., 2016). Binnen de cyberweerbaarheid krijgen *near-misses* nog weinig aandacht (Bair et al., 2017; Ebert et al., 2023; Zimmermann & Renaud, 2019). Het is onduidelijk wat wordt gezien als *near-miss*, in hoeverre deze *near-misses* onderdeel zijn van het risicobeeld van een organisatie en in hoeverre geleerd wordt van *near-misses*. Om een vollediger beeld van dreigingen te krijgen, is een bredere benadering aan te raden (Ainslie et al., 2023; Pollini et al., 2022). Dit omvat het integreren van zowel technische informatie van externe en interne bronnen (zoals *insider threats*) als niet-technische informatie, zoals door medewerkers opgemerkte en gemelde risicovolle situaties.

Na het detecteren van een cyberincident volgt de repressiefase met processen om zo veel mogelijk de schade te beperken en de systemen te herstellen. Binnen deze fase richt een digitaal forensisch onderzoek zich op het duiden van malafide activiteiten binnen de IT-infrastructuur (NCSC, 2024b). Een *root-cause* analyse is een methode om de onderliggende redenen van een incident te analyseren. In de praktijk gebeurt dit vaak vanuit de aanname dat een incident ontstaat vanuit een keten van gebeurtenissen. De oorzaak wordt in deze aanpak veelal achterhaald door te onderzoeken wat de zwakke schakel in de keten is geweest, vaak resulterend in de uitspraak ‘de mens is ergens de zwakste schakel gebleken’ (Ebert et al., 2023; Hielscher et al., 2023; Moody et al., 2018). De huidige aanpak heeft echter zijn beperkingen. De ‘incident-als-keten’-benadering kan zorgen voor een te simplistische kijk op de werkelijkheid, wat kan leiden tot symptoombestrijding (Ebert et al., 2023). Meerdere onderzoekers

suggereren dat een meer holistische analyse effectiever kan zijn, waarbij technische en socioculturele/menselijke aspecten in interactie met elkaar worden geanalyseerd (Ebert et al., 2023; Jansen, 2023; Morgan et al., 2020; Pollini et al., 2022; Spithoven et al., 2024; Zimmermann & Renaud, 2019). Verschillende benaderingen van de rol van de mens zijn uitgebreid in paragraaf 3.6 besproken.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe kunnen detectieprocessen, rekening houdend met verschillende volwassenheidniveaus van organisaties, laagdrempelig worden ingericht of worden verbeterd? Welke rol spelen niet-technische informatiebronnen, zoals door medewerkers gemelde risicovolle situaties, in het verrijken van CTI? In hoeverre beïnvloedt de technische complexiteit van CTI de risicoperceptie en -beoordeling door managementteams? Op welke manieren kan CTI effectiever gecommuniceerd worden naar besluitvormers op C-niveau om een volledig begrip van het dreigingsbeeld te waarborgen? Wat zou een succesvolle inrichting van de informatieloop kunnen zijn? Hoe wordt een '*near-miss*' gedefinieerd binnen de context van cyberweerbaarheid, en hoe worden deze '*near misses*' geïdentificeerd en gerapporteerd binnen organisaties? In welke mate maken '*near-misses*' deel uit van het risicobeeld van een organisatie op het gebied van cyberweerbaarheid, en hoe wordt er van deze gebeurtenissen geleerd om toekomstige cyberincidenten te voorkomen? En op welke wijze kan de markt betrokken worden bij het vergroten van de cyberweerbaarheid van organisaties?

5.4 INCIDENT RESPONSE IN HET MKB

Onderzoek wijst uit dat een relatief groot deel van het mkb slachtoffer wordt van cybercriminaliteit, waarbij schattingen variëren van 5% tot 16% voor het kleinbedrijf en 12% tot 20% van het grotere mkb (Notté et al., 2019; CBS, 2022; Verweijen et al., 2023). Vandaar dat wordt geconcludeerd dat het mkb onvoldoende weerbaar is tegen cyberaanvallen (DTC, 2023).

Desondanks schatten ondernemers het risico op slachtofferschap relatief laag in en vinden zij dat het treffen van maatregelen veel tijd en geld kost in verhouding tot de mogelijke baten (Verweijen et al., 2023).

Daarnaast bereiden relatief weinig ondernemers zich voor op een mogelijk cyberincident. Verweijen en collega's (2023) tonen aan dat een groot deel van hun respondenten behoefte heeft aan informatie over mogelijke handelingsperspectieven in het geval van een cyberaanval. Uit onderzoek van Kaspersky (2023) blijkt dat minder dan een derde van de 311 bevraagde Nederlandse bedrijven een *incident response*-plan heeft. Het aantal bedrijven met een draaiboek is met 21% nog lager. Onderzoek van ABN AMRO (Krauwer, 2024) wijst uit dat van de bevraagde mkb-organisaties 33% maatregelen heeft genomen voor hulpverlening indien zij te maken hebben met een cyberincident. Uit een benchmarkonderzoek van het Digital Trust Center (DTC) blijkt dat 63% van de bevraagde mkb'ers geen bellijst heeft opgesteld voor een digitaal noodgeval (Jacobs & Paardenkoper, 2023). Desondanks lijkt er wel de intentie te zijn om *cyberincident response* te organiseren. Uit onderzoek van Wielers (2022) blijkt dat ruim een kwart van de geënquêteerde mkb'ers een hoge intentie heeft om *cyberincident response*-plannen in te passen; minder dan de helft heeft een gemiddelde/gematigde intentie om dit te doen, en een kwart heeft een lage intentie. Daarbij wordt geconcludeerd dat bedrijven die druk voelen vanuit leveranciers of klanten om *incident response*-plannen op te stellen, een hogere intentie hebben om dit te doen. Een studie van IBM laat echter zien dat ruim de helft van de organisaties met een *incident response*-plan die plannen niet test (IBM Security, 2019).

Er zijn verschillende opties voor het mkb om *incident response* te organiseren, maar het is nog niet duidelijk welke goed aansluiten op de behoeften van het mkb. Relatief veel mkb'ers hebben een externe IT-dienstverlener, 64% volgens Jacobs en Paardenkoper (2023), en gaan ervan uit dat deze hen kan helpen in het geval van een cyberincident. Harsch en collega's (2014) geven echter aan dat IT-professionals vaak niet

de vaardigheden hebben voor *incident response*, zoals forensisch onderzoek. Echter, het sluiten van een contract met een cybersecuritybedrijf voor *incident response*-ondersteuning is gezien de kosten voor veel mkb'ers niet haalbaar. Andere opties om *cyberincident response* te organiseren is het afsluiten van een cyberverzekering, waarbij de verzekeraar de *response* faciliteert door contact te leggen met experts (Woods & Böhme, 2022). Hierbij zijn echter ook nadelen te benoemen; de ingangseisen zijn hoog, premies stijgen, soms moet een aanbetaling gedaan worden die cashflowproblemen kan opleveren, de experts kunnen onbekende onderaannemers inhuren die moeilijker zijn te controleren op kwaliteit, en niet alle *response*-diensten vallen standaard binnen de polis (MBO digitaal, z.d.; Woods & Böhme, 2022). MBO digitaal (z.d.) heeft daarom een alternatief opgezet: *cyber risk pooling*, waarin mbo-instellingen onderling een financiële bijdrage leveren bij een cyberaanval.

Voor een effectieve *incident response* zijn verschillende expertisegebieden noodzakelijk. Zo is enerzijds technische kennis nodig over IT-systemen en cybersecuritymaatregelen, en anderzijds expertise van crisismanagement, communicatie en reputatiemanagement (Verweijen, 2022). Uit verschillende (evaluatie)onderzoeken blijkt echter dat de samenwerking tussen deze expertises in organisaties beperkt is (Ebbers et al., 2021). Een belangrijke reden daarvoor is dat de taal en het referentiekader van ICT'ers enerzijds en crisismanagers en bestuurders anderzijds verschillen (Verweijen, 2022, p. 101). Zo is het voor technisch personeel niet altijd duidelijk wanneer een IT-incident opgeschaald moet worden naar een crisis, in verband met bredere consequenties voor de organisatie, klanten, en de maatschappij. In algemene zin wordt gesproken over 'twee werelden' (Verweijen, 2022), waarbij cybersecurity gezien wordt als een 'IT-feestje' (Ebbers et al., 2021). Deze constatering past binnen een bredere conclusie in een onderzoek naar cybersecurity, waarin men concludeert dat er een gebrek aan verbinding is tussen security en business-doelen en -processen (Sadok et al., 2020)

en securitypersoneel en gebruikers (Albrechtsen & Hovden, 2009; Da Veiga & Martins, 2017).

Er is tot nu toe weinig onderzoek gedaan naar de manier hoe *cyberincident response* georganiseerd dient te worden om aan te sluiten op de behoeften van mkb'ers en de omstandigheden waarmee zij te maken hebben. Om effectieve *incident response* te kunnen organiseren is het onder andere nodig om een beeld te vormen van de beleving van mkb'ers die slachtoffer zijn geworden (slachtoffer *journey*) en de drempels en succesfactoren die bepalen of een slachtoffer goede *incident response*-ondersteuning kan krijgen. Ten slotte is het belangrijk om *incident response* niet als afzonderlijke risicomanagementfase te beschouwen, maar als vliegwiel om preventie, detectie en preparatie te bevorderen.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe kan *incident response* voor het mkb georganiseerd worden, zodat het aansluit bij de behoeften en werkomstandigheden van mkb'ers? Welke vormen van *incident response*-ondersteuning zijn momenteel gericht op en betaalbaar voor het mkb, en worden deze vormen al gevonden door mkb'ers? Welke drempels en succesfactoren zijn van invloed op *cyberincident response* voor het mkb? Hoe kan *incident response*-ondersteuning bijdragen aan verbetering van preventie, detectie en preparatie? Hoe verloopt de communicatie en samenwerking tussen cybersecurity professionals, bestuurders, en gebruikers bij cyberincidenten in organisaties en welke barrières worden er ervaren? En hoe kunnen de communicatie en samenwerking tussen deze doelgroepen tijdens cyberincidenten verbeterd worden?

5.5 KRITIEKE-INFRASTRUCTUURSECTOREN (GMTS)

De wereldwijde, doelbewuste aanvallen op kritieke infrastructuren door cyberdreigingsactoren zijn zorgwekkend vanwege de ernstige, potentiële gevolgen voor de wereldwijde veiligheid en de wereldeconomie. Tijdens de COVID-19-pandemie

zijn het kritieke karakter en de kwetsbaarheid van onze toeleveringsketens aangetoond. Dit is onder andere duidelijk binnen het wereldwijde maritieme transportsysteem (GMTS). Het GMTS is een systeem van systemen en omvat niet alleen schepen, maar ook waterwegen, havens en verbindingen over land, die personen en goederen van en naar het water vervoeren. GMTS speelt een belangrijke rol in de wereldeconomie: meer dan 80% van alle vracht wordt per schip vervoerd (Bronk & Dewitt, 2020) en vrachtvervoer per schip vertegenwoordigt 70% van de wereldhandel in waarde (Loomis et al., 2021). Tegelijkertijd verouderen de vloten en hun technologie, waardoor ze kwetsbaarder worden voor cyberaanvallen. Zo is 38% van de olietankers en 59% van de stukgoedschepen ouder dan twintig jaar (Tam & Jones, 2018). Bevoorradingsketens zelf zijn steeds kwetsbaarder voor cyberaanvallen. Dit is vooral de laatste jaren opvallend: '… Europese bronnen schatten een groei van 400% in cyberaanvallen op de bevoorradingsketen in 2021 ten opzichte van 2020' (Kessler & Shepard, 2022). GMTS is een belangrijk onderdeel van die wereldwijde toeleveringsketen en zal in toenemende mate het doelwit zijn van cyberdreigingsactoren.

In een rapport beschreven Daffron et al. (2019) een hypothetische cyberaanval op vijftien havens in Azië en de Stille Oceaan met malware die van schepen naar havens overging. Ze voorspelden dat het verlies zou kunnen oplopen tot 110 miljard dollar en dat het overgrote deel van dat bedrag door geen enkele verzekering zou worden gedekt. Er is in de maritieme sector nog geen cyberaanval op deze schaal geweest, maar er zijn wel talloze havens en schepen getroffen door aanvallen met ransomware, destructieve malware en het hacken van operationele technologie. Deze aanvallen zijn opgezet door criminele groepen en statelijke hackers. Het bekende geval van Maersk, dat in 2017 meer dan 300 miljoen dollar verloor door de NotPetya-malwareaanval, is hier een goed voorbeeld van (Mathews, 2017).

In maart 2020 blokkeerde de MV Ever Given het Suezkanaal en verstoorde zo het GMTS ernstig. Hoewel het incident niet door een cyberaanval werd veroorzaakt, toont het de

kwetsbaarheid aan van het GMTS, aangezien het ongeveer 9 miljard dollar per dag kostte (Lee & Wong, 2021). Een ander niet-cyber GMTS-incident vond plaats in 2024 toen de MV Dali in botsing kwam met de Francis Scott Key Bridge in Baltimore, waardoor deze instortte en zes arbeiders die aan de brug werkten omkwamen. Een groter verlies aan mensenlevens werd voorkomen dankzij de snelle actie van de havenautoriteiten om de brug minder dan een minuut na de instorting af te sluiten voor verkeer. De instorting blokkeerde de haven en veroorzaakte tweede-orde-effecten. Bruce Carnegie-Brown, voorzitter van Lloyd's of London (de grootste commerciële (her)verzekeringsmarkt ter wereld) zei dat dit 'mogelijk het grootste verzekerde verlies ooit op zee' was, met een omvang van 4 miljard dollar (Reid, 2024). Dergelijke incidenten kunnen gemakkelijk opzettelijk worden veroorzaakt door een cyberaanval. Een cyberdreigingsacteur zou dit kunnen bereiken door de navigatie- of voortstuwingssystemen van een schip op verschillende manieren aan te tasten. Het doel van een dergelijke aanval kan deel uitmaken van een conflict tussen grootmachten (bijv. de Verenigde Staten/China), in een regionaal conflict (bijv. Israël/Iran) of door cybercriminelen die losgeld eisen of short gaan op de aandelenmarkt.

Een voorbeeld van een samenwerkingsverband binnen het maritieme transportsysteem op het gebied van cyberweerbaarheid is FERM. In de Rotterdamse haven zijn bedrijven door sterke onderlinge afhankelijkheid en verbonden processen een kwetsbare keten voor cyberaanvallen (FERM Rotterdam, z.d.). Om het bewustzijn over cyberrisico's van bedrijven in de Rotterdamse haven te vergroten, de samenwerking te stimuleren en uiteindelijk de best digitaal beveiligde haven te worden, is in 2021 FERM gestart. FERM voorziet bedrijven van hulpmiddelen door het faciliteren van onderling uitwisselen van dreigingsinformatie, het in kaart brengen van kwetsbaarheden en dreigingen en het organiseren van trainingen. Zo heeft FERM onder andere een centraal meldpunt voor cyberincidenten ingericht (Bras, z.d.).

Toekomstig onderzoek gericht op de cyberweerbaarheid van het maritieme transportsysteem zou zich kunnen concentreren op vragen als: Wat is de aard, oorzaak en impact van cyberaanvallen in de maritieme sector tot nu toe? Hoe kan die informatie realistische maritieme cybersimulaties informeren om cyberbewustzijn, operationele procedures en ons begrip van de menselijke factor te vergroten? Hoe kan die informatie toekomstige beleidsmaatregelen, wetgeving en technologie informeren om de maritieme sector weerbaar te maken tegen toekomstige aanvallen?

6

CYBERCRIMINELEN

Rutger Leukfeldt, Luuk Bekkers, Joeri Loggen, Asier Moneva, Robby Roks

6.1 ONTWIKKELPADEN EN RISICOFACTOREN VOOR DADERSCHAP VAN CYBERCRIME

Om de cyberweerbaarheid van burgers, organisaties en samenleving als geheel te vergroten is het van belang om op de hoogte te blijven van de ontwikkelingen aan de daderkant van online criminaliteit, zoals hoe cybercriminelen in het criminele circuit terecht zijn gekomen. Ontwikkelpaden beschrijven de processen gerelateerd aan het beginnen, voortzetten en stoppen met criminaliteit. Binnen de literatuur zijn alleen ontwikkelpaden voor online fraude en hacking te onderscheiden. Bij online fraude lijken potentiële cyberdaders te ervaren dat ze niet genoeg geld hebben om maatschappelijke doelen te bereiken (Adejoh et al., 2019; Ebot, 2017). Om deze doelen toch te realiseren, besluiten ze om online fraude te plegen (Adejoh et al., 2019; Ebot, 2017; Hutchings, 2013). Deze beslissing lijkt deels te worden beïnvloed door leeftijdsgenoten. Via *social learning* verkrijgen potentiële daders de kennis en vaardigheden om online fraude te plegen (Adejoh et al., 2019; Adou & Kolé, 2020; Ebot, 2017; Hutchings, 2013; Whitty, 2018). Het blijven plegen van of stoppen met online fraude lijkt samen te hangen met een kosten-batenafweging en het gebruik van neutralisatietechnieken (Ebot, 2017; Hutchings, 2013; Whitty, 2018). Gekeken naar risicofactoren gerelateerd aan het initiatieproces, lijkt *social learning* de meest robuuste factor te zijn (Adou & Kolé, 2020; Ibrahim, 2016; Ogunleye et al., 2020).

Voor hacken lijken individuen door nieuwsgierigheid, interesse in technologie en het spelen van videogames, in contact te komen met leeftijdsgenoten die zich bezighouden met

hacken, en zo de benodigde kennis en vaardigheden te verkrijgen om te kunnen hacken (Hutchings, 2013, 2014; McAlaney et al., 2020; National Crime Agency, 2017; Steinmetz, 2015). In het begin is het hacken 'onschuldig' en zonder criminele bedoelingen (Leppänen et al., 2020; Richet, 2017). Naarmate hackers meer ervaring opdoen, worden hun cybercriminele activiteiten ernstiger (Aiken et al., 2016; Bachmann, 2011; Hutchings, 2014; Richet, 2017). Risicofactoren die een rol lijken te spelen bij het initiatieproces zijn onder andere een relatief jonge leeftijd (Chua & Holt, 2016; Holt & Steinmetz, 2021; Lee & Holt, 2020; McBrayer, 2014; Steinmetz, 2015), mannelijk geslacht (Bossler, 2021; Fox & Holt, 2021; Holt et al., 2020a; Lee & Holt, 2020), slechte zelfcontrole (Fox & Holt, 2021; Holt et al., 2021; Holt & Steinmetz, 2021; Lee & Holt, 2020), en deviante leeftijdsgenoten (Bossler, 2021; Fox & Holt, 2021; Holt et al., 2020; Lee & Holt, 2020; McAlaney et al., 2020).

Risicofactoren gerelateerd aan betrokkenheid bij het ontwikkelen of verspreiden van malware, zijn onder andere relatief lagere cognitieve vaardigheden (Treadway, 2017), goede IT-kennis (Chua & Holt, 2016; Morris & Blackburn, 2009; Peersman et al., 2022), en *social learning* (Chon, 2016; Morris & Blackburn, 2009). Voor DDoS-aanvallen lijken tot op heden geen robuuste risicofactoren te zijn geïdentificeerd (Loggen et al., 2024b). Samenvattend is er op dit moment een gebrek aan literatuur omtrent de ontwikkelpaden van nagenoeg alle vormen van cybercrime. Ditzelfde geldt ook voor risicofactoren (Loggen et al., 2024a; Loggen, Moneva & Leukfeldt, 2024b).

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe zien de ontwikkelpaden bij DDoS-aanvallen en malware eruit? Welke factoren spelen een rol bij het in stand houden van cybercriminele activiteiten? En welke beschermende factoren dragen bij aan het stoppen met cybercrime?

6.2 DE STRUCTUUR EN ORGANISATIE VAN CYBERCRIMINELE NETWERKEN

In onderzoek naar online criminaliteit krijgt het thema van de structuur en organisatie van de bestudeerde groeperingen of netwerken de nodige aandacht. De aanname hierbij is dat het internet een prima gelegenheidsstructuur vormt voor gedecentraliseerde, flexibele netwerken van criminelen die losjes georganiseerd samenwerken en werkzaamheden verdelen op basis van kennis en kunde. In een aantal studies heeft men dit onderzocht door onder andere te kijken of er sprake is van een hiërarchische, gecentraliseerde structuur of van lossere verbanden. Dit heeft geresulteerd in typologieën van (groepen van) cyberdaders op basis van de organisatiegraad.

Een vraag die in diverse publicaties wordt opgeworpen is in hoeverre online criminaliteit kan worden gezien als georganiseerde criminaliteit. In diverse studies naar financieel gemotiveerde dadergroepen die aanvallen uitvoeren op klanten van banken, kunnen drie lagen in de structuur van de cybercriminele netwerken worden herkend. Bovenaan staan de kernleden die de criminele activiteiten plannen, een lange tijd met elkaar samenwerken en andere geschikte mededaders zoeken. Onder deze kernleden staan facilitators die specifieke criminele diensten leveren. De onderste laag wordt gevormd door geldezels, die ingezet worden om het spoor naar de criminele groep te verhullen. Hiermee laten deze studies zien dat cybercriminele samenwerkingsverbanden wel een netwerkstructuur hebben, maar toch ook hiërarchische elementen kunnen bevatten.

Recentelijk hebben Whelan en collega's (2024) zich gericht op de structuur en organisatie van een andersoortige cybercriminele verschijningsvorm, namelijk groeperingen die betrokken zijn bij ransomware. De auteurs beschrijven dat de structuur van groeperingen die zich bezighouden met ransomware bestaat uit een kerngroep van een relatief klein aantal individuen die de malware ontwikkelen en de activiteiten van de groep coördineren. Daarnaast worden

'affiliates' onderscheiden in de periferie van het netwerk, die samenwerken met de kernleden en vaak verantwoordelijk zijn voor het uitvoeren van een aanzienlijk deel van de ransomware-aanvallen. Dit brengt de auteurs tot de conclusie dat ransomware-groepen verschillen van het stereotiepe (en achterhaalde) beeld van maffiagroeperingen, en dat zij gestructureerd zijn als legitieme bedrijven. Ransomware-groepen lijken een netwerkvorm te vertonen die door auteurs wordt getypeerd als een hybride vorm van georganiseerde criminele samenwerkingsverbanden; er valt een combinatie waar te nemen van de structuur van offline georganiseerde criminele samenwerkingsverbanden met, tegelijkertijd, enige mate van hiërarchie en arbeidsverdeling. Dit lijkt van toepassing te zijn op veel cybercriminele netwerken, ongeacht het type online criminaliteit.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Hoe ziet de structuur van het hele palet aan cybercriminele netwerken eruit en wat zijn de verschillen en overeenkomsten van netwerken die zich bezighouden met *cyber-dependent* en *cyber-enabled crime*? Hoe verweven zijn traditionele georganiseerde criminaliteit en cybercriminele netwerken? En hoe kunnen cybercriminele netwerken het beste gefrustreerd worden en welke alternatieve interventies zijn hierbij effectief?

6.3 ONTSTAAN EN ONTWIKKELING CYBERCRIMINELE SAMENWERKING

Hoe ontstaan cybercriminele vormen van samenwerking? Allereerst wijzen studies op de rol van online marktplaatsen; er zijn diverse forums, websites, socialemediaplatforms en apps die dienen als digitale ontmoetingsplaatsen (Soudijn & Zegers, 2012). Toegang tot dergelijke digitale ontmoetingsplaatsen lijkt laagdrempeliger dan in het geval van offline criminele ontmoetingsplaatsen (meer hierover in par. 6.4).

Op basis van de beschikbare literatuur lijken er twee belangrijke redenen om over te gaan tot online cybercriminele

samenwerking. Ten eerste kunnen op deze manier eenvoudig(er) nieuwe netwerkleden met de juiste vaardigheden en connecties worden gevonden. Ten tweede biedt het internet de mogelijkheid om de eigen identiteit goed af te schermen, waardoor de pakkans wordt geminimaliseerd. Echter, deze anonimiteit, die de pakkans zo laag maakt, kan ook juist zorgen voor problemen in de samenwerking, bijvoorbeeld ten aanzien van het beoordelen van de betrouwbaarheid van mededaders. Forums hebben hier wel allerlei slimme trucs op bedacht, zoals ratingsystemen en zelfs conflictoplossing, maar deze blijken niet zo goed te werken als (dreiging met) geweld en gebruik maken van bekende sociale contacten.

Samenwerking komt echter niet alleen online tot stand. Diverse studies laten zien dat bij cybercriminele netwerken vier typen van ontstaan en groei te zien zijn; van netwerken die geheel bestaan uit leden met offline sociale relaties tot netwerken die geheel ontstaan zijn op basis van online contacten. Tussen deze uitersten bevinden zich netwerken waarbij zowel sprake is van online als offline sociale banden. De cyberdaders die onderdeel uitmaken van deze groepen hebben elkaar doorgaans offline leren kennen, maar maken gebruik van contacten die ze hebben opgedaan op online markten om daarmee de criminele activiteiten te faciliteren. Echter, in deze studie was ook sprake van een netwerk waarbij de kernleden elkaar op een online forum ontmoetten en vervolgens toch ook gebruik maakten van offline sociale contacten om geld wit te wassen.

Ook hier zien we het belang van vertrouwen en anonimiteit terugkomen. Eén van de grootste problemen van traditionele georganiseerde misdaad is dat bij conflicten tussen twee partijen geen gebruik kan worden gemaakt van legale manieren van conflictoplossing, en er ook geen aangifte kan worden gedaan. Dit is één van de belangrijke redenen waarom traditionele netwerken gebruik maken van geweld. Ten tweede werkt men het liefst samen met personen die ze goed kennen en vertrouwen, zoals familie of kennissen. Het zijn precies deze mechanismen die we ook gedeeltelijk terugzien bij cybercriminele vormen van samenwerking. Ondanks

dat de mogelijkheden van online criminaliteit grenzeloos zijn, zien we dat een deel van de samenwerkingsverbanden wordt gekenmerkt door een zekere mate van lokale inbedding.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Is het mogelijk om een typologie te ontwikkelen van alle verschijningsvormen van georganiseerde vormen van cybercrime en welke opsporingsstrategieën kunnen worden gekoppeld aan de diverse varianten binnen die typologie? Welke rol spelen online en offline sociale banden bij het ontstaan en groeien (rekrutering) van het hele palet aan cybercriminele netwerken, en wat zijn de verschillen en overeenkomsten van netwerken die zich bezighouden met *cyber-dependent* en *cyber-enabled crime*? En hoe groot is de lokale inbedding bij de diverse vormen van cybercrime, en hoe kan deze lokale inbedding worden gebruikt bij de opsporing en disruptie van cybercriminele netwerken?

6.4 CYBERCRIME-AS-A-SERVICE

De term '*cybercrime-as-a-service*' (CaaS) verwijst naar het aanbieden van tools, diensten en expertise op het gebied van cybercriminaliteit, meestal via ondergrondse marktplaatsen en netwerken (Manky, 2013). CaaS stelt personen die zelf niet de technische vaardigheden bezitten in staat om cybercrimes te plegen (Europol, 2014). Diensten op het gebied van cybercriminaliteit zijn relatief eenvoudig online toegankelijk, zijn op veel plekken verkrijgbaar, zijn betaalbaar (of in sommige gevallen gratis) en worden geleverd met tutorials of zelfs een 'helpdesk' voor onervaren gebruikers (Hyslip, 2020). Door de toegangsdrempel voor cybercriminaliteit te verlagen, vormt CaaS een extra bedreiging voor de cyberweerbaarheid van individuen en organisaties.

CaaS is er in vele soorten en maten, van '*phishing-as-a-service*' tot '*denial-of-service-as-a-service*'. Er zijn meer dan dertig soorten CaaS gedocumenteerd en de lijst blijft groeien (Akyazi et al., 2021; Huang et al., 2017). De trend is dat elke

technologische ontwikkeling die door cybercriminelen kan worden misbruikt, ook als een dienst wordt aangeboden.

Vertrouwen is van groot belang op markten waar illegale goederen en diensten worden aangeboden (Munksgaard, 2024). Onderzoek geeft inzicht in hoe CaaS-markten werken, welke producten ze aanbieden en hoe ze deze aanbieden, welke kenmerken verband kunnen houden met het succes van de markten, welke factoren kunnen wijzen op een betrouwbare verkoper, en hoe de markten toegankelijk zijn (Allodi et al., 2016; Campobasso, 2024). Wat de toegankelijkheid betreft, lijkt er sprake te zijn van een verschuiving van het dark web naar het clear web en dan vooral naar applicaties als Telegram (Roks & Monshouwer, 2020). Kortom, cybercriminele markten worden dus steeds toegankelijker.

Ondanks al het onderzoek blijven bepaalde vragen onbeantwoord. We hebben bijvoorbeeld nog geen goede manier om de ware omvang en schaal van het CaaS-ecosysteem te bepalen, noch de specifieke impact ervan op slachtofferschap onder burgers en bedrijven. Schattingen lopen uiteen en zijn onnauwkeurig.

Vanuit een toegepast perspectief is een ander aspect waar we weinig van weten, de vraag welke strategieën effectief zijn bij het ontwrichten van CaaS-ecosystemen. Afgezien van de uitschakeling van specifieke markten, gecoördineerd door opsporingsinstanties, is het onbekend welke maatregelen de markten kunnen destabiliseren, bijvoorbeeld door het vertrouwen van de leden te ondermijnen of klanten te ontmoedigen bepaalde diensten af te nemen. Ook is het onduidelijk welke beschermende maatregelen burgers en organisaties weerbaarder kunnen maken tegen aanvallen van niet-technische actoren die gebruik maken van CaaS-diensten. Met name voor dat eerste punt is evaluatieonderzoek hard nodig: wat werkt en waarom? Dat zijn de grootste vragen op dit moment.

> Oftewel, toekomstig onderzoek zou zich kunnen richten op vragen als: Wat is de werkelijke omvang van het CaaS-ecosysteem? Wat werkt om CaaS-markten te verstoren? En wat werkt om organisaties cyberweerbaar te maken tegen CaaS-aanvallen?

6.5 GELDEZELS / MONEY MULES

Geldezels zijn een cruciale schakel in de uitvoering van financieel-economische online criminaliteit (Leukfeldt & Loggen, 2022; Leukfeldt et al., 2017a, 2017b, 2017c, 2017d; Nazzarri, 2023). De term geldezel heeft betrekking op mensen die hun bankrekening laten gebruiken voor het wegsluizen van gestolen geld. Hierbij wordt geld vanaf de bankrekening van slachtoffers direct overgemaakt naar de bankrekening van geldezels, waarna het geld vaak snel wordt gepind. Door deze constructie blijven daders van bijvoorbeeld phishing, bankhelpdeskfraude en WhatsAppfraude zelf uit beeld van de politie en banken, en kunnen zij ongestoord gebruik maken van de illegale opbrengsten. Vanwege het belang van geldezels in de uitvoering van online criminaliteit, is het ook een belangrijke doelgroep voor wetenschappelijk onderzoek. Toch staat dit onderzoek nog in de kinderschoenen.

De beperkte literatuur dusver toont aan dat geldezels worden geronseld op sociale media en ook via bestaande sociale relaties in de fysieke wereld (Rani et al., 2024; Bekkers et al., 2023; Bekkers & Leukfeldt, 2023; Leukfeldt et al., 2017a, 2017b, 2017c, 2017d). Ze zijn onderdeel van deviante sociale omgevingen, waarin het plegen van fraude voor financieel gewin genormaliseerd en geaccepteerd is (Leukfeldt & Kleemans, 2019; Bekkers et al., 2024a, 2024b). Hoewel een financieel motief en een verhoogde status inderdaad een rol spelen bij het gedrag van geldezels, wordt een deel mogelijk ook misleid of gedwongen tot deelname aan fraude (Bekkers & Leukfeldt, 2023; Bekkers et al., 2024b). Grotendeels is nog onbekend hoe de criminele carrière van geldezels eruitziet en welke individuele factoren een rol spelen bij de betrokkenheid van geldezels bij online criminaliteit en bij *desistance*

van online criminaliteit (Bekkers et al., 2023, 2024a, 2024b). Daarnaast is er weinig onderzoek gedaan naar de aanpak van geldezels in de praktijk en de effectiviteit van bestaande interventies (Bekkers et al., 2024b). Dergelijk onderzoek is dus niet alleen theoretisch relevant, maar heeft ook direct meerwaarde voor de politie en de betrokken ketenpartners wat betreft interventie en preventie.

> Toekomstig onderzoek zou zich kunnen richten op vragen als: Wat kenmerkt de criminele carrière van geldezels? Welke interventies worden in de praktijk toegepast op de doelgroep geldezels en wat zijn de effecten van deze interventies? Welke risicofactoren en beschermende factoren spelen een rol bij geldezels? En welke processen en factoren spelen een rol bij het onderbreken of stopzetten van crimineel gedrag van geldezels (*desistance*)?

6.6 DE OVERLAP TUSSEN TRADITIONELE CRIMINALITEIT EN ONLINE CRIMINALITEIT

Criminaliteit hybridiseert. Daders van online criminaliteit leunen ook op de fysieke wereld in de voorbereiding en uitvoering van delicten, en daders van traditionele criminaliteit hebben geleerd hoe ze technologie kunnen gebruiken om delen van het *crime script* te faciliteren of verbeteren (Roks et al., 2021; Leukfeldt & Holt, 2022; Van der Laan et al., 2021; Bekkers et al., 2024; Leukfeldt et al., 2021). Op basis van analyse van politiedossiers tonen Roks en collega's (2021) bijvoorbeeld aan dat mensen die betrokken waren bij het plegen van overvallen en het dealen van drugs, nu ook geldezels ronselen voor phishing. Tegelijkertijd trof de politie bij een woninginval bij daders van phishing grote hoeveelheden drugs aan. In de Monitor Jeugdcriminaliteit (Van der Laan et al., 2021) is de grote trend inderdaad dat online en offline criminaliteit steeds meer overlappen. Dit impliceert dat een groot deel van de inspanningen van de politie en het Openbaar Ministerie ook gericht zou moeten zijn op de aanpak

van digitale vormen van criminaliteit (Ruiter et al., 2023; Bekkers et al., 2024).

Het is dus belangrijk dat er meer (toegepast) wetenschappelijk onderzoek plaatsvindt. Dit helpt om bredere ontwikkelingen in de maatschappij te begrijpen en is nodig om de overheid te kunnen informeren in veiligheidsbeleid en politiepraktijk. Helaas staat dergelijk onderzoek nog in de kinderschoenen. Er is weinig bekend over hoe de hybridisatie van criminaliteit zich precies manifesteert, bijvoorbeeld met betrekking tot de rol van de drugshandel en het gebruik van geweld. Ook is het voor een groot deel nog onduidelijk hoe mensen betrokken raken bij online criminaliteit en hoe de verdere criminele carrière van daders van online criminaliteit eruitziet. Op basis van de kennishiaten in de literatuur (Roks et al., 2021; Bekkers et al., 2024; Ruiter et al., 2023) zou toekomstig onderzoek zich kunnen richten op vragen als: Wat kenmerkt de criminele carrière van daders van online criminaliteit en op welke manier spelen traditionele vormen van criminaliteit daarbij een rol? In hoeverre en op welke manier zijn het gebruik van geweld en de drugshandel verweven in de wereld van financieel-economische online criminaliteit? Welke factoren spelen een rol bij de hybridisatie van criminaliteit en wat kenmerkt de daders die zich specialiseren of juist generaliseren in delictgedrag? En wat zijn aanknopingspunten voor een effectieve aanpak van gehybridiseerde vormen van criminaliteit?

LITERATUUR

Adejoh, S. O., Alabi, T. A., Adisa, W. B., & Emezie, N. M. (2019). 'Yahoo boys' phenomenon in Lagos metropolis: A qualitative investigation. *International Journal of Cyber Criminology, 13*(1), 1–20. https://doi.org/10.5281/zenodo.3366298

Adou, E. F. S., & Kolé, M. S. (2020). 'Je suis au bara' or the deviant use of the Internet among Abidjan's scammers. In J. Atchoua, J. Bogui, & S. Diallo (Eds.), *Digital technologies and African societies* (1st ed., pp. 107–126). Wiley. https://doi.org/10.1002/9781119777304.ch6

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643–652.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717–723.

Aiken, M., Davidson, J., & Amann, P. (2016). *Youth pathways into cybercrime.* Europol: European Cybercrime Centre / UCD Geary institute for public policy / Middlesex University.

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers and Security, 132*. https://doi.org/10.1016/j.cose.2023.103352

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

Akkermans, M., Arends, J., Derksen, E., & Reep, C. (2023). Online veiligheid en criminaliteit 2022. *Centraal Bureau voor de Statistiek.* Geraadpleegd van www.cbs.nl/-/media/_pdf/2023/19/online-veiligheid-en-criminaliteit-2022.pdf

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). Veiligheidsmonitor 2023. *Centraal Bureau voor de Statistiek.* Geraadpleegd van https://open.overheid.nl/documenten/dpc-9a9f6b051ff743f1b469040b00d8946351c6f009/pdf

Akyazi, U., Van Eeten, M., & Gañán, C. H. (2021, July). Measuring cybercrime as a service (caas) offerings in a cybercrime forum. In *Workshop on the Economics of Information Security* (pp. 1-15).

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security, 28*(6), 476–490.

Allodi, L., Corradin, M., & Massacci, F. (2016). Then and Now: On the Maturity of the Cybercrime Markets The Lesson That Black-Hat Marketeers Learned. *IEEE Transactions on Emerging Topics in Computing, 4*(1), Article 1. https://doi.org/10.1109/TETC.2015.2397395

Analistennetwerk Nationale Veiligheid. (2023). *Themastudie extremisme.* Geraadpleegd van www.rijksoverheid.nl/documenten/kamerstukken/2023/10/17/tk-bijlage-themastudie-extremisme-analistennetwerk-nationale-veiligheid

Andriessen, M, Van Leuken, M., & Van 't Hoff-de Goede, M. S. (2024). *Jong ICT-talent op het rechte pad houden. Een plan- en procesevaluatie.* De Haagse Hogeschool. Geraadpleegd van www.dehaagsehogeschool.nl/media/jong-ict-talent-op-het-rechte-pad-houden

Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology, 9*(1), 35–54. https://doi.org/10.5281/zenodo.22239

Ask, T. F., Lugo, R. G., Knox, B. J., & Sütterlin, S. (2021). Human-human communication in cyber threat situations: A systematic review. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), *13096 LNCS*, 21–43. https://doi.org/10.1007/978-3-030-90328-2_2

Bachmann, M. (2011). Deciphering the hacker underground: First quantitative insights. In T. J. Holt & B. H. Schell (Eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 105–126). IGI Global. https://doi.org/10.4018/978-1-61692-805-6

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Geraadpleegd van https://arxiv.org/pdf/1901.02672

Bair, J., Bellovin, S. M., Manley, A., Reid, B. E., Shostack, A., & De Vries, J. P. (2017). That was close! Reward Reporting of cybersecurity 'near misses.' *SSRN Electronic Journal, 327.* https://doi.org/10.2139/ssrn.3081216

Bantema, W., & Twickler, S. (2023). Waar mondiale het lokale treft: de APV als instrument in de strijd tegen online aangejaagde ordeverstoringen. *Computerrecht, 65*(2), 118–125.

Bantema, W., Twickler, S., & De Vries, S. (2022). *Juridische grenzen en kansen bij openbare-ordehandhaving: Een onderzoek naar mogelijkheden van de APV voor de aanpak van online aangejaagde ordeverstoringen.* Onderzoeksgroep Cybersafety.

Bantema, W., Twickler, S., Munneke, S., Duchateau, M., & Stol, W. (2018). *Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld.* Sdu Uitgevers.

Bantema, W., Westers, S., & Munneke, S.A.J. (2020). *Niet bevoegd, wel verantwoordelijk? Handhavingsmogelijkheden bij online aangejaagde ordeverstoringen.* Boom bestuurskunde.

Beerthuizen, M. G. C. J., Sipma, T., & Van der Laan, A. M. (2020). *Aard en omvang van dader-en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland.* Den Haag: WODC.

Bekkers, L., & Leukfeldt, E. R. (2022). Recruiting money mules on instagram: A qualitative examination of online involvement mechanisms into cybercrime. *Deviant Behaviour.* https://doi:10.1080/01639625.2022.2073298

Bekkers, L. M., Moneva, A., & Leukfeldt, E. R. (2024a). Understanding cybercrime involvement: A quasi-experiment on engagement with money mule recruitment ads on Instagram. *Journal of Experimental Criminology, 20*(2), 375–394.

Bekkers, L., Van Leuken, M., & Leukfeldt, E. R. (2024b). *Criminele netwerken achter geldezels.* De Haagse Hogeschool. Geraadpleegd van https://hetccv.nl/app/uploads/2024/10/Criminele-netwerken-achter-geldezels-DIGI-versie-kopie.pdf

Bekkers, L., Van der Kleij, R., & Leukfeldt, E.R. (2020). *Verkenning best practices cybersecurity informatiedeling.* De Haagse Hogeschool. Geraadpleegd van www.ncsc.nl/binaries/ncsc/documenten/publicaties/2020/september/23/verkenning-best-practices-cybersecurity-informatiedeling/W2008+0190+Rapport+A4+Lectoraat+Cybersecurity+in+het+mkb.pdf

Bekkers, L., Van der Kleij, R., & Leukfeldt, E. R. (2021). *Cyber-ketenweerbaarheid: Een verkennend onderzoek naar dreigingen, kwetsbaarheden en geleerde lessen.* De Haagse Hogeschool. Geraadpleegd van https://securitydelta.nl/media/com_hsd/report/353/document/rapport-cyber-ketenweerbaarheid-digi.pdf

Bliss, J. P. (1993). *The cry-wolf phenomenon and its effect on alarm responses.* University of Central Florida.

Bluhm, K., Borwell, J., & Stol, W. (2022). De slachtofferimpact van cybercrime versus traditionele criminaliteit: Aanknopingspunten voor slachtofferzorg en preventieprioriteiten. *Tijdschrift voor Veiligheid, 21*(3-4), 13–31. https://doi.org/10.5553/TvV/.000045

Bluhm, K., Andriessen, M., Van De Wal, M., Berkenpas, M., De Boer, D., Leukfeldt, R., Spithoven, R., & Jansen, J. (2024). *Een eerste blik op het verloop en de werking van cyberweerbaarheidsprojecten in Nederland: Procesevaluaties van CCV City Deal projecten Deelrapport 1: Tranche 1 en 2.* Cyberweerbaar NL.

Bonnes, J., & Divendal, O. (2024). Innovatie in het strafrecht: effectieve aanpak van cybercriminaliteit vergt brede bestrijding en verdient betere regulering. *Ars Aequi*, 320–330. AA20240320.

Borwell, J., Jansen, J., & Stol, W. (2021). Comparing the victimization impact of cybercrime and traditional crime: Literature review and future research directions. *Journal of Digital Social Research, 3*(3), 85–110.

Bossler, A. M. (2021). Neutralizing cyber attacks: Techniques of neutralization and willingness to commit cyber attacks. *American Journal of Criminal Justice, 46*(6), 911–934. https://doi.org/10.1007/s12103-021-09654-5

Brandt, R. (2024, 5 december). Evaluatie Melissa: inzichten in de succesvolle (samen)werking rondom bestrijding ransomware. *Kennedy Van Der Laan.* Geraadpleegd van https://kvdl.com/artikelen/evaluatie-melissa-inzichten-in-de-succesvolle-samenwerking-rondom-bestrijding-ransomware

Bras, E. (z.d.) *FERM.* Digital Trust Center (DTC) & Ministerie van Economische Zaken. Geraadpleegd van www.digitaltrustcenter.nl/samenwerkingsverband/ferm

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications.* Springer International Publishing. https://doi.org/10.1007/978-3-030-31069-1

Briggs, P., Jeske, D., & Coventry, L. (2017). The design of messages to improve cybersecurity incident reporting. In *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5* (pp. 3–13). Springer International Publishing

Bronk, C., & Dewitte, P. (2022). Maritime cybersecurity: meeting threats to globalization's great conveyor. In *Cyber Security: Critical Infrastructure Protection* (pp. 241–254). Cham: Springer International Publishing.

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology, 9*(1), 55–119.

Buitenhuis, M. (2022). De burgemeester: burgervader, handhaver van de openbare orde en sheriff van het internet? (deel 1). *Gemeentestem, 44*, 230–238.

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R., & Wang, V. (2022). Assessing the seriousness of cybercrime: The case of computer misuse crime in the United Kingdom and the victims' perspective. *Criminology & Criminal Justice, 25*(2), 670-691. https://doi.org/10.1177/17488958221128128

Bijleveld, C., Salet, R., Damstra, A., & Stéfanovic, D. (2021). *Politiefunctie in een veranderende omgeving.* Wetenschappelijke Raad voor het Regeringsbeleid.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications, 42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Campobasso, M. (2024). *Understanding and Characterizing the Cybercriminal Ecosystem Enabling Attack Innovation at Scale* [Doctoral thesis, Eindhoven University of Technology]. https://pure.tue.nl/ws/portalfiles/portal/320429925/20240307_Campobasso_hf.pdf

CBS. (2023, november 10). Nederlanders digitaal steeds vaardiger. Centraal Bureau voor de Statistiek. Geraadpleegd van www.cbs.nl/nl-nl/nieuws/2023/45/nederlanders-digitaal-steeds-vaardiger

CCV (2023). *Interventies op het gebied van jeugd en cybercrime. Aanzet voor de City Deal innovatie.* Centrum voor Criminaliteitspreventie en Veiligheid. Via: https://hetccv.nl/onderzoek-naar-interventies-jeugd-en-cybercrime-voor-innovatieve-aanpak-in-city-deal/

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. *Computers in Human Behavior*, 108. https://doi.org/10.1016/j.chb.2020.106311

Chon, K. H. (2016). *Cybercrime precursors: Towards a model of offender resources* [PhD Thesis, Australian National University]. http://hdl.handle.net/1885/107344

Chua, Y. T., & Holt, T. J. (2016). A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Victims & Offenders, 11*(4), 534–555. https://doi.org/10.1080/15564886.2015.1121944

Clarke, R. V. (1980). 'Situational' crime prevention: Theory and practice. *The British Journal of Criminology, 20*(2), 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Clarke, R. V. (2017). Situational crime prevention. In R. Wortley & M. Townsley (Eds.), *Environmental criminology and crime analysis* (2nd ed., pp. 1–25). Routledge, Taylor & Francis Group.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. In M. J. Smith & D. B. Cornish (Eds.), *Theory for practice in situational crime prevention* (pp. 41–96). Criminal Justice.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Cross, C. (2018). Denying victim status to online fraud victims: The challenges of being a 'non-ideal victim'. *Revisiting the ideal victim concept*, 243–262.

Cybbar & CSD. (2023*). Cybercrime against businesses in the EU: Challenges to Reporting* [Policy Brief] (pp. 1–4).

Cyber Security Raad. (2022, 24 juni). *CSR Meerjarenstrategie 2022-2025.* Geraadpleegd van www.cybersecurityraad.nl/binaries/cybersecurityraad/documenten/jaarplannen/2022/06/24/csr-meerjarenstrategie-2022-2025/CSR_Meerjarenstrategie_2225_def_webversie.pdf

Daffron, J., Ruffle, S., Coburn, A., Copic, J., Quantrill, K., Strong, K., & Leverett, E. (2019). *Shen attack: Cyber risk in asia pacific ports.* Cambridge Centre for Risk Studies: Cambridge, MA, USA.

Davies, K. (2006). What is effective intervention? – using theories of health promotion. *British Journal of Nursing, 15(*5), 248–251. https://doi.org/10.12968/bjon.2006.15.5.20638

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70*, 72-94.

Deloitte. (2024, 26 april). *Cyberweerbaarheidskloof Aanbevelingen voor een cyberweerbaar mkb en het verkleinen van de cyberweerbaarheidskloof in Nederland.* Geraadpleegd van https://prod1-plate-attachments.s3.amazonaws.com/attachments/fecd9a9ff3/deloitte-nl-risk-cyberweerbaarheid-mkb.pdf

Demirel, B., Koens, L., & Vennekens, A. (2023, april 6). De digitale overheid in kaart? *Rathenau Instituut.* Geraadpleegd van www.rathenau.nl/nl/wetenschap-cijfers/de-digitale-overheid-kaart

De Groot, R.M., Kaal, H.L. & Stol, W. Ph. (2022). The online lives of adolescents with mild or borderline intellectual disabilities in the Netherlands: Care staff knowledge and perceptions. *Journal of Intellectual & Developmental Disability, 47*(2), pp. 1–10. https://doi.org/10.3109/13668250.2021.2004635

De Kimpe, L. (2020). *The Human Face of Cybercrime: Identifying targets, victims, and their coping mechanisms*. Universiteit van Antwerpen/Ghent University.

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., … Martin, R. (2021). A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice, 15*(2), 1429–1445.

Diaz, A., Sherman, A. T., & Joshi, A. (2020). *Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44*(1), 53–67. https://doi.org/10.1080/01611194.2019.1623343

Digital Trust Center. (z.d.). *De 5 basisprincipes van veilig digitaal ondernemen.* Ministerie van Economische Zaken. Geraadpleegd van www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

Ditton, J., & Innes, M. (2005). 'The Role of Perceptual Intervention in the Management of Crime Fear'. In N. Tilly (Ed.), *Handbook of Crime Prevention and Community Safety.* Collumpton: Willan Publishing.

Domenie, M., Leukfeldt, E. R., Van Wilsem, J. A., Jansen, J., & Stol, W. P. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit.* Den Haag: Boom Lemma uitgevers.

Dupont, B. (2019). *The Cyber-Resilience of Financial Institutions: A preliminary working paper on significance and applicability of digital resilience.* Global risk institute.

Durlak, J. A., & DuPre, E. P. (2008). Implementation Matters: A Review of research on the influence of implementation on program outcomes and the factors affecting implementation. *American Journal of Community Psychology, 41*(3-4), 327–350. https://doi.org/10.1007/s10464-008-9165-0

Duymedjian, R., & Rüling, C. C. (2010). Towards a foundation of bricolage in organization and management theory. *Organization studies, 31*(2), 133–151.

Ebbers, S., Koch, J., Jansen, J., Groenendaal, J., Bantema, W., & Leukfeldt, R. (2021). *Cybercrsis bij gemeenten: Een verkennend onderzoek naar de voorbereidingen, ervaringen en uitdagingen.* NHL Stenden Hogeschool & De Haagste Hogeschool.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. In *Computers and Security* (Vol. 134). Elsevier Ltd. https://doi.org/10.1016/j.cose.2023.103435

Ebot, T. A. (2017). *Explaining two forms of Internet crime from two perspectives: Toward stage theories for phishing and Internet scamming* [PhD Thesis, University of Jyväskylä]. http://urn.fi/URN:ISBN:978-951-39-6954-7

Eldredge, L. K. B., Markham, C. M., Ruiter, R. A., Fernández, M. E., Kok, G., & Parcel, G. S. (2016). *Planning health promotion programs: an intervention mapping approach.* John Wiley & Sons.

Emmen, B., De Poot, C. J., & Stol, W. Ph. (2023). Politieoptreden op het darkweb. *Tijdschrift voor de Politie, 85*(2), 32–35.

Eurobarometer (2022). *SMEs and Cybercrime.* Flash Eurobarometer 496. https://europa.eu/eurobarometer/surveys/detail/2280

European Commission. (2022). *Flash Eurobarometer 496—SMEs and cybercrime.* https://doi.org/10.2837/89101

Europese Raad & Raad van Europa. (2024, 10 juni). *Cyberbeveiliging: EU-aanpak van cyberdreigingen.* Geraadpleegd van www.consilium.europa.eu/nl/policies/cybersecurity/

Europol. (2014). *IOCTA 2014: Internet Organised Crime Threat Assessment 2014.* Europol. Geraadpleegd van www.europol.europa.eu/cms/sites/default/files/documents/europol_iocta_web.pdf

Fattah, E. (1993). Research on Fear of Crime. Some Common Conceptual and Measurement Problems. In W. Bilsky, C. Pfeiffer & P. Wetzels (Eds.), *Fear of Crime and Criminal Victimization* (pp. 45–70). Stuttgart: Enke.

FERM Rotterdam. (z.d.). *Wat is FERM?* Geraadpleegd van https://ferm-rotterdam.nl/wat-is-ferm/

Feth, D., & Polst, S. (2019). Heuristics and models for evaluating the usability of security measures. In *Proceedings of Mensch und Computer 2019* (pp. 275–285).

Fox, J. (2016). The dark side of social networking sites in romantic relationships. In B. K. Wiederhold, G. Riva & P. Cipresso (Eds.), *The psychology of social networking: Communication, presence, identity, and relationships in online communities* (pp. 78-86) Berlin: DeGruyter Open.

Fox, B., & Holt, T. J. (2021). Use of a multitheoretic model to understand and classify juvenile computer hacking behavior. *Criminal Justice and Behavior, 48*(7), 943–963. https://doi.org/10.1177/0093854820969754

Furnell, S. (2005). Why users cannot use security. *Computers & Security,24*(4), 274–279.

Gnoni, M. G., Tornese, F., Guglielmi, A., Pellicci, M., Campo, G., & De Merich, D. (2022). Near miss management systems in the industrial sector: A literature review. In *Safety Science* (Vol. 150). Elsevier B.V. https://doi.org/10.1016/j.ssci.2022.105704

Goudriaan, H. (2006). *Reporting crime: Effects of social context on the decision of victims to notify the police*. Universiteit Leiden.

Graham, A., Kulig, T. C., & Cullen, F. T. (2020). Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing, 43*(1), 1–16. https://doi.org/10.1108/PIJPSM-07-2019-0115

Greenberg, M. S., & Ruback, R. B. (1992). *After the Crime* (Vol. 9). Springer US. https://doi.org/10.1007/978-1-4615-3334-4

Griffin, R. J., Dunwoody, S., Dybro, T., & Zabala, F. (1994). The relationship of communication to risk perceptions and preventive behavior related to lead in drinking water. In *Science Communication Interest Group, Association for Education in Journalism and Mass Communication, at the 1994 annual convention*. Atlanta, GA.

Griffin, R. J., Dunwoody, S., & Neuwirth, K. (1999). Proposed model of the relationship of risk information seeking and processing to the development of preventive behaviors. *Environmental research, 80*(2), S230–S245. Hale, 1996.

Griffin, R. J., Dunwoody, S., & Zabala, F. (1998). Public reliance on risk communication channels in the wake of a cryptosporidium outbreak. *Risk Analysis, 18*(4), 367–375.

Guerra, C., & Ingram, J. R. (2020). Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior*, 1–17. https://doi.org/10.1080/01639625.2020.1774707

Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: A review of situational crime prevention

evaluations. *Criminology, 47*(4), 1331–1368. https://doi.org/10.1111/j.1745-9125.2009.00177.x

Harsch, A., Idler, S., & Thurner, S. (2014, May). Assuming a state of compromise: A best practise approach for SMEs on incident response management. In *2014 Eighth International Conference on IT Security Incident Management & IT Forensics* (pp. 76-84). IEEE.

Hartel, P. H., Junger, M., & Wieringa, R. J. (2010). *Cyber-crime Science = Crime Science + Information Security* (CTIT Technical Report Series; No. 10-34). Centre for Telematics and Information Technology (CTIT).

Hartholt, S. (2023, januari 23). Overheids-ict valt 1,3 miljard duurder uit. *Binnenlandsbestuur.nl.* Geraadpleegd van www.binnenlandsbestuur.nl/digitaal/overheids-ict-valt-opnieuw-13-miljard-duurder-uit

Hielscher, J., Menges, U., Parkin, S., Kluge, A., & Sasse, A. (2023). *'Employees who don't accept the time security takes are not aware enough': The CISO view of human-centred security.* www.usenix.org/system/files/sec23fall-prepub-110-hielscher.pdf

Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security, 115*, 102611. https://doi.org/10.1016/j.cose.2022.102611

Hof, T., Van der Kleij, R., & Mergler, S. (2024). Veilig digitaal ondernemen: Inzicht in motivaties en barrières door doelgroepsegmentatie. *TNO.* Den Haag. https://resolver.tno.nl/uuid:482ca8d1-ddcb-475e-b525-2d014c7f1c4b

Hollis, V., & Tsaousi, E. (2018). Digital Literacy and Cybersecurity: Integrating Cyber Awareness in Education. *Education and Information Technologies, 23*(3), 1249–1265.

Hollnagel, E. (2011). RAG – The resilience analysis grid. In E. Hollnagel, J. Pariès, D. D. Woods & J. Wreathall (Eds.), *Resilience Engineering in Practice. A Guidebook*. Farnham, UK: Ashgate.

Hollnagel, E. (2014). Resilience engineering and the built environment. *Building Research & Information, 42*(2), 221–228.

Holt, T. J., Cale, J., Brewer, R., & Goldsmith, A. (2021). Assessing the role of opportunity and low self-control in juvenile hacking. *Crime & Delinquency, 67*(5), 662–688. https://doi.org/10.1177/0011128720978730

Holt, T. J., Navarro, J. N., & Clevenger, S. (2020a). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime & Delinquency, 66*(11), 1533–1555. https://doi.org/10.1177/0011128719875697

Holt, T. J., & Steinmetz, K. F. (2021). Examining the role of power-control theory and self-control to account for computer hacking. *Crime & Delinquency, 67*(10), 1491–1512. https://doi.org/10.1177/0011128720981892

Holt, T. J., Van Wilsem, J., Van de Weijer, S., & Leukfeldt, R. (2020b). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review, 38*(2), 187–206.

Huang, K., Siegel, M., & Madnick, S. (2017). *Cybercrime-as-a-Service: Identifying Control Points to Disrupt* [Technical Report]. Massachusetts Institute of Technology (MIT).

Hutchings, A. (2013). *Theory and crime: Does it compute?* [PhD Thesis, Griffith University]. https://research-repository.griffith.edu.au/handle/10072/365227

Hutchings, A. (2014). Crime from the keyboard: Organised cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law and Social Change, 62*(1), 1–20. https://doi.org/10.1007/s10611-014-9520-z

Hyslip, T. S. (2020). Cybercrime-as-a-Service Operations. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 815–846). Springer International Publishing. https://doi.org/10.1007/978-3-319-78440-3_36

IBM Security. (2019). *Cost of a Data Breach Report 2019*. Ponemon Institute & IBM Security. Geraadpleegd van https://insights.integrity360.com/hubfs/2019-cost-of-a-data-breach-report-04_03025203USEN.pdf

Ibrahim, S. (2016, June). Causes of socioeconomic cybercrime in Nigeria. In *2016 IEEE international conference on cybercrime and computer forensic (ICCCF)* (pp. 1-9). IEEE.

Inspectie Veiligheid en Justitie (2015). *Aanpak van internetoplichting door de politie. Inspectieonderzoek naar een vorm van cybercrime.* Ministerie van Justitie en Veiligheid. Geraadpleegd van https://cyberwar.nl/d/20150401_Inspectierapport-Aanpak-van-internetoplichting-door-de-politie.pdf

International Telecommunication Union. (2020). *Cybersecurity for Youth: Guidance for Education and Training.* Geneva: ITU.

Jackson, J., & Gray, E. (2010). Functional Fear and Public Insecurities about Crime. *British Journal of Criminology, 50*(1), 1–21.

Jacobs, W., & Paardenkoper, J. (2023, 16 maart). *Digital Trust Center (DTC) Benchmark onderzoek*. Digital Trust Center (DTC). Geraadpleegd van www.digitaltrustcenter.nl/sites/default/files/2023-05/Rapportage_DTC_Benchmark_CyberVeiligCheck.pdf

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience.* [Doctoral Thesis]. Open Universiteit. Geraadpleegd van https://research.ou.nl/files/9260429/2018_Proefschrift_Jansen.pdf

Jansen, J. (2023). *Digitale weerbaarheid van mens en organisatie: De kracht van verbinding.* Onderzoeksgroep Cybersafety. Geraadpleegd van https://api.publinova.nl/api/products/ae7f3865-09a2-4b48-b31b-69f46ad40ece/download/0d08840a-6f09-42c4-ac8d-aadb41b46e88

Jansen, J., & Leukfeldt, R. (2015). *How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases. In Proceedings* - 5th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2015 (pp. 24–31). https://doi.org/10.1109/STAST.2015.12

Jansen, J., Westers, S., Twickler, S., & Stol, W. Ph. (2019). *Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing.* Sdu Uitgevers (reeks Politie en Wetenschap).

Jones, S., Kirchsteiger, C., & Bjerke, W. (1999). The importance of near miss reporting to further improve safety performance. *Journal of Loss Prevention in the Process Industries, 12*(1), 59–67. https://doi.org/10.1016/S0950-4230(98)00038-2

Kaspersky. (2023). *Kaspersky Incident Response 2023.* Geraadpleegd van https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2024/05/13125640/Kaspersky-IR_Analyst_report_2023_EN.pdf

Kaur, M., Van Eeten, M., Janssen, M., Borgolte, K., & Fiebig, T. (2021). *Human factors in security research: Lessons learned from 2008-2018*. arXiv preprint arXiv:2103.13287.

Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2023). When do businesses report cybercrime? Findings from a UK study. *Criminology & Criminal Justice, 23*(3), 468–489. https://doi.org/10.1177/17488958211062359

Kessler, G. C., & Shepard, S. D. (2020). *Maritime cybersecurity: a guide for leaders and managers*, 2nd. ed.

KIA. (2023, 31 oktober). *Kennis- en Innovatie Agenda VEILIGHEID 2024-2027*. Holland High Tech. Geraadpleegd van https://hollandhightech.nl/_asset/_public/Documenten/KIA-Veiligheid-2024-2027-311020.pdf

Kievik, M. (2017). The time of telling tales: *The determinants of effective risk communication* [PhD-thesis]. Twente University .

Kop, N. (2012). *Van opsporing naar criminaliteitsbeheersing. Vijf strategische implicaties.* Politieacademie.

Krauwer, J. (2023, 27 juni). *Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker.* ABN AMRO. Geraadpleegd van www.abnamro.nl/nl/media/202404_Steeds-verfijndere-cyberaanvallen_tcm16-228031.pdf

Kroes, P., Ter Veen, H., & Kop, N. (2023). *Bundel krachten en vier successen: Zes jaar onderzoek naar innovatie binnen de Nederlandse politie*. Politieacademie.

Landelijk Kenniscentrum LVB (z.d.). *Dossier LVB & Criminaliteit.* www.kenniscentrumlvb.nl/themas/risicos-lvb/dossier-criminaliteit-lvb

Lazarus, R. S., & Folkman, S. (1984). *Stress, Appraisal, and Coping*. New York, NY: Springer.

Lee, J. R., & Holt, T. J. (2020). Assessing the factors associated with the detection of juvenile hacking behaviors. *Frontiers in Psychology, 11*, 1–10. https://doi.org/10.3389/fpsyg.2020.00840

Lee, J. M. Y., & Wong, E. Y. C. (2021). Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain. In *MATEC web of conferences* (Vol. 339,). EDP Sciences.

Leppänen, A., Toiviainen, T., & Kankaanranta, T. (2020). From a vulnerability search to a criminal case: Script analysis of an SQL injection attack. *International Journal of Cyber Criminology, 14*(1), 63–80. https://doi.org/10.5281/zenodo.3740361

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017) Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology.* DOI:10.1093/bjc/azw009.

Leukfeldt, E.R., Kleemans, E.R. & Stol, E.R. (2017) Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime, Law and Social Change.* DOI: 10.1007/s10611-016-9647-1.

Leukfeldt, E.R., Kleemans, E.R. & Stol, W.P. (2017) A typology of cybercriminal networks: From low tech locals to high tech specialists. *Crime, Law and Social Change*. DOI: 10.1007/s10611-016-9646-2.

Leukfeldt, E.R., Lavorgna A. & Kleemans E.R. (2017) Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. European Journal on Criminal Policy and Research. *23*(3) 287-300.

Leukfeldt, E. R., & Holt, T. J. (2022). Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals. *Computers in Human Behavior, 126,* 106979.

Leukfeldt, E.R., & Kleemans E.R. (2019). Cybercrime, money mules and situational crime prevention. In S. Hufnagel & A. Moiseienko (Eds.), *Criminal Networks and Law Enforcement: Global Perspectives on Illicit Enterprise*. London: Routledge.

Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime, 22*, 324–345.

Leukfeldt, E. R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. WODC.

Leukfeldt, E.R., R.J. Notté, & M. Malsch (2019b). Exploring the needs of victims of cyber-dependent and cyber-enabled crime, *Victims and Offenders 2019, 15*(1), p. 60–77.

Leukfeldt, E. R., Spithoven, R., & Misana-ter Huurne, E. F. J. (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In C. de Poot et al. (Eds.), *Politie en cybercriminaliteit* (pp. 203–222). Gompel&Scavina.

Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and Human Factors of Malware Attacks. *ACM Transactions on Privacy and Security, 21*(4), 1–30. https://doi.org/10.1145/3210311

Levi-Strauss, C. (1966). *The savage mind.* University of Chicago Press.

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). Risky Experiences for Children Online: Charting European Children's Internet Use. *EU Kids Online.*

Loggen, J., & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. *Trends in Organized Crime, 25*(2), 205–225.

Loggen, J., Moneva, A., & Leukfeldt, R. (2024a). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. *Computer Law & Security Review, 52*, 105858. https://doi.org/10.1016/j.clsr.2023.105858

Loggen, J., Moneva, A., & Leukfeldt, R (2024b). Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. *Victims & Offenders*. https://doi.org/10.1080/15564886.2024.2370295

Longo, M. (2018). Exploring the subtle mental boundary between the real and the virtual. In A. Marzi (Ed.), *Psychoanalysis, Identity, and the Internet* (pp. 51–74). Routledge.

Loomis, W., Singh, V. V., Kessler, G. C., & Bellekens, X. (2021). *Raising the colors: Signaling for cooperation on maritime cybersecurity.* Atlantic Council.

Maiman, L. A., & Becker, M. H. (1974). The health belief model: Origins and correlates in psychological theory. *Health education monographs, 2*(4), 336–353.

Malsch, M., Dijkman, N., & Akkermans, A.J. (2015). *Het zichtbare slachtoffer: privacy van slachtoffers binnen het strafproces*. Den Haag: WODC.

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud & Security, 2013(*6), 9–13. https://doi.org/10.1016/S1361-3723(13)70053-8

Maple, C., Short, E., & Brown, A. (2011). *Cyberstalking in the United Kingdom: An analysis of the ECHO pilot survey.* University of Bedfordshire.

Mathews, L. (2017). *NotPetya ransomware attack cost shipping giant Maersk over $200 million*. Forbes, Aug, 16.

Matthijsse, S., Van 't Hoff-de Goede, S., & Leukfeldt, R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organised Crime*, 1–27.

Matthijsse, S. R., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2024). Onderhandelen, betalen en melden na slachtofferschap van ransomware: Een mixed methods onderzoek naar de factoren die bijdragen aan beslissingsgedrag van burgers en ondernemers. *Politie & Wetenschap.*

MBO digitaal (z.d.). *Cyberrisicopooling.* Geraadpleegd op https://mbodigitaal.nl/programmas/programma-cyberveiligheid-mbo/incidenten-herstellen/cyberrisicopooling/

McAlaney, J., Hambidge, S., Kimpton, E., & Thackray, H. (2020). Knowledge is power: An analysis of discussions on hacking forums. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 477–483. https://doi.org/10.1109/EuroSPW51379.2020.00070

McBrayer, J. (2014). *Exploiting the digital frontier: Hacker typology and motivation* [Master's Thesis]. The University of Alabama.

Mesch, G. S., & Dodel, M. (2018). Low Self-Control, Information Disclosure, and the Risk of Online Fraud. *American Behavioral Scientist, 62*(10), 1356–1371.

Michie, S, Atkins, L., & West, R. (2014). *The Behaviour Change Wheel: A guide to designing interventions.* Silverback Publishing.

Michie, S., Atkins, L., & West, R. (2018). *Het gedragsveranderingswiel: 8 stappen naar succesvolle interventies.* Amsterdam University Press.

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*, 1-12.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H. J. (2020). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology.* https://doi.org/10.1177/0306624X20981041

Ministerie van Economische Zaken en Klimaat. (2022, november). Strategie Digitale Economie: Werken aan een weerbare en welvarende digitale economie. Geraadpleegd van https://open.overheid.nl/documenten/ronl-c6a3495a523bef54ca41011f629b77b7b611045f/pdf

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Morgan, P. L., Asquith, P. M., Bishop, L. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). A new hope: Human-centric cybersecurity research embedded within organizations. *Lecture Notes in Computer Science, 12210*, 206–216. https://doi.org/10.1007/978-3-030-50309-3_14

Morris, R. G., & Blackburn, A. G. (2009). Cracking the code: an empirical exploration of social learning theory and computer crime. *Journal of Crime and Justice, 32*(1), 1–34. https://doi.org/10.1080/0735648X.2009.9721260

Munksgaard, R. (2024). Marketness and Governance: A Typology of Illicit Online Markets. *Deviant Behavior*, 1–18. https://doi.org/10.1080/01639625.2024.2323526

Näsi, M., Danielsson, P., & Kaakinen, M. (2021). Cybercrime Victimisation and Polyvictimisation in Finland – Prevalence and Risk Factors. *European Journal on Criminal Policy and Research.* https://doi.org/10.1007/s10610-021-09497-0

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) (2022). *Nederlandse Cybersecuritystrategie 2022-2028.* Ministerie van Justitie en Veiligheid. Geraadpleegd van https://open.overheid.nl/documenten/ronl-82f59d66894e136f786c3a34e62d1ce52d26b1c8/pdf

Nationale Coördinator Terrorismestrijding en Veiligheid (NCTV) (2023). *Cybersecuritybeeld Nederland 2023.* Ministerie van Justitie en Veiligheid. Geraadpleegd van www.nctv.nl/binaries/nctv/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023/CSBN2023.pdf

Nationaal Cyber Security Centrum (NCSC). (2021). *Het NCSC en dreigingsinformatie.* Geraadpleegd van www.Ncsc.Nl/Actueel/Weblog/Weblog/2021/Het-Ncsc-En-Dreigingsinformatie

Nationaal Cyber Security Centrum (NCSC). (2022). *NCSC Onderzoeksagenda 2023-2026.* Geraadpleegd van www.ncsc.nl/documenten/publicaties/2022/oktober/11/ncsc-onderzoeksagenda-2023---2026

Nationaal Cyber Security Centrum (NCSC). (2024a). *Detectie in cybersecurity.* Geraadpleegd van www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/detecteren/detectie-in-cybersecurity

Nationaal Cyber Security Centrum (NCSC). (2024b). *Forensics.* Geraadpleegd van www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/reageren/forensics

National Crime Agency. (2017). Pathways into cyber crime (0325-CYB v1.0; p. 18). National Crime Agency. www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file

Nazzari, M. (2023). From payday to payoff: Exploring the money laundering strategies of cybercriminals. *Trends Organ Crim*e, 1–18. https://doi.org/10.1007/s12117-023-09505-1

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery: Preventing e-commerce crime.* Willan.

Northwave (2022). *After the crisis comes the blow. The mental impact of ransomware attacks*. Opgevraagd via www.persberichten.com/Bestanden/Bedrijven/6375/bijlages/Northwave%20Research%20-%20After%20the%20crisis%20comes%20the%20blow%20-%20The%20mental%20impact%20of%20ransomware%20attacks.pdf

Notté, R., Leukfeldt., E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology, 27*(3), 272–294. https://doi.org/10.1177/02697580211010692

Notté, R. J., Slot, L. K., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2019). *Cybersecurity in het MKB. Nulmeting.* De Haagse Hogeschool, lectoraat Cybersecurity in het MKB.

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2020). Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria. *International Journal of Cyber Criminology, 13*(2), 309–325. https://doi.org/10.5281/ZENODO.3702333

Omlo, J., Bool, M., & Rensen, P. (2013). *Weten wat werkt: Passend evaluatieonderzoek in het sociale domein.* SWP Uitgeverij.

Ooyen-Houben, M. M. J., & Leeuw, F. L. (2010). *Evaluatie van justitiële (beleids)interventies.* WODC. Geraadpleegd van https://repository.wodc.nl/bitstream/handle/20.500.12832/888/memorandum2010-2-volledige-tekst-nieuw_tcm28-78177.pdf?sequence=1&isAllowed=y

Openbaar Ministerie (OM) & Politie (2024). *Cybercrime Beeld Nederland 2024*. Geraadpleegd van www.politie.nl/nieuws/2024/juni/11/00-om-en-politie-brede-bestrijding-cybercrime-door-wereldwijde-omvang-en-dreiging-belangrijker-dan-ooit.html

Ovelgönne, M., Dumitras, T., Prakash, B. A., Subrahmanian, V. S., & Wang, B. (2017). Understanding the Relationship between Human Behavior and Susceptibility to Cyber Attacks. *ACM Transactions on Intelligent Systems and Technology, 8*(4), 1–25. https://doi.org/10.1145/2890509

Parry, D. A., Davidson, B. I., Sewall, C. J. R., Fisher, J. T., Mieczkowski, H., & Quintana, D. S. (2021). A systematic review and meta-analysis of discrepancies between logged and self-reported digital media use. *Nature Human Behaviour.* https://doi.org/10.1038/s41562-021-01117-5

Partin, R. D., Meldrum, R. C., Lehmann, P. S., Back, S., & Trucco, E. M. (2021). Low Self-Control and Cybercrime Victimization: An Examination of Indirect Effects Through Risky Online Behavior. *Crime and Delinquency, 68*(13–14), 2476–2502.

Passchier, R. (2021) *Artificiële intelligentie en de rechtsstaat. Over verschuivende overheidsmacht, Big Tech en de noodzaak van constitutioneel onderhoud.* Boom.

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security, 132*, 103309. https://doi.org/10.1016/j.cose.2023.103309

Patterson, C. M., Nurse, J. R., & Franqueira, V. N. (2024). 'I don't think we're there yet': The practices and challenges of organisational learning from cyber security incidents. *Computers & Security, 139*, 103699.

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding motivations and characteristics of financially-motivated cybercriminals* (p. 23). Bristol Cyber Security Group, University of Bristol. https://arxiv.org/abs/2203.08642

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Sciences, 2*(2), 379–398. https://doi.org/10.3390/forensicsci2020028

Politie. (z.d.). *Doel en werkwijze No More Leaks.* Geraadpleegd van www.politie.nl/informatie/doel-en-werkwijze-no-more-leaks.html

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work, 24*(2), 371-390.

Rani, M. I., Nazri, S. N. F., & Zolkaflil, S. (2024). A systematic literature review of money mule: Its roles, recruitment and awareness. *Journal of Financial Crime, 31*(2), 347–361.

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open, 11*(1), 21582440211000049.

Reid, J. (2024, March 28). *Baltimore disaster may be the largest-ever marine insurance payout, Lloyd's boss says.* CNBC.com. Geraadpleegd van www.cnbc.com/2024/03/28/baltimore-disaster-may-be-largest-ever-marine-insurance-payout-lloyds-.html

Richards, K., & Cross, C. (2018). Online fraud victims' experiences of participating in qualitative interviews. *Criminal Justice Studies, 31*(1), 95–111. https://doi.org/10.1080/1478601X.2017.1396217

Richet, J. L. (2017). How to become a cybercriminal? An explanation of cybercrime diffusion. In M. Khosrow-Pour (Ed.), *The dark web: Breakthroughs in research and practice* (pp. 51–63). IGI Global. https://doi.org/10.4018/978-1-5225-3163-0.ch004

Rijksoverheid. (2022, april 22). *Kabinetsbeleid Digitalisering - Digitale Overheid.* Geraadpleegd van www.digitaleoverheid.nl/kabinetsbeleid-digitalisering/

Rijksoverheid. (2023, 3 april). *Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023-2029.* Geraadpleegd van www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden/Veiligheidsstrategie+voor+het+Koninkrijk+der+Nederlanden.pdf

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty (Eds.), *Social Psychophysiology: a source book* (pp. 153-176). Guilford Press.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of health behavior research 1: Personal and social determinants* (pp. 113-132). New York, NY, US: Plenum Press.

Roks, R. A., Leukfeldt, E. R., & Densley, J. A. (2021). The hybridization of street offending in the Netherlands. *The British Journal of Criminology, 61*(4), 926–945. https://doi.org/10.1093/bjc/azaa091

Roks, R., & Monshouwer, N. (2020). F-gamers die 'mapsen', 'swipen' en 'bonken': Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële verkenningen, 46*(2), 44–58. https://doi.org/10.5553/JV/016758502020046002004

Ruiter, S., Van Leuken, M., Van Ruitenburg, T., Schiks, J., & Leukfeldt, E. R. (2023). *In- en doorstroom van cybercriminaliteit in de strafrechtketen.* Den Haag: WODC.

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security, 28*(3), 467–483.

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing secure systems that people can use* (pp. 13–30). O'Reilly: Sebastopol, US.

Schiks, J. A. M., Hansen, S., Foppen, E., Leukfeldt, E. R., & Spithoven, R. (2021b). *HackShield in Noord-Holland. Een evaluatie van de implementatie en resultaten van HackShield in Nood-Hollandse gemeenten.* De Haagse Hogeschool. Geraadpleegd van https://hetccv.nl/app/uploads/2023/09/Rapportage_HackShield_in_Noord-Holland_HHs_Saxion.pdf

Schiks, J. A. M., Van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2021a). *Een alternatief voor jeugdige hackers. Plan- en procesevaluatie van Hack_Right.* Den Haag: Sdu Uitgevers.

Schiks, J., Van 't Hoff-de Goede, S., & Leukfeldt, R. (2022). Op zoek naar de parels bij de lokale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit: een verkennend onderzoek. *Politie & Wetenschap, 89*.

Schwab, K. (2024). The Fourth Industrial Revolution: what it means, how to respond. In Simsek, Z., Heavey, C., & Fox, B. C. (Eds.) *Handbook of research on strategic leadership in the Fourth Industrial Revolution (*pp. 29–34). Edward Elgar Publishing.

Seiler-Hwang, S., Arias-Cabarcos, P., Marín, A., Almenares, F., Díaz-Sánchez, D., & Becker, C. (2019, November). 'I don't see why I would ever want to use it': Analyzing the Usability of Popular Smartphone Password Managers. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1937-1953).Sundar, S. (2020, June 30). Nudging towards a Secure Containerised Environment. TechBlog. https://medium.com/axel-springer-tech/nu dging-towards-a-secure-containerised-environment-f4d6c08a253

Sellers, M. (2017). Don't Give Them the Finger: Why Passwords Are More Secure Than TouchID. *Cryptography.* https://derekbruff.org/blogs/fywscrypto/practical-crypto/dont-give-them-the-finger-why-passwords-are-more-secure-than-touchid/

Sharif, M., Urakawa, J., Christin, N., Kubota, A., & Yamada, A. (2018). Predicting impending exposure to malicious content from user behavior. *Proceedings of the ACM Conference on Computer and Communications Security,* 1487–1501.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373–382).

Shepperd, J. A., Waters, E., Klein, W. M. P., & Weinstein, N. D. (2013). A primer on unrealistic optimism. Current Directions. *Psychological Science, 24*, 232–237.

Sheridan, L. P., & Grant, T. (2007). Is cyberstalking different? *Psychology, Crime & Law, 13*(6), 627–640. https://doi.org/10.1080/10683160701340528

Short, E., Linford, S., Wheatcroft, J. M., & Maple, C. (2014). The impact of cyberstalking: The lived experience-a thematic analysis. *Studies in health technology and informatics, 199*(1), 133–137.

Skogan, W. G. (1984). Reporting Crimes to the Police: The Status of World Research. *Journal of Research in Crime and Delinquency, 21*(2), 113–137.

Sligo, F. X., & Jameson, A. M. (2000). The knowledge-behavior gap in use of health information. *Journal of the American Society for Information Science, 51*(9), 858–869.

SLO (2024). *Conceptkerndoelen digitale geletterdheid en toelichtingsdocument.* Amersfoort: SLO. Geraadpleegd van www.slo.nl/publish/pages/21532/slo_conceptkerndoelen_en_toelichtingsdocument_digitale_geletterdheid_opleverversie_dd-29-2-2024-.pdf

Sondorp, E., Torregrosa, L., Höing, M., & Te Mebel, K. (2019). *Procesevaluatie pilot HALT-interventie.* WODC. Geraadpleegd van https://repository.wodc.nl/bitstream/handle/20.500.12832/2396/2908_Volledige_Tekst_tcm28-388709.pdf?sequence=2&isAllowed=y

Spithoven, R. (2017). *Keeping trouble at a safe distance. Unravelling the significance of 'the fear crime'*. Eleven International Publishing.
Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society.* Boom Criminologie.
Spithoven, R., Jansen, J., Verweijen, B., & Ebbers, S. (2024). *Mensgerichte cyberweerbaarheid: Een praktische uitwerking van het 'human-as-solution'-paradigma.* Cyberweerbaar NL, Hogeschool Saxion, NHL Stenden Hogeschool & Politieacademie. http://dx.doi.org/10.13140/RG.2.2.21474.24002
Spithoven, R., & Leukfeldt, E. R. (2023). Gemeenten lijden aan digitale koudwatervrees. In: *Secondant* (27 maart 2023). Geraadpleegd op https://hetccv.nl/secondant-gemeenten-lijden-aan-digitale-koudwatervrees/
Spithoven, R., Leukfeldt, R., Misana-ter Huurne, E., Van 't Hoff-de Goede, S., Van Houten, Y., Bekkers, L., Foppen, E., & Te Bos, J. (2022). *Cyberweerbaarheid – een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime.* Hogeschool Saxion, De Haagse Hogeschool & NSCR. Geraadpleegd van www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/cyberweerbaarheid---eindrapport---werkpakket-5.pdf
Spithoven, R., & Van Tuijl, C. (Red.) (2024). *Cyberpesten: Theorie over en onderzoek naar de onbegrensde, digitale leefwereld van kinderen en adolescenten in Nederland*. Boom.
Spruit, M., Oosting, D., & Kreffer, C. (2024). Factors that influence secure behaviour while using mobile digital devices. *Information & Computer Security, 32*(5), 729–747.
Staats, W., Meerts, C., Kleemans, E. R., & Huisman, W. (2021). *Nieuwe manieren van samenwerken: Een systematische literatuurreview naar (de effectiviteit van) publiek-private samenwerkingsverbanden op het gebied van financieel-economische criminaliteit en cybercrime*. Vrije Universiteit Amsterdam.
Steinmetz, K. F. (2015). Becoming a Hacker: Demographic Characteristics and Developmental Factors. *Journal of Qualitative Criminal Justice & Criminology, 3(*1), 1–29. https://doi.org/10.21428/88de04a1.af131ffc
Steur, J., Van der Vorst, T., Van Wijk, A., Driesse, M., & Sahebali, W. (2019). *Mogelijkheden voor het aanpakken van kinderporno op basis van bestuursrechtelijke handhaving*. Bureau Beke. https://content.dialogic.nl/wp-content/uploads/2019/07/Dialogic-Mogelijkheden-van-overheidshandelen-aanpak-kinderporno.pdf
Stol, W., & Bantema, W. (2019). De gemeente en de digitaal veilige stad. In J.W. Sap & E. Kolthoff (Red.), *De veilige stad als collectief doel* (pp. 123-130). Nijmegen: Ars Aequi Libri.
Stol, W., & Bantema, W. (2020). Stadsbestuur en digitale veiligheid. Een analyse van beleidsplannen. In M. Malsch & J. W. Sap (Red.), *Orde en verwarring in de stad* (pp. 363-385). Den Haag: Boom Criminologe.
Stol, W., Jansen, J., & Landman, W. (2024). Digitalisering en de politiefunctie: hoe het speelveld verandert en wat dat van de politie vraagt. *Tijdschrift voor Veiligheid, 23*(1-2), 52–69. https://doi.org/10.5553/TvV/.000071
Stol, W. Ph., Kaspersen, H. W. K., Kerstens, J., Leukfeldt, E. R., & Lodder, A. R. (2009). Governmental Filtering of Websites: The Dutch Case. *Computer Law & Security Report, 25*, 251–262.
Stroebe, W., Van Koningsbruggen, G. M., Papies, E. K., & Aarts, H. (2013). Why most dieters fail but some succeed: A goal conflict model of eating behavior. *Psychological Review, 120*(1), 110.
Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 147–164.

Ter Huurne, E. F. J. (2008). *Information seeking in a risky world: the theoretical and empirical development of FRIS: a Framework of Risk Information Seeking.* University of Twente.

Treadway, K. N. (2017). *Comparing the cognitive abilities of hackers and non-hackers using a self report questionnaire* [Master's Thesis]. Purdue University.

Tsaousi, E., Hollis, V., & Van der Veen, C. (2022). The Role of Teachers in Cybersecurity Education: Challenges and Opportunities. *Computers & Education, 186,* 104–115.

Twickler, S., De Boer, D., & Bantema, W. (2024). *Vergunningverlening en digitale veiligheid van bedrijven: een verkenning van lokale handelingsperspectieven*. Onderzoeksgroep Cybersafety: Leeuwarden.

Van Balkom, J. (2022, 23 februari). Zorg voor kwetsbare geldezels. *Tijdschrift voor de Politie.* www.websitevoordepolitie.nl/zorg-voor-kwetsbare-geldezels/

Van de Weijer, S. G. A. (2019). Predictors of Cybercrime Victimization: Causal Effects or Biased Associations? In E. R. Leukfeldt & T. J. Holt (Eds.), *The human factor of cybercrime* (pp. 83–110). Eleven international publishing.

Van de Weijer, S., & Leukfeldt, E. R. (2020). Slachtoffer van onlinecriminaliteit, wat nu?: Een onderzoek naar aangiftebereidheid onder burgers en ondernemers. *Politie en Wetenschap,* 120.

Van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology, 16*(4), 486–508. https://doi.org/10.1177/1477370818773610

Van de Weijer, S. G. A., Leukfeldt, E. R., & Van der Zee, S. (2020). *Slachtoffer van online criminaliteit, wat nu? Een onderzoek naar de aangiftebereidheid onder burgers en ondernemers.* SDU Uitgevers. www.politieenwetenschap.nl/publicatie/politiewetenschap/2020/slachtoffer-van-onlinecriminaliteit-wat-nu-356/

Van de Weijer, S. G. A., Leukfeldt, E. R., & Van der Zee, S. (2021). *Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands* (pp. 303–325). https://doi.org/10.1007/978-3-030-60527-8_17

Van den Eeden, C. A. J., Van Berkel, J. J., Lankhaar, C. C., & De Poot, C. J. (2021). *Opsporen, vervolgen en tegenhouden van cybercriminaliteit.* WODC. Geraadpleegd van https://repository.wodc.nl/bitstream/handle/20.500.12832/3114/Cahier%202021-23-volledige%20tekst-nw.pdf?sequence=7&isAllowed=y

Van der Berg, B. Weggemans, D., & Nobbenhuis, M. (2024). *Samenwerken tegen Ransomware: Evaluatie Melissa.* Universiteit Leiden. Geraadpleegd van https://cyberveilignederland.nl/upload/userfiles/images/news/rapport%20evaluatie%20Melissa_%20Samenwerken%20tegen%20Ransomware.pdf

Van der Kleij, R. (2022). From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design. In T. Ahram & W. Karwowski (Eds.), *Human Factors in Cybersecurity. International Conference. AHFE Open Access*, vol 53. AHFE International, USA. http://doi.org/10.54941/ahfe1002209

Van der Kleij, R., Van 't Hoff-de Goede, S., Van de Weijer, S., & Leukfeldt, R. (2020a). Ons cybergedrag is veel onveiliger dan we zelf denken. Implicaties voor effectief beïnvloedingsbeleid door de overheid. *Justitiële verkenningen, 46*(2), 113–128. https://doi.org/10.5553/JV/016758502020046002011

Van der Kleij, R., Wijn, R., & Hof, T. (2020b). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers & Security,* Vol. 97. https://doi.org/10.1016/j.cose.2020.101970

Van der Laan, A. M., Beerthuizen, M. G. C. J., & Boot, N. (2021). *Monitor Jeugdcriminaliteit 2020. Ontwikkelingen in de jeugdcriminaliteit 2000-2020.* Den Haag.

Van der Varst, L., Groenendaal, J., Bantema, W., & Cools, F. (2022). *Bestuurlijke bevoegdheden cyber: Bevoegdheden en interventiemogelijkheden van burgemeesters en/of voorzitters veiligheidsregio bij (dreigende) digitale incidenten.* Arnhem: Nederlands Instituut Publieke Veiligheid.

Van der Wagen, W., & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480–497. https://doi.org/10.1177/1477370818812016

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, 185–200. Gompel&Svacina.

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*. www.rathenau.nl/sites/default/files/2021-07/Rathenau_Instituut_Rapport_Online_ontspoord.pdf

Van Ruijven, T., & Keijser, B. (2017). *Ketenweerbaarheid tegen cyberdreigingen: Uitgangspunten, good practices en een stappenplan voor het vergroten van cyber ketenweerbaarheid.* TNO.

Van 't Hoff-de Goede, S., & Janssen, J. (2024). De overlap tussen online en offline geweld in afhankelijkheidsrelaties: Naar een typologie voor professionals. *PROCES, 102*(1), 57–66.

Van 't Hoff-de Goede, S., & Leukfeldt, E. R. (2021). WhatApp-fraude komt veelvuldig voor in Nederland. *Secondant*. Beschikbaar via https://ccv-secondant.nl/platform/article/whatsappfraude-komt-veelvuldig-voor-in-nederland

Van 't Hoff-de Goede, S., & Leukfeldt, E. R. (2024). Slachtofferschap van cybercriminaliteit. In W. van der Wagen, J.-J. Oerlemans & M. Weulen Kranenbarg (Red.), *Basisboek Cybercriminaliteit* (in druk).

Van 't Hoff-de Goede, S., Leukfeldt, R., & Van de Weijer, S. (2023). Explaining cybercrime victimization using a longitudinal population-based survey experiment. Are personal characteristics, online routine activities, and actual online behavior related to future cybercrime victimization? *Journal of Crime and Justice,* 1–20. https://doi.org/10.1080/0735648X.2023.2222719

Van 't Hoff-de Goede, S., Van der Kleij, R., Van de Weijer, S., & Leukfeldt, R. (2019). *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*. Den Haag: WODC, Centre of Expertise Cybersecurity, De Haagse Hogeschool Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Beschikbaar via https://wodc.nl/wodc-nieuws-2020/hoe-veilig-gedragen-wij-ons-online.aspx

Van Wijngaarden, N. (2024). *Plegerschap van sexting-misbruik: de motieven van jonge plegers achter dit gedrag.* Offlimits.

Van Wilsem, J. (2013a). 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168–178. https://doi.org/10.1093/esr/jcr053

Van Wilsem, J. (2013b). Hacking and Harassment-Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437–453. https://doi.org/10.1177/1043986213507402

VAR (2022). *Interventieoverzicht Cyberweerbaarheid. VeiligheidsAlliantie regio Rotterdam.* Geraadpleegd van https://veiligheidsalliantie.nl/action/?action=download&id=849

Veenstra, S. (2023). Het ontrafelen en integraal aanpakken van een cybercrimineel jeugdnetwerk: Geleerde lessen uit RIEC-casuïstiek in Nood-Nederland. *Tijdschrift voor Veiligheid, 22*(2). https://doi.org/10.5553/TvT/.000055

Veenstra, S., Zuurveen, R., & Stol, W. (2015). *Cybercrime onder bedrijven: Een onderzoek naar slachtofferschap van cybercrime onder het midden-en kleinbedrijf en zelfstandigen zonder personeel in Nederland*. Cybersafety Research Group.

Verweijen, B. (2022). Leren van cyberincidenten: een meta-analyse van evaluatierapporten ten behoeve van organisatorisch leren. *Tijdschrift voor Veiligheid, 21*(3-4), 89–108. https://doi.org/10.5553/TvV/.000046

Verweijen, B., Kievik, M., & Spithoven, R. (2023). *Naar een cyberweerbaar Gelders mkb Een verkennend onderzoek naar barrières en ondersteuningsmogelijkheden.* Hogeschool Saxion. Geraadpleegd van www.saxion.nl/binaries/content/assets/onderzoek/areas--living/maatschappelijke-veiligheid/publieksrapportage_naar-een-cyberweerbaar-gelders-mkb_saxion.pdf

Voce, I., & Morgan, A. (2023). *Cybercrime in Australia 2023* (43). Australian Institute of Criminology. https://doi.org/10.52922/sr77031

Vrbnjak, D., Denieffe, S., O'Gorman, C., & Pajnkihar, M. (2016). Barriers to reporting medication errors and near misses among nurses: A systematic review. *International Journal of Nursing Studies, 63*, 162–178. https://doi.org/10.1016/j.ijnurstu.2016.08.019

Vuik, G., & Bantema, W. (2021). Perspectief uit de praktijk: Het digitale gebiedsverbod als gemeentelijk instrument tegen online aangejaagde ordeverstoringen. *Bestuurswetenschappen, 75*(3), 94–108.

Wade, C. R., Molony, S. T., Durbin, M. E., Klein, S. H., & Wahl, L. E. (1992). *Communicating with the Public about Risk. U.S. Department of Energy.*

Wall, D. S. (2024). *Cybercrime: The Transformation of Crime in the Information Age*, 2nd edition. https://doi.org/10.13140/RG.2.2.28017.45928

Wanamaker, K. A. (2019). *Profile of Canadian businesses who report cybercrime to police: The 2017 Canadian Survey of Cyber Security and Cybercrime*. Public Safety Canada.

Warr, M. (2000). Fear of crime in the United States: Avenues for research and policy. In D. Duffee (Ed.), *Criminal justice 2000: Vol.4. Measurement and analysis of crime and justice* (pp. 451–490). Washington, DC: National Institute of Justice.

Weigand, S. (2021, September 9). *Younger remote workers see security as a hindrance. SC media.* Geraadpleegd van www.scma gazine.com/news/training/younger-remote-workers-see-security-as-a-hindrance.

Whitten, A., & Tygar, J. D. (1999, August). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX security symposium* (Vol. 348, pp. 169–184).

Whitty, M. T. (2018). 419 – it's just a game: Pathways to cyber-fraud criminality emanating from West Africa. *International Journal of Cyber Criminology, 12*(1), 97–114. https://doi.org/10.5281/ZENODO.1467848

'Wie schiet deze lelijkerd dood?' De grenzeloze terreur van Telegram-groep Looijkartel. (2023, 17 juni). NOS. https://nos.nl/regio/noord-holland/artikel/407215-wie-schiet-deze-lelijkerd-dood-de-grenzeloze-terreur-van-telegram-groep-looijkartel

Wielers, F. (2022). *Factors affecting the intention to adopt cyber incident response planning among Dutch SMEs: an empirical investigation*. [Master's Thesis]. Radboud Universiteit. https://theses.ubn.ru.nl/bitstreams/4d5b6f69-d26d-4fa7-a9d4-608871c2677e/download

Wilcockson, T. D. W., Ellis, D. A., & Shaw, H. (2018). Determining typical smartphone usage: What data do we need? *Cyberpsychology, Behavior, and Social Networking, 21*(6), 395–398. https://doi.org/10.1089/cyber.2017.0652

Willemse, K. (2021). Cybersecurity Education: The Need for Awareness in Schools. *Journal of Cyber Policy, 7*(1), 33–54.

Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through Situational Crime Prevention. *Communications of the ACM, 52*(9), 133–137. https://doi.org/10.1145/1562164.1562198

Witte, K. (1992). Putting the Fear back in Fear Appeals: The Extended Parallel Process Model. *Communication Monographs, 59*(4), 329–349.

Witte, K. (1996). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In *Handbook of communication and emotion* (pp. 423–450). Academic Press.

Woods, D. W., & Böhme, R. (2022). *The commodification of consent. Computers & Security, 115*. https://doi.org/10.1016/j.cose.2022.102605

Yeung, T. H., Horyniak, D. R., Vella, A. M., Hellard, M. E., & Lim, M. S. C. (2014). Prevalence, correlates and attitudes towards sexting among young people in Melbourne, Australia. *Sexual Health, 11*(4), 332. https://doi.org/10.1071/SH14032

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

OVER DE AUTEURS

REDACTEUREN

Rutger Leukfeldt, Bijzonder hoogleraar Governing Cybercrime, Leiden University, directeur Centre of Expertise Cybersecurity en lector Cybercrime & Cybersecurity, De Haagse Hogeschool, Senior Onderzoeker Cybercrime, NSCR.

Remco Spithoven, Lector Online Weerbaarheid, Hogeschool Saxion.

Jurjen Jansen, Lector Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool, Politieacademie.

Carlyn van Amersfoort, Onderzoeker lectoraat Online Weerbaarheid, Hogeschool Saxion.

AUTEURS

Willem Bantema, Lector Bestuur en Veiligheid in een Digitaliserende Samenleving, NHL Stenden Hogeschool.

Luuk Bekkers, Postdoctoraal onderzoeker, NSCR, Onderzoeker lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool.

Kimberley Bluhm, Docent/onderzoeker lectoraat Digitale Weerbaarheid, NHL Stenden Hogeschool.

Jildau Borwell, Senior cybercrime analist, Politie-eenheid Noord-Nederland, Onderzoeker lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool, Buitenpromovendus, Open Universiteit.

Sander Ebbers, Buitenpromovendus, Open Universiteit, Docent/onderzoeker lectoraat Digitale Weerbaarheid, NHL Stenden Hogeschool.

Robin Christiaan van Halderen, Associate Lector Online Weerbaarheid, Hoofddocent Master Veiligheid en Digitalisering, Hogeschool Saxion.

Susanne van 't Hoff-de Goede, Associate Lector Cybercrime & Cybersecurity, De Haagse Hogeschool, Research Fellow, NSCR.

Ynze van Houten, Senior onderzoeker lectoraat Online Weerbaarheid, Hoofddocent Master Veiligheid en Digitalisering, Hogeschool Saxion.

Jurjen Jansen, Lector Digitale Weerbaarheid van Mens en Organisatie, NHL Stenden Hogeschool, Politieacademie.

Milou Kievik, Senior onderzoeker lectoraat Online Weerbaarheid, Hogeschool Saxion.

Rick van der Kleij, Lector Cyber Resilience, Avans Hogeschool, Senior onderzoeker cybersecurity, TNO.

Renske Korenromp, Onderzoeker lectoraat Cyberweerbare Organisaties, Avans Hogeschool.

Rutger Leukfeldt, Bijzonder Hoogleraar Governing Cybercrime, Leiden University, directeur Centre of Expertise Cybersecurity, De Haagse Hogeschool, Senior Onderzoeker Cybercrime, NSCR.

Joeri Loggen, Promovendus lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool, buitenpromovendus, Universiteit Leiden.

Sifra Mathijsse, Promovendus lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool, buitenpromovendus, Universiteit Leiden.

Stephen McCombie, Lector Maritime IT Security, NHL Stenden Hogeschool.

Ellen Misana-ter Huurne, Senior onderzoeker lectoraat Online Weerbaarheid, Hogeschool Saxion.

Asier Moneva, Onderzoeker, lectoraat Cybercrime & Cybersecurity, De Haagse Hogeschool, NSCR.

Peter Roelofsma, Lector Risk management & Cyber Security, De Haagse Hogeschool, gast Senior onderzoeker, Erasmus MC.

Robby Roks, Universitair hoofddocent Criminologie, Onderzoeker, Erasmus School of Law, Erasmus Universiteit Rotterdam.

Remco Spithoven, Lector Online Weerbaarheid, Hogeschool Saxion, hoofdredacteur, *Tijdschrift voor Veiligheid*.

Marcel Spruit, Lector Cyber Security & Safety, De Haagse Hogeschool.

Wouter Stol, Bijzonder hoogleraar Politiestudies, Open Universiteit, Lector Cybersafety, NHL Stenden Hogeschool en Politieacademie, operationeel specialist Cyber en Intel, Politie-eenheid Noord-Nederland.

Renze Tjoelker, Onderzoeker lectoraat Online Weerbaarheid, coördinator master Veiligheid & Digitalisering, Hogeschool Saxion, buitenpromovendus, Universiteit Twente.

Thijs van Valkengoed, Docent/onderzoeker lectoraat Digitale Weerbaarheid, NHL Stenden Hogeschool.

Bruno Verweijen, Senior onderzoeker lectoraat Online Weerbaarheid, docent master Veiligheid & Digitalisering, Hogeschool Saxion.

Saskia Westers, Docent/onderzoeker lectoraat Digitale Weerbaarheid, NHL Stenden Hogeschool, Interventiespecialist, Team Cybercrime, Politie-eenheid Noord-Nederland.