Digitale weerbaarheid van mens en organisatie

De kracht van verbinding

Dr. Jurjen Jansen

POLITIEACADEMIE

THORBECKE ACADEMIE
NHL STENDEN

Dr. Jurjen Jansen

Digitale weerbaarheid van mens en organisatie

De kracht van verbinding

Publicatie ter gelegenheid van lectorale rede
(30 mei 2023)

De missie van het lectoraat Digitale Weerbaarheid van Mens en Organisatie is het bevorderen van de veiligheid in de digitaliserende samenleving. Middels hoogwaardig praktijkgericht onderzoek draagt het lectoraat bij aan: kennisontwikkeling en het delen van kennis, oplossingen voor de beroepspraktijk en maatschappelijke vraagstukken, en de kwaliteit en toekomstbestendigheid van onderwijs en professionalisering. De onderzoekslijnen zijn:

1. Digitale weerbaarheid van burgers
2. Digitale weerbaarheid van organisaties
3. Digitale weerbaarheid van politie

Colofon

Inhoud

Voorwoord en dankwoord

In mei 2010 trad ik in dienst bij de onderzoeksgroep Cybersafety van prof. dr. Wouter Stol, die toen nog onderdeel was van NHL Hogeschool. Waar het bestuderen van digitale veiligheid traditioneel onderdeel uitmaakte van het technische domein, is dit de eerste onderzoeksgroep in Nederland die de menselijke aspecten ervan bestudeerde. Vanuit de onderzoeksgroep Cybersafety wordt al bijna vijftien jaar hoogwaardig, praktijkgericht onderzoek gedaan naar veiligheidsvraagstukken die samenhangen met de digitale samenleving. Dat doen we met veel enthousiasme en zijn dan ook trots op wat we in die periode samen met collega's, studenten, partners en het werkveld hebben gerealiseerd.

Naast mijn werk als onderzoeker was ik als docent verbonden aan de opleiding Integrale Veiligheidskunde. Na ongeveer drie jaar veel kennis en ervaring te hebben opgedaan over uiteenlopende vraagstukken op het gebied van digitalisering en veiligheid, en bijgedragen te hebben aan de (door) ontwikkeling en het verzorgen van onderwijs op dit thema, kwam de kans voorbij om promotieonderzoek te doen naar de veiligheid van internetbankieren waarbij de eindgebruiker centraal staat in het denken over veiligheid. Dit paste uitstekend bij mijn interesse in mens-computer interactie en de menselijke c.q. gedragsmatige aspecten van digitale veiligheid. Ik heb mij daar vier jaar volledig op gestort en het traject met goed gevolg afgesloten.

Na het behalen van mijn doctoraat in 2018 aan de Open Universiteit was ik nog niet uitgekeken op dit onderwerp. Door snelle technologische ontwikkelingen is het werk en onderzoek op dit terrein voorlopig nog niet klaar. Bovendien zorgen de snelle veranderingen voor diverse maatschappelijke veiligheidsissues waardoor je als onderzoeker en docent continu wordt uitgedaagd om te blijven leren, verbeteren en innoveren. Door deze uitdagingen heb ik mij in de dertien jaar dat ik met het onderwerp bezig ben weinig hoeven te vervelen. De afhankelijkheid van technologie neemt toe, digitale dreigingen en -incidenten nemen toe, maar de digitale weerbaarheid blijft – naar mijn mening spijtig genoeg – nog te ver achter.

Na mijn promotieonderzoek kreeg ik de kans om als senior onderzoeker de onderzoekslijn over digitale weerbaarheid binnen de onderzoeksgroep verder te ontwikkelen en uit te breiden. Doordat het bestuderen van digitale (on)veiligheid steeds populairder werd, en ook andere kennisinstellingen hier kansen zagen, hebben we ons als onderzoeksgroep een aantal keer – met succes – opnieuw moeten uitvinden. Tijdens de laatste visitatie (2019) werd duidelijk dat verbreding en verdieping nodig was, om een sterk fundament neer te zetten en toekomstbestendig te zijn. Dit leidde er onder andere toe dat we een duurzame relatie zijn aangegaan met de sector Kennis en Onderzoek van de Politieacademie, een kennispartner met wie we al veel samenwerkten. Ook resulteerde die uitkomst in twee vacatures voor nieuwe lectoren cybersafety. Samen met mijn college Willem Bantema geef ik nu leiding aan de onderzoeksgroep Cybersafety, waarbij ik mij – samen met mijn kenniskring – volop bezighoudt met vraagstukken op het gebied van digitale weerbaarheid. Dat doen we op onderzoekslijnen burgers, organisaties en politie, waarover later in deze bijdrage meer.

Al deze ontwikkelingen hoef ik dus niet in mijn eentje bij te houden, daar onderzoek naar te doen en uit te dragen. Dat doe ik samen met een topteam van enthousiaste en gedreven docent-onderzoekers. Daarom allereerst een expliciet woord van dank aan mijn collega's van het lectoraat: Saskia Westers, Sander Ebbers, Maike Berkenpas en Kimberly Bluhm, en de onderzoeksgroep in brede zin: Joyce Kerstens, Suzanna Twickler, Sipke de Vries, Anna Bartels, Denise de Boer en Laura Postma. Ook wil ik mijn dank uitspreken aan Lenneke Sprik en Esther Holman, die middels hun bijdrage aan het SPRONG-project waardevol werk verrichten voor de onderzoeksgroep. Natuurlijk mag Marja Blok niet ontbreken die als 'spin-in-het-web' op de achtergrond allerlei zaken voor ons tot in de puntjes regelt en Monique van Dijk die ons een tijd lang fantastisch heeft ondersteund. Jildau Borwell en Thijs van Valkengoed, die vanuit hun werk bij de politie een speciale band hebben met de onderzoeksgroep, ben ik dankbaar voor de fijne samenwerking en de goede spar-momenten.

Het is vanzelfsprekend dat ik Willem Bantema wil bedanken voor de prettige samenwerking en het 'samen navigeren naar een digitaal veilige samenleving'; de gemeenschappelijke titel van onze inauguratie. Het wordt ongetwijfeld een mooi avontuur! Uiteraard wil ik ook een woord van dank richten aan Wouter Stol die een belangrijke rol heeft gespeeld in de ontwikkelingen die ik heb meegemaakt binnen de hogeschool en de onderzoeksgroep. Ik kijk terug op een inspirerende samenwerking, goede discussies en de mooie resultaten die we hebben bereikt. Verder wil ik mijn collega's van het kenniscentrum Digitalisering, Intelligence en Technologie bedanken en alle andere collega's van de sector Kennis en Onderzoek van de Politieacademie. Een speciaal woord van dank aan Paul Moss en Edwin Bakker die een cruciale rol hebben gespeeld om deze samenwerking mogelijk te maken.

Daarnaast wil ik mijn collega's van de opleiding Integrale Veiligheidskunde specifiek en Thorbecke Academie breed bedanken voor de geweldige sfeer waarin we ons werk kunnen doen, en voor hun enthousiasme en bereidheid om mogelijk te maken dat het onderwerp en de onderzoeksresultaten landen binnen de opleidingen. De teamleiders – Marika Toutenhoofd, Edou Hilverda en Lucinda Wondel – spelen daarin een cruciale rol, dus ook jullie ben ik zeer erkentelijk. Tevens wil ik Richard Delger, de academiedirecteur, bedanken voor het mogelijk maken van deze positie en mij de verantwoordelijkheid daarvoor te geven, alsook het College van Bestuur van NHL Stenden Hogeschool – Erica Schaper, Oscar Couwenberg en Marc Otto – voor hun vertrouwen in mij om de lectortaak uit te mogen voeren.

Voorts ben ik nog veel meer mensen dank verschuldigd. In willekeurige volgorde betreffen dat de collega's van de Academie ICT & Creative Technologies, waarmee we steeds nauwer samenwerken, en alle andere NHL Stenden collega's – van andere opleidingen, academies, lectoraten, commissies, (ondersteunende) diensten, enzovoorts – met wie we goede relaties onderhouden. Een expliciet woord van dank aan Elske Posthuma en Floor May met wie momenteel interessante projecten uitvoeren.

Zoals later in deze bijdrage duidelijk zal worden is samenwerking essentieel om de digitale weerbaarheid in Nederland omhoog te brengen. Hierbij wil ik dan ook graag alle opdrachtgevers, samenwerkings- en netwerkpartners bedanken voor het werk wat we de afgelopen jaren al hebben gedaan, en de komende tijd en daarna nog gaan doen. Het gaat hierbij niet alleen om het werkveld, zoals politie, gemeenten, belangenorganisaties en private organisaties, maar ook om partners van kennisinstellingen. In deze laatste categorie wil ik Rutger Leukfeldt en Remco Spithoven, samen met hun kenniskring, specifiek benoemen met wie we een duurzame samenwerking zijn aangegaan in het SPRONG Expertisenetwerk Cyberweerbaar Nederland.

Tot slot mijn familie en vrienden; bedankt voor jullie support! Mijn vrouw Bianca; voor je aanmoediging en interesse. En mijn prachtige dochters Féline en Hannah; voor de benodigde afleiding waar jullie altijd voor zorgen en het laten zien dat er meer is dan werk alleen.

Aan allen: Stay safe, cybersafe!

Jurjen Jansen
Heerenveen, 17 april 2023

Hoofdstuk 1

Digitale weerbaarheid: verkenning en positiebepaling

1.1 Inleiding

In 2013, precies tien jaar geleden, startte ik met mijn promotieonderzoek naar de digitale weerbaarheid van eindgebruikers in de context van internetbankieren. Dit promotietraject markeerde het begin van het digitale weerbaarheidsonderzoek binnen de onderzoeksgroep Cybersafety van NHL Stenden Hogeschool, dat in 2018 als officiële onderzoekslijn werd bestempeld. Nu, tien jaar later, is digitale weerbaarheid ondergebracht in een zelfstandig lectoraat en mag ik mijn lectorale rede uitspreken over dit boeiende, en snel in ontwikkeling zijnde onderwerp.

In deze publicatie, met als subtitel 'de kracht van verbinding', ga ik in op de onderzoekslijnen en -thema's die we vanuit het lectoraat voor de komende jaren hebben vastgesteld, de onderzoeken waaraan we werken en de verdere plannen die we daarvoor aan het uitwerken zijn. Deze staan centraal in hoofdstuk 2. Vervolgens ga ik in hoofdstuk 3 dieper in op hoe we invulling geven aan deze plannen – en de uitdagingen die daar onder liggen – samen met collega's van binnen en buiten het lectoraat en de onderzoeksgroep, studenten en het werkveld. Ik ben ervan overtuigd dat om de problemen en uitdagingen die ons wachten op het gebied van digitalisering en veiligheid alleen adequaat aangepakt kunnen worden in goede samenwerking, over verschillende disciplines heen. Vandaar: de kracht van verbinding.

Voordat ik de onderzoeksplannen uit de doeken doe, ga ik in dit eerste hoofdstuk nader in op het onderwerp waar we binnen het lectoraat onderzoek naar doen, en op de kernbegrippen en uitdagingen die hiermee verband houden (par. 1.2 en 1.3). Daarmee tracht ik enkele vragen te beantwoorden die mogelijk bij de lezer zijn opgekomen, zoals: Wat is de context als we het hebben over digitalisering en digitale weerbaarheid? Welke uitdagingen spelen er op dit terrein? Wat is digitale weerbaarheid nu precies? En: Waarom is het van belang om hier onderzoek naar te doen, projecten voor uit te voeren en onderwijs voor te verzorgen? Tevens beschrijf ik waarom de mens een essentiële en potentieel sterke – en dus niet(!) de zwakste – schakel vormt in de digitale veiligheidsketen. In par. 1.4 ga ik in op de noodzaak voor een ander perspectief op de rol van de mens, namelijk een waarbij de mens wordt beschouwd als iemand die positief bijdraagt aan digitale veiligheid in plaats van iemand die problemen veroorzaakt. Tot slot sta ik stil bij de uitdagingen van de politie aangaande digitalisering en de voorwaarden die nodig zijn om daarop te acteren (par. 1.5).

1.2 Digitalisering en veiligheids-uitdagingen

In deze paragraaf bespreek ik de uitdagingen die gepaard gaan met digitalisering. Tevens bespreek ik de achterliggende oorzaken daarvan.

De mens is 'van nature een technologisch wezen, dat haar omgeving op inventieve wijze transformeert' (Van Mensvoort, 2019, p.117). De voortdurende en snelle voortgang van de digitalisering[1] van de maatschappij blijft onverminderd doorgaan.[2] Digitalisering speelt op steeds meer plaatsen en op steeds meer verschillende manieren een rol in het dagelijks leven. In het recentste Cybersecurity Beeld Nederland (NCTV, 2022) worden digitale processen omschreven als het 'zenuwstelsel' van de maatschappij en onze economie (zie ook Van Dijk, 2012). Simpelweg omdat de maatschappij zonder niet meer goed kan functioneren. Veiligheid is een basisvoorwaarde voor een samenleving die vitaal en weerbaar is en waarin mensen naar tevredenheid kunnen leven en zich kunnen ontplooien. Ducheine (2018) noemt veiligheid een 'delicaat krachtenspel', want bij te veel veiligheid staan initiatief en vrijheid onder druk, terwijl te weinig veiligheid kan leiden tot chaos. Een goede balans is dus noodzakelijk.

In Nederland kunnen burgers, bedrijven en overheden niet meer zonder digitale technologieën. Bijna iedereen maakt gebruik van internet en een smartphone, voor tal van taken en bezigheden. Daarnaast wordt het internet ook steeds meer gebruikt voor het aansturen van maatschappelijk vitale objecten, zoals bruggen en energiecentrales. Alles raakt met elkaar verbonden; ook (huishoudelijke) apparaten. Dit wordt ook wel aangeduid met de term Internet of Things (IoT). IoT is niet per se een nieuwe ontwikkeling, maar wel een die de afgelopen jaren een flinke vlucht heeft genomen (Van Boheemen e.a., 2020). IoT-ontwikkelingen zien we niet alleen terug in de privésfeer, maar bijvoorbeeld ook in organisaties, in auto's en in de openbare ruimte. Dit laatste wordt ook wel aangeduid met de term smart cities (AP, 2021), waarbij digitale technieken worden ingezet om vraagstukken aan te pakken aangaande klimaat, mobiliteit en gezondheid.[3] Omdat dergelijke technieken kwetsbaarheden bevatten – voor uitval, verstoring en aanvallen (NCTV, 2022) – maakt het een interessant onderwerp van studie.[4]

Nederland is één van de meest gedigitaliseerde landen ter wereld. Digitale ontwikkelingen gaan steeds verder en kunnen daarmee ook nieuwe uitdagingen met zich meebrengen op veiligheidsgebied. Denk bijvoorbeeld aan ontwikkelingen als kunstmatige intelligentie, machine learning, robotica, 6G, kwantum computing, augmented reality en metaverse (Accenture, 2023; Jansen e.a., 2023). Met digitale technologieën kunnen mensen elkaar ook geweld aan doen, bijvoorbeeld door dreigtweets te sturen, DDoS-aanvallen uit te voeren (i.e., het verstoren of platleggen van een systeem door middel van overbelasting), phishing pogingen te ondernemen en systemen te hacken. Dit kan leiden tot slachtofferschap van burgers, faillissement van bedrijven alsook tot maatschappelijke ontwrichting. Digitale veiligheid raakt in die zin ook de nationale veiligheid. Doordat we vrijwel volledig afhankelijk zijn van de eenmaal gedigitaliseerde systemen en processen is digitale veiligheid essentieel geworden

[1] Digitalisering is 'de ontwikkeling die inhoudt dat geautomatiseerde werken op steeds meer plaatsen en op steeds meer verschillende manieren een rol spelen in het dagelijks leven' (Stol & Strikwerda 2017, p.304).

[2] Hoewel voor de doorontwikkeling van kunstmatige intelligentie recent een open brief is gestuurd vanuit de techsector en wetenschap om deze tijdelijk te pauzeren. Zie: https://nos.nl/artikel/2469350-techprominenten-pleiten-voor-tijdelijke-rem-op-risicovolle-ontwikkeling-ai

[3] https://www.g40stedennetwerk.nl/nieuws/rijk-en-gemeenten-moeten-samen-bouwen-aan-slimmere-steden

[4] Recent hebben we samen met collega's van de Haage Hogeschool verkennend onderzoek gedaan naar twee specifieke smart city-toepassingen. We bestudeerden een casus over intelligente verkeersregelinstallaties en een casus over slimme camera's voor druktemeting (Kerpershoek e.a., 2022a; 2022b).

voor burgers, bedrijven en overheden. Het tegengaan van digitaal geweld en/of het reduceren van de impact ervan vergt kennis, handelingsbekwaamheid en visie. Ook vergt het samenwerking (zie hoofdstuk 3). Het lectoraat levert hieraan een bijdrage middels hoogwaardig praktijkgericht onderzoek (zie hoofdstuk 2).

Het lijkt er nu wellicht op dat ik vooral theoretische problemen beschrijf, maar in de praktijk zien we (helaas) genoeg voorbeelden voorbij komen waaruit blijkt dat we met een harde realiteit te maken hebben. Ter illustratie, met de digitalisering van de samenleving is de criminaliteit ook voor een groot deel gedigitaliseerd (Holt & Bossler, 2014). Belangrijk is om vervolgens te weten wat de aard en omvang van het probleem zijn. We vertrouwen daarbij veelal op zelfrapportagestudies, zoals de Veiligheidsmonitor van het Centraal Bureau voor de Statistiek (CBS), en aangifteregistraties die bekend zijn bij de politie. Voor de eerste geldt dat soortgelijke informatie voor organisaties minder inzichtelijk is. Voor de tweede geldt het zogeheten dark number (i.e., niet-geregistreerde criminaliteit) als een belangrijke beperking (Beerthuizen e.a., 2020; Smit e.a., 2018). De aangiftebereidheid van online criminaliteit ligt over het algemeen namelijk laag (Kemp e.a., 2021; Van de Weijer e.a., 2020; Domenie e.a., 2013). Dit geldt zowel voor burgers als voor organisaties. Redenen daarvoor omvatten schaamte, reputatieschade, conflicterende belangen (bedrijfscontinuïteit als prioriteit), maar ook een gebrek aan vertrouwen in de afhandeling ervan door opsporingsautoriteiten.

Wanneer het gaat over criminaliteit dan bedoel ik elke gedraging die als misdrijf strafbaar is gesteld. Als het gaat over online criminaliteit dan wordt vaak onderscheid gemaakt in twee vormen: (i) criminaliteit die mogelijk is geworden door digitalisering, waarbij ICT zowel het middel als het doel is, en (ii) criminaliteit die door digitalisering een andere verschijningsvorm kreeg, waarbij ICT het middel is, maar niet het doel. De eerste noemen we cybercriminaliteit (of cybercrime in enge zin; bijv. hacken) en de tweede noemen we gedigitaliseerde criminaliteit (of cybercrime in ruime zin; bijv. onlinefraude). Voor het leesgemak hanteer ik in het vervolg de koepelterm 'online criminaliteit'.

In de recentste Veiligheidsmonitor lezen we dat in 2021 17% van alle Nederlanders van 15 jaar en ouder in een jaar tijd slachtoffer is geworden van een of meerdere (gemeten) vormen van online criminaliteit (CBS, 2022).[5] Omgerekend komt dit neer op zo'n 2,5 miljoen Nederlanders. In werkelijkheid kan het aantal nog hoger liggen, omdat slachtofferschap voor een beperkte set van delicten is uitgevraagd. Wat in ieder geval duidelijk is, is dat we te maken hebben met een groot maatschappelijk probleem (Beerthuizen e.a., 2020). Ter vergelijking, ook voor de gemeten vormen van traditionele criminaliteit in de Veiligheidsmonitor is het slachtofferpercentage 17. Dat grote groepen mensen slachtoffer worden van online criminaliteit is overigens geen nieuwe bevinding (Domenie e.a., 2013). Wanneer de cijfers over langere tijd worden bekeken, dan zien we dat het aandeel traditionele delicten waarvan men slachtoffer wordt lijkt terug te lopen, terwijl die voor online criminaliteit juist een stijgende tendens laten zien. Dit geldt niet alleen voor Nederland[6], maar voor heel Europa (Europol, 2020). Ook onder bedrijven zien we relatief grote aantallen slachtoffers van uiteenlopende vormen van online criminaliteit (Jansen e.a., 2016; Notté e.a., 2019). Onderzoek laat zien dat in een jaar tijd een op de vijf ondernemers in het midden- en kleinbedrijf (mkb) daarvan slachtoffer is geworden (Notté e.a., 2019).[7]

Nederlandse burgers worden volgens de cijfers van het CBS (2022) vooral slachtoffer van online oplichting en fraude. Bedrijven lijken vooral kwetsbaar voor ransomware en phishing. Ook bij grotere bedrijven en publieke organisaties zien we dat uitval van dienstverlening en bedrijfsvoering tot de grootste risico's behoren. Naast ransomware kunnen fouten in software, zoals in 2019 de Citrix-kwetsbaarheid[8] liet zien, maar bijvoorbeeld ook kwetsbaarheden in ketens een belangrijk risico vormen (SURF, 2022; IBD, 2022). Wereldwijd werd de schade van online criminaliteit in 2021 groter geschat dan de schade van de georganiseerde handel in drugs (Ahamad, 2020; Naidoo, 2020). Online criminaliteit gaat echter verder dan financiële schade alleen. Zo leren we uit diverse onderzoeken dat slachtofferschap gepaard gaat met soms vergaande sociaal-emotionele gevolgen, zoals schaamte en verlies van vertrouwen (bijv. in eigen handelen, internet en medemens), en lichamelijke klachten, zoals hartkloppingen en slecht ervan slapen (Borwell e.a., 2021b; Jansen & Leukfeldt, 2018; Leukfeldt e.a., 2020a).

Voor organisaties geldt dat als de dienstverlening en bedrijfsvoering uitvallen dit beperkt kan blijven tot een (intern) incident, maar ook kan leiden tot een cybercrisis[9]; een andere veiligheidsuitdaging die gepaard gaat met digitalisering. Een cybercrisis is 'een verstoring, uitval of misbruik van een gedigitaliseerd proces, (informatie)systeem of informatiedienst die de continuïteit, integriteit en/of vertrouwelijkheid bedreigt of ernstig verstoort en waarbij onder (een gevoel van) tijdsdruk en onzekerheid besluiten moeten worden genomen' (Ebbers e.a., 2021, p.10). In Nederland hebben bijvoorbeeld de gemeenten Lochem en Hof van Twente hiermee te maken gehad (De Winter, 2019; 2021).

Een digitale aanval kan ook fysieke gevolgen met zich mee brengen. Een van de eerste en meest bekende digitale incidenten met fysieke impact is de Stuxnet-worm. Deze computerworm[10], die vermoedelijk via een besmette USB-stick werd geïnstalleerd, beïnvloedde bepaalde Siemens-apparatuur op schadelijke wijze; het wijzigde de PLC (programmable logic controller) waarmee de motoren van ultracentrifuges aangestuurd werden

[5] Opgemerkt dient te worden dat het CBS ook het niet-strafbare cyberpesten rekent tot online criminaliteit.

[6] https://www.cbs.nl/nl-nl/nieuws/2022/09/minder-traditionele-criminaliteit-meer-online-criminaliteit

[7] Zie ook: https://www.digitaltrustcenter.nl/nieuws/aanpak-preventie-cybercrime-bij-mkb

[8] https://nos.nl/artikel/2339151-lek-bij-citrix-actief-gebruikt-door-hackers-en-spionnen

[9] Kaouass en Zannoni (2017) onderscheiden vier verschijningsvormen van cybercrisis: (i) grootschalige én langdurige IT-uitval, (ii) datalek van persoonsgevoelige informatie (medewerkers), (iii) datalek van bedrijfsgevoelige informatie en (iv) onbetrouwbaarheid van datasystemen/datamanipulatie.

[10] Een worm is 'kwaadaardige code die zichzelf, zonder tussenkomst van een mens, vermenigvuldigt en verspreidt over verschillende digitale systemen (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, pp. 108-109).

in een Iraanse uraniumverrijkingsinstallatie.[11] Een bekend voorbeeld met fysieke impact in eigen land betreft de NotPetya-aanval die Maersk trof in 2017. NotPetya (ook een worm), leek aanvankelijk op een ransomware-aanval, maar bleek uiteindelijk zogenoemde wiperware, waarbij data onherstelbaar worden beschadigd (Van Duin & Maan, 2018). Deze aanval resulteerde in aanzienlijke en langdurige uitval van IT-systemen bij Maersk. Dit had niet alleen gevolgen voor het bedrijf zelf, maar ook voor de gemeente Rotterdam. Het containervervoer in de haven van Rotterdam werd grotendeels stilgelegd, waardoor verkeersopstoppingen en lange files ontstonden rond de haven (Van Duin & Maan, 2018; WRR, 2019). Cyberincidenten of -crises kunnen leiden tot cascade-effecten; wanneer een individueel probleem invloed heeft op de rest van de keten, het netwerk of zelfs daarbuiten (WRR, 2019). De NotPetya-aanval kan hiertoe worden gerekend. De aanval was gericht op, en begon in, Oekraïne en verspreidde zich snel naar andere landen zoals Denemarken, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten, en dus ook Nederland (Van Duin & Maan, 2018). De kosten die met deze aanval gemoeid zijn worden geschat op vele miljarden euro's (WRR, 2019).

Er zijn naast online criminaliteit en cybercrises nog tal van andere dreigingen te identificeren die gepaard gaan met digitalisering. Het voert echter te ver om daar uitgebreid aandacht aan te besteden, omdat die buiten de context van ons onderzoek vallen. Denk bijvoorbeeld aan zaken als online spionage en cyber warfare. De NCTV (2022) stelt dat digitale aanvallen met als doel inlichtingen te vergaren het 'nieuwe normaal' zijn. Hoewel we daar als lectoraat op dit moment niet op directe wijze aan bijdragen, komt dit wel terug in het onderwijsprogramma van de Thorbecke Academie; expliciet bij de minor Intelligence & Counterintelligence. Andere schadelijke fenomenen op het internet, zoals polarisatie, haatzaaien en desinformatie, behoren ook niet tot de primaire onderzoeksthema's van ons lectoraat, maar worden wel binnen het grotere collectief van de onderzoeksgroep opgepakt. Aan dergelijke thema's wordt veelvuldig aandacht besteedt binnen het lectoraat Bestuur in een Digitaliserende Samenleving (Bantema, 2023). Ook hangen vraagstukken hieromtrent nauw samen met mediawijsheid, zoals: Hoe houd ik regie op mijn eigen data? En: Hoe kan ik verifiëren dat wat ik op internet lees feitelijk juist is? Dergelijke vraagstukken staan centraal in de crossover Digital Citizenship tussen de onderzoeksgroep Cybersafety en het lectoraat Organisations and Social Media van NHL Stenden Hogeschool.

Na een aantal dreigingen en uitdagingen te hebben geïdentificeerd, ga ik nu in op enkele oorzaken die hieraan ten grondslag liggen. Op hoofdlijnen zien we dat de mens de *primary attack vector* is, waarbij veelal gebruik wordt gemaakt van social engineering. Social engineering omvat technieken 'die erop gericht zijn een doelwit over te halen om specifieke informatie te onthullen of een specifieke actie uit te voeren om onwettige redenen.'[12] Technieken die worden gebruikt zijn onder meer het gebruik van namen van geloofwaardige organisaties of actuele

[11] https://www.bbc.com/timelines/zc6fbk7
[12] https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

gebeurtenissen in combinatie met uitspraken die een beroep doen op angst, bedreiging, urgentie of opwinding, om mensen te beïnvloeden om te reageren (Viswanath e.a., 2011). De meest dominante vorm van social engineering is phishing. Phishing wordt niet alleen gedaan via e-mail, maar bijvoorbeeld ook via sms en app-berichten. De praktijk van phishing ontstond alweer zo'n dertig jaar geleden, maar werd pas medio jaren 2000 algemeen bekend.[13] Vandaag de dag speelt het nog steeds een grote rol aangaande digitale veiligheid. Statistieken laten zien dat in het derde kwartaal van 2022 – dus in een tijdsbestek van drie maanden – 1,27 miljoen phishing-aanvallen zijn uitgevoerd.[14]

Het internet heeft een aantal kenmerken waardoor de gelegenheid voor criminaliteit toeneemt (Yar, 2005; Leukfeldt, 2016). We leven in een netwerksamenleving waarin 'iedereen' met elkaar verbonden is (Van Dijk, 2012) en waarin criminelen zich goed kunnen organiseren. Het internet zorgt ervoor dat – met een beperkt aantal handelingen – veel potentiële slachtoffers worden bereikt. Potentiële slachtoffers zijn goed zichtbaar en toegankelijk via het internet.[15] Bovendien kunnen digitale aanvallen tijd en plaats onafhankelijk worden uitgevoerd; kwaadwillenden hoeven niet af te reizen naar een locatie of op een bepaald tijdstip aanwezig te zijn, maar kunnen vanuit hun eigen woning aanvallen uitvoeren op het moment dat zij het willen. Dit heeft ook als consequentie dat daders de impact die slachtoffers ervaren niet (direct) meekrijgen. Daarnaast zijn digitale goederen, zoals data en giraal geld, eenvoudig verplaatsbaar. Het internet zorgt er verder voor dat criminelen een relatief hoge mate van anonimiteit genieten, waarbij die anonimiteit tevens versterkt kan worden door privacy-enhancing technologies.[16] De opbrengsten van online criminaliteit zijn hoog, terwijl de pakkans daarentegen vrij laag is. Het internet vormt in die zin een grote criminele speelplaats.

Een belangrijk kenmerk van online criminaliteit en andere online dreigingen is dat deze vaak schaalbaar zijn (NCTV, 2022). Opschalen verwijst naar het vermogen om systemen en processen dusdanig aan te passen om te voldoen aan een grotere vraag. De NCTV stelt verder dat criminelen steeds beter en intensiever met elkaar samenwerken op dit terrein en daarbij hun aanvallen ook innoveren. Dit stelt steeds hogere eisen aan digitale weerbaarheid. Digitale weerbaarheid is namelijk veel minder schaalbaar. Omdat digitale dreigingen en risico's continu van aard kunnen veranderen (Van Boheemen e.a., 2020; Spithoven e.a., 2022a), en menselijk gedrag daarentegen lastig te veranderen is, moet voortdurend worden geïnvesteerd in digitale weerbaarheid. Of zoals Rothrock (2022, p.174) treffend zegt: 'Digital resilience does not happen overnight.'

[13] https://www.phishing.org/history-of-phishing
[14] https://apwg.org/trendsreports/
[15] Cijfers van het CBS tonen dat 96,8% van de Nederlanders thuis toegang heeft tot internet en dat 89,5% het internet dagelijks gebruikt. Zie: https://www.cbs.nl/nl-nl/cijfers/detail/84888NED
[16] Het woord 'relatief' is niet voor niets gekozen. De politie heeft diverse opties om afgeschermde criminele activiteiten inzichtelijk te maken (Jansen e.a., 2023). Zie ook: https://www.politie.nl/nieuws/2023/april/12/02--oost-nederland-politie-benadert-afnemers-gestolen-data.html

Het zou mooi zijn wanneer we uiteindelijk niet zoveel hoeven over te laten aan menselijke beslissingen, en zoveel mogelijk problemen aan de 'voorkant' kunnen voorkomen. Een veilige digitale wereld begint bij het veilig ontwerpen van systemen en processen (o.a. De Bruine, 2018). Dit betekent dat door aanpassingen aan het ontwerp van een applicatie, procedure of omgeving verleidingen om onveilig gedrag te vertonen zoveel mogelijk worden weggenomen en dat het gemakkelijker wordt gemaakt om veilig gedrag te vertonen. Dit kan bijvoorbeeld gerealiseerd worden door het toepassen van principes als security-by-design en privacy-by-design. We zien echter dat veiligheid nog steeds geen prioriteit is voor veel ontwikkelaars (NCTV, 2022). Dit geldt ook voor privacy, omdat de verdienmodellen van veel techbedrijven gebaat zijn om zoveel mogelijk te weten van de gebruiker. Bovendien zijn veel mensen bereid om met hun eigen (kostbare) gegevens 'gratis' diensten af te nemen.

Bovenstaande betekent echter niet dat we als mensheid ten onder zullen gaan aan al het technologische of digitale geweld. Zo benoemt Stol (2010, p.12) – in de gedachte van Lewis Mumford – '[...] dat mensen niet alleen in staat zijn om technologische ontwikkelingen in gang te zetten, maar ook om ze bij te sturen of zelfs om te buigen.' De overheid speelt daarin een belangrijke rol en kan via wetgeving, certificering en standaardisatie leveranciers stimuleren om de digitale producten en diensten die op de markt verschijnen beter te laten beveiligen (Van Boheemen e.a., 2020).

Digitale veiligheid en de strijd tegen online criminaliteit zijn al langer een prioriteit binnen Europa. Ter illustratie, het Verdrag van Boedapest inzake cybercriminaliteit dateert van 2001 en de inwerkingtreding ervan van 2004.[17] De eerste EU Cybersecurity Strategie is van 2013[18] en de eerste versie van de EU Network and Information Security (NIS) richtlijn komt uit 2016[19]. In 2018 trad de Algemene Verordening Gegevensbescherming (AVG) in werking, met als doel de belangen van natuurlijke personen te beschermen.[20] In 2019 werd de EU Cyber Security Act (CSA) in het leven geroepen, onder andere bedoeld om een Europees kader op te zetten voor cybersecurity certificering voor ICT-producten, -diensten en -processen.[21] Tot slot zijn in 2020 de Digital Services Act (DSA) en de Digital Market Act (DMA) voorgesteld.[22] De DSA is bedoeld om een digitale omgeving te creëren die veiliger is en waarin de fundamentele rechten van alle gebruikers van digitale diensten beschermd worden. De doelstelling van de DMA is om een gelijk speelveld te creëren voor innovatie, groei en concurrentie, zowel binnen de Europese interne markt als op mondiaal niveau.

Op dit moment zien we verdere positieve ontwikkelingen vanuit Europa om meer regie te krijgen

[17] https://www.coe.int/en/web/cybercrime/the-budapest-convention#
[18] https://www.eucybernet.eu/wp-content/uploads/2020/08/2013-cybersecurity-strategy-of-the-european-union.pdf
[19] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[20] https://gdpr.eu/what-is-gdpr/
[21] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[22] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

over en grip te krijgen op digitale veiligheid. Ik noem twee voorbeelden die hierop betrekking hebben. De eerste is de nieuwe NIS2 richtlijn[23], een vervolg op de NIS, waarvoor geldt dat organisaties die essentiële diensten leveren en digitale dienstverleners extra maatregelen moeten treffen om de digitale weerbaarheid te vergroten (Brouwer & Van Mil, 2023). De tweede is de Cyber Resilience Act (CRA)[24], waarbij fabrikanten van hardware en software aantoonbaar beveiligingsrichtlijnen moeten opvolgen. Daarbij wordt in het bijzonder aandacht geschonken aan IoT-apparatuur.

Op dit soort ontwikkelingen willen we als lectoraat – samen met het onderwijs – anticiperen. Voor de eerste (NIS2) geldt dat diverse organisaties voor de nodige nieuwe vraagstukken komen te staan. Ter vergelijking, dergelijke vragen zagen we ook op het moment dat de AVG werd aangekondigd, waarbij veel bedrijven – met name uit het mkb – bij ons aanklopten voor ondersteuning bij de (verdere) implementatie ervan. Voor de tweede (CRA) geldt dat fabrikanten van IoT-apparatuur vanaf 2024 aan strengere veiligheidsmaatregelen moeten voldoen. Zo niet, dan kan hun product worden geweerd van de Europese markt. Dit lost echter nog niet alle problemen op. Denk bijvoorbeeld aan de IoT-apparaten die voor 2024 zijn aangeschaft en geïmplementeerd. Dat zijn er nogal wat. Schattingen gaan uit van 12,2 miljard appraten in 2021.[25] Deze devices hoeven niet aan de nieuwe vereisten te voldoen. Wat betekent dit in termen van veiligheid? Hoe gaan we daarmee om? Vooralsnog moet daar bewust actie op worden ondernomen. Dit zijn twee voorbeelden van praktische vraagstukken waarbij onderzoek en onderwijs (via studenten) kunnen bijdragen aan het vinden van oplossingen voor het digitaal veiliger maken van de samenleving.

Resumerend, digitale veiligheid is vandaag de dag van fundamenteel belang voor een digitaal en onderling verbonden Nederland, Europa en wereld, want welvaart en vooruitgang zijn steeds afhankelijker geworden van digitalisering. Omdat de afhankelijkheid toeneemt, neemt ook de potentiële impact toe op moment dat het mis gaat. Dit betekent dat we naar een situatie toe moeten waarin we – als samenleving – voldoende digitaal weerbaar zijn.

1.3 Digitale weerbaarheid

In deze paragraaf licht ik toe wat digitale weerbaarheid is en ga ik dieper in op de essentiële rol die de mens speelt aangaande digitale veiligheid.

1.3.1 Digitale weerbaarheid op hoofdlijnen

De steeds grotere digitale connectiviteit die we verwezenlijken is zowel een aanjager als bedreiging voor de hedendaagse samenleving. 'Om ongestoord te kunnen functioneren, is weerbaarheid van de samenleving tegen digitale dreiging cruciaal.' Deze quote uit het recentste Cybersecuritybeeld Nederland (NCTV, 2022, p.7) geeft de essentie weer waar we met het lectoraat aan willen bijdragen. Met digitale weerbaarheid bedoel ik niet dat we 100% veiligheid moeten nastreven. Dat is simpelweg niet mogelijk. Digitale processen kunnen door technisch falen, menselijk handelen of een combinatie daarvan uitvallen. Bovendien zien we dat aanvallen steeds geavanceerder worden, georganiseerder worden uitgevoerd en statelijk actoren in toenemende mate daarbij betrokken lijken te zijn (NCTV, 2022).[26]

Wat bedoel ik dan wél met digitale weerbaarheid? Het is voor onderzoek belangrijk om te werken met heldere definities. Er zijn verschillende definities in omloop van het containerbegrip digitale weerbaarheid. Ik sluit voor een groot deel aan bij de definitie die wordt gehanteerd in de Nederlandse Cybersecuritystrategie 2022-2028 (NCSC, 2022, p.9). Deze luidt als volgt: '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.'

De essentie is dus om digitale risico's adequaat te managen en de impact te reduceren op het moment dat (ondanks getroffen maatregelen) zich een incident voordoet (Jansen, 2018). Het gaat er niet per se om dat alle aanvallen buiten de deur worden gehouden. Die strijd kan niet worden gewonnen. Echter, digitale weerbaarheid is van essentieel belang om stand te houden in de strijd (Rothrock, 2022). Van Boheemen e.a. (2020, p.3) vergelijken digitale weerbaarheid met het menselijk immuunsysteem. Dat systeem slaagt er ook niet in om alle aanvallen buiten de deur te houden. 'Het immuunsysteem rekent met indringers en interne incidenten af, of probeert ze onder de duim te houden. Wie gezond is, en preventieve maatregelen neemt, slaagt daar beter en langer in.' Dat geldt ook voor digitale veiligheid (Crossler, e.a., 2019).

Een wezenlijk aspect dat ik aan voorgaande definitie wil toevoegen is het leervermogen (zie ook Hollnagel, 2014; Van der Kleij & Leukfeldt, 2019; Rothrock, 2022). Op het moment dat zich incidenten, of bijna-incidenten, voordoen is het belangrijk dat daaruit lering wordt getrokken. In een ideaal geval vindt het leren niet alleen plaats daar waar het betreffende voorval zich voltrok, maar worden de *lessons learned* ook breder met elkaar gedeeld. Door dit te doen vindt leren gezamenlijk plaats wat de weerbaarheid ten goede komt (Verweijen, 2022). Dat kan op verschillende niveaus, bijvoorbeeld op het niveau van netwerken. In par. 3.1 noem ik een voorbeeld van zo'n netwerk waarvan het lectoraat deel uit maakt. Een illustratief voorbeeld van een organisatie die openlijk communiceerde over een ransomware-aanval is de Universiteit van Maastricht.[27]

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
[24] https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
[25] https://iot-analytics.com/number-connected-iot-devices/

[26] Let op dat het uitvoeren van criminele online handelingen niet is voorbehouden aan technisch onderlegde mensen en goed georganiseerde samenwerkingsverbanden. Denk aan cybercrime-as-a-service (Caas), waarbij 'diensten' voor het uitvoeren van bijvoorbeeld malware- en DDoS-aanvallen te koop worden aangeboden op het darkweb. Dit stelt niet-technische criminelen in staat om geavanceerde aanvallen uit te voeren zonder dat ze kennis hoeven te hebben van de technieken die erachter zitten. Ook jongeren lijken zich op steeds jongere leeftijd schuldig te maken aan online criminaliteit (Van der Wagen e.a., 2019). Zie ook: https://www.politie.nl/nieuws/2023/januari/19/politie-registreert-minder-cybercrime.html
[27] https://www.surf.nl/wat-universiteit-maastricht-leerde-van-de-ransomwareaanval-deel-1

Het concept digitale weerbaarheid is nog relatief nieuw, maar dat komt alleen doordat digitale technologie relatief nieuw is. 'The fact is that digital resilience is a subset of resilience, which is a characteristic of biological, ecological, social, national, and institutional systems that have survived and thrived, some of them since the immemorial' (Rothrock, 2022, p.14). Digitale weerbaarheid gaat er in die zin dus om hoe we leven en werken in een (socio-technische) omgeving die steeds meer verbonden is en complexer wordt. Digitale weerbaarheid is, net zoals weerbaarheid in algemene zin, dus geen keuze, maar onmisbaar en iets waar we actief invulling aan moeten geven. Rothrock gaat nog verder en stelt dat het – beschouwd vanuit een organisatiecontext – een 'state of mind' en 'operational philosophy' is.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV, 2022) ziet dat slachtofferschap vooral voorkomt wanneer onvoldoende basismaatregelen zijn getroffen. De digitale weerbaarheid is niet overal op orde, waardoor burgers en organisaties kwetsbaar zijn voor incidenten (CBS, 2021; CSR, 2021; Furnell & Vasileiou, 2019; NCTV, 2022). Dit probleem speelt niet alleen in Nederland, maar ook in breder Europees en internationaal verband (o.a. ENISA, 2022; SANS, 2022; WEF, 2023a; 2023b). De vraag die vervolgens op komt is: Hoe kunnen we digitale weerbaarheid vergroten en hoe organiseren we dat? In de definitie die zojuist is gegeven komt een aantal kernactiviteiten aan bod. Dit vertaalt zich ruwweg in (i) preventieve acties ('risico's reduceren' en 'incidenten voorkomen'), (ii) repressieve acties ('incidenten ontdekken', 'schade beperken' en 'herstellen') en de aan de definitie toegevoegde (iii) evaluatieve acties ('continu leren'). Vermeld dient te worden dat preventie niet alleen gaat om het voorkomen van incidenten, maar ook om het inperken van de mogelijke impact ervan.

Essentiële eerste stappen voor het realiseren van digitale weerbaarheid – en dit is met name gerede-neerd vanuit organisaties – is volgens Rothrock (2022) het goed in beeld brengen van het eigen netwerk en technische kwetsbaarheden (risico's) – inclusief de externe bereikbaarheid van data en processen – en het organiseren van 24/7 monitoring van de netwerken van de organisatie, om een snelle, actieve verdediging mogelijk te maken. Het is dus onder meer van belang om te weten welke dreigingen relevant zijn en dus een relevant risico kunnen vormen, maar ook welke 'kroonjuwelen' maximaal beschermd moeten worden, welke risico's gecontroleerd kunnen worden en waar restrisico's moeten worden geaccepteerd. Het gaat dus ook om het bepalen van de zogenoemde *risk appetite*; de bereidheid van een organisatie of individu om risico's te nemen bij het nastreven van doelen. Het hebben van een adequate risicoperceptie is essentieel om risico's te kunnen beperken. Het stuurt niet alleen de digitale veiligheidsstrategie op organisatieniveau aan, maar ook de houding van het individu (Alnifie & Kim, 2023; Van Schaik e.a., 2020). Risicopercepties kunnen overigens per type dreiging verschillen (Van Schaik e.a., 2017; 2018).

Een andere belangrijke stap is erkennen dat zelfs bewuste en weerbare eindgebruikers fouten zullen maken en dit feit onderdeel maken van de digitale veiligheids- of weerbaarheidsstrategie. De bescherming van vitale informatie en processen vormt de basis van digitale weerbaarheid. Het omvat ook een herstelplan, waarbij leren van incidenten centraal staat alsook het versterken van het netwerk, de organisatie en medewerkers. Daarnaast moet er niet alleen geleerd worden op het niveau van risicovolle situaties en bijna-incidenten, maar ook van de dingen die goed gaan. Dat laatste bespreek ik uitgebreider in par. 1.4.

In Nederland hebben we naast het Nationaal Cybersecurity Centrum (NCSC) – 'het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland'[28] – ook het Digital Trust Center (DTC) – dat als missie heeft om 'ruim 2 miljoen Nederlandse bedrijven, van zzp'ers [zelfstandigen zonder personeel] tot en met het grootbedrijf, weerbaarder te maken tegen toenemende cyberdreigingen'[29]. Waar het NCSC primair gericht is op de Rijksoverheid en de vitale sector richt het DTC zich op bedrijven binnen de niet-vitale sector. Het DTC hanteert een vijftal basisprincipes waaraan ondernemers moeten voldoen om een minimaal niveau van digitale weerbaarheid te hanteren.[30] Dit noemen we ook wel de basis-cyberhygiëne.

Om meer structureel aandacht te geven aan digitale veiligheid en weerbaarheid kunnen organisaties ervoor kiezen om zich bijvoorbeeld te laten certificeren. Verschillende kwaliteitsmanagementsystemen kunnen daarvoor worden gebruikt, zoals ISO27001.[31] Een tendens die we zien is dat steeds meer bedrijven en organisaties in meer of mindere mate worden verplicht om aan dergelijke certificering te voldoen. Sommige organisaties verwachten dit van bijvoorbeeld leveranciers, maar we zien ook dat internationale wetgeving dergelijke verplichtingen oplegt, zoals met de nieuwe NIS2 richtlijn (zie par. 1.2).

Om de activiteiten die nodig zijn voor digitale weerbaarheid op een adequate wijze op te volgen is een multidisciplinaire aanpak vereist. Daarbij werken we in mijn lectoraat vanuit de driehoek: mens, techniek en organisatie, en houden daarbij rekening met ethiek (zie hoofdstuk 3). De primaire bijdrage van het lectoraat ligt op de menselijke aspecten van digitale weerbaarheid en deels op de organisatorische. We gebruiken theorie en inzichten vanuit de gedragswetenschappen, zoals psychologie, communicatiewetenschap en criminologie, alsook de maatschappijwetenschappen, zoals sociologie en rechtsgeleerdheid. Voor de technische aspecten (cybersecurity) werken we samen met docent-onderzoekers van andere academies en instellingen.

Waarom richten wij ons vooral op digitale weerbaarheid en de menselijke aspecten daarvan? Ten eerste, omdat digitale aanvallen steeds vaker worden gericht op de eindgebruiker. Het is bijvoorbeeld makkelijker voor een kwaadwillende om het wachtwoord van een iPhone rechtstreeks aan een potentieel slachtoffer te vragen dan om het wachtwoord zelf te kraken. Ten tweede, omdat technische maatregelen alleen – hoewel deze een goede basis vormen en in zeker mate verplicht zijn – onvoldoende in staat zijn om criminaliteit en andere vormen van onveiligheid tegen te houden. Ten derde maakt het virtuele en soms internationale karakter online criminaliteit en onveiligheid veelal moeilijk te bestrijden. Rothrock (2022, p.14) zegt hierover: 'Digital security is an incomplete answer. Digital resilience completes the answer.' Eindgebruikers vormen derhalve een essentiële schakel in de veiligheidsketen en vormen dus een belangrijk onderwerp van studie.

1.3.2 De mens als essentiële schakel in de digitale veiligheidsketen

Digitale veiligheid is een verantwoordelijkheid van velen. Een belangrijke verdedigingslinie kan worden opgeworpen door softwareontwikkelaars en hardwarefabrikanten op het moment dat zij veilige producten op de markt brengen. Digitale veiligheid begint namelijk al bij het ontwerp. We leren uit het Cybersecuritybeeld Nederland 2022 echter dat dit geen sinecure is (zie ook par. 1.2). Vervolgens zijn andere partijen aan zet, zoals dienstverleners die hun diensten digitaliseren en via het internet aanbieden, maar bijvoorbeeld ook webbeheerders en internetserviceproviders. De (lokale) overheid kan faciliteren door digitale weerbaarheid te promoten onder hun doelgroepen.

De primaire verdedigingslinie lijkt echter nog steeds toebedeeld aan eindgebruikers. Of het nu gaat om thuisgebruik of werkcontext, eindgebruikers worden zelf verantwoordelijk geacht voor hun eigen digitale veiligheid. En dat betekent dat zij daar dus ook zelf mee aan de slag moeten. Denk hierbij aan het gebruiken van een wachtwoordmanager, het implementeren van multifactorauthenticatie[32] en aan het niet ingaan op een frauduleuze advertentie. Ook zorgvuldig zijn met het online delen van persoonlijke gegevens hoort daarbij. En daar zit ook meteen de crux. De digitale veiligheid kan in het geding komen op het moment dat eindgebruikers zich onveilig gaan gedragen. Niet alleen kan dat henzelf schaden, ook de devices waarmee zij werken kunnen daardoor kwetsbaar worden. Het is daarom van belang om de mens te bestuderen als onderdeel van het digitale veiligheidsdomein (Coventry e.a., 2014; Furnell & Clarke, 2012; Jansen, 2018).

Toch worden vandaag de dag nog veel associaties gemaakt met technische aspecten wanneer wordt gesproken over digitale veiligheid en weerbaarheid, zoals het toepassen van complexe technische veiligheidsmaatregelen en fraudepreventie- en detectiesystemen (Jansen, 2018). Het vakgebied werd dan ook lange tijd gedomineerd door de technische disciplines. Onderzoek op dit gebied was grotendeels gericht op het begrijpen van de technische eigenschappen van informatiesystemen en netwerken om de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen (Kaur e.a., 2021).[33] Het wordt algemeen erkend dat digitale veiligheid niet alleen met technische maatregelen kan worden aangepakt (Arachchilage & Love, 2014; Furnell & Clarke, 2012; Jansen, 2018; Rothrock, 2022). Digitale weerbaarheid omvat dus meer dan alleen techniek.

[28] https://www.nctv.nl/onderwerpen/nationaal-cyber-security-centrum
[29] https://www.digitaltrustcenter.nl/over-het-digital-trust-center
[30] Deze basisprincipes zijn: (1) inventariseer kwetsbaarheden, (2) kies veilige instellingen, (3) voer updates uit, (4) beperk toegang en (5) voorkom virussen en andere malware. Zie: https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen
[31] https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging
[32] Een 'methode om vast te stellen of een gebruiker of digitaal systeem wel is wie of wat hij zegt te zijn' (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.48). Bij deze methode worden minimaal twee factoren gebruikt om in te loggen, bijvoorbeeld naast een wachtwoord (iets dat je weet) ook met een vingerafdruk (iets dat je bent) of een token (iets dat je hebt).
[33] Vertrouwelijkheid wil zeggen dat niet-geautoriseerde gebruikers geen toegang mogen hebben tot de systemen. Integriteit wil zeggen dat men zekerheid heeft over de nauwkeurigheid van data. Met beschikbaarheid wordt de zekerheid tot de beschikking over data bedoeld.

Naast techniek kregen ook organisatorische aspecten veel aandacht. De meeste organisaties richten zich, naast het implementeren van technische beveiligingsmaatregelen, zoals firewalls en antivirussoftware, op het opzetten van goed gedefinieerde beleidsregels en processen, bijvoorbeeld voor het verminderen van datalekken. Ook richten organisaties zich op het garanderen van de bedrijfscontinuïteit door medewerkers aan te stellen die verantwoordelijk zijn voor de digitale veiligheid (Rothrock, 2022).

Hoewel een basis-cyberhygiëne voorwaardelijk moet zijn voor interactie met systemen en netwerken en tot op zekere hoogte een barrière vormt tegen technische aanvallen (NCTV, 2022), kan het niet altijd voorkomen dat eindgebruikers een malware-infectie oplopen, noch kan het eindgebruikers beschermen tegen het vrijgeven van gevoelige informatie aan een dader wanneer zij worden overgehaald om dit te doen (Jansen, 2018). Vanwege de snelle maatschappelijke acceptatie van computersystemen en de daaropvolgende acceptatie van internet, identificeerden onderzoekers tevens nieuwe beveiligingsproblemen die voortkwamen uit de interactie tussen mensen en computers (Furnell & Clarke, 2012; Kaur e.a., 2021; Sasse e.a., 2001).

Ruim twintig jaar geleden merkten Sasse en collega's (2001) op dat menselijke aspecten van digitale veiligheid gemakkelijk worden genegeerd, terwijl mensen over het algemeen worden gezien als de zwakste schakel in de informatiebeveiligingsketen. Ongeveer tien jaar geleden begon de studie naar de menselijke aspecten van digitale veiligheid meer aandacht te krijgen. De belangrijkste reden hiervoor is dat digitale veiligheidsincidenten steeds meer mensen treffen (Furnell & Clarke, 2012). Technologische ontwikkelingen faciliteren dit omdat deze steeds meer geïntegreerd zijn in de samenleving, waardoor ook steeds weer nieuwe dreigingen ontstaan (zie par. 1.2). Menselijke aspecten, zoals cognitieve vaardigheden en risicopercepties, hebben invloed op hun gedrag als eindgebruikers, wat uiteindelijk de effectiviteit van digitale weerbaarheid beïnvloedt. Bovendien zijn eindgebruikers degenen die interacteren met informatiesystemen, waardoor het rekening houden met menselijke aspecten per definitie belangrijk is (Jansen, 2018).

Hoewel het enige tijd heeft geduurd voordat menselijke aspecten voldoende werden erkend in zowel de praktijk als onderzoek, zien we nu dat 'mens, techniek en organisatie' steeds meer worden beschouwd als de drie pijlers van digitale veiligheid, zie bijvoorbeeld het Dreigingsbeeld 2023-2024 van de Informatiebeveiligingsdienst (IBD, 2022). Echter, de aandacht voor menselijke aspecten blijft vaak nog beperkt tot (lopende) awareness campagnes (Hallas, 2018), die niet altijd het gewenste resultaat hebben of slechts een kortstondig effect sorteren (Bullée, 2017; Jansen e.a., 2018). Daarnaast ziet het professionele cybersecurityveld de menselijke actor nog grotendeels als de zwakste schakel. Ik zal in de volgende paragraaf betogen dat dit standpunt achterhaald is. Immers, digitale veiligheidsincidenten ontstaan vaak als gevolg van een combinatie van gebrekkige techniek, falende procedures of tekortschietend (onveilig) ontwerp. Vanuit dit perspectief kunnen menselijke fouten zowel de oorzaak zijn als het gevolg (Zimmermann & Renaud, 2019).

Bovendien stelt Hallas (2018) dat de menselijke factor de sleutel is om vooruitgang te boeken op het gebied van digitale veiligheid. Andere onderzoekers zijn het met deze constatering eens en zien de menselijke factor ook als de achilleshiel voor het bereiken van adequate digitale weerbaarheid (Jansen, 2018; Liang & Xue, 2010; Sasse e.a., 2001; Zimmermann & Renaud, 2019). Gelukkig wordt er steeds meer onderzoek gedaan naar de menselijke aspecten en wordt het belang hiervan al minstens twintig jaar bepleit. Echter, er is nog steeds geen echte verandering in de collectieve manier van denken over de menselijke factor. De huidige tendens onder professionals is dat het onveilige gedrag van eindgebruikers vaak de belangrijkste oorzaak is van het welslagen van een poging tot online criminaliteit. Zo wordt in een recente rapportage van het World Economic Forum (WEF, 2022) bijvoorbeeld vermeldt dat 95% van de cybersecurity problemen zijn terug te voeren op menselijke fouten. Hoewel ik daar anders tegen aan kijk (zie par. 1.4), kunnen we wel stellen dat het bestuderen van menselijk handelen op en/of via internet waardevol is voor het aanpakken en mitigeren van digitale risico's (Coventry e.a., 2014).

Dat we onszelf moeten beveiligen en digitaal weerbaar moeten worden behoeft geen discussie meer. De politiek pakt het op, beleid wordt gemaakt en geïmplementeerd, in onderzoeksagenda's wordt er aandacht aan besteedt en er wordt veelvuldig over gepubliceerd. De bewustwording en erkenning is er dus. Wat achter blijft is het handelen. Waarom blijft dit handelen achter? Dat heeft verschillende oorzaken. Zo kunnen eindgebruikers de juiste expertise en vaardigheden missen om zichzelf weerbaar op te stellen. Naast capaciteit kan het ook ontbreken aan motivatie en gelegenheid. Die motivatie is er overigens vaak wel op het moment dat zich een incident heeft voorgedaan, maar dan is het dus te laat. Ook worden maatregelen ten behoeve van digitale weerbaarheid nogal eens opgevat als kostenpost, terwijl het – in een organisatiecontext althans – ook als een investering kan worden gezien (Hoekstra e.a., 2022; Rothrock, 2022). Grotere organisaties hebben vaak een specifieke afdeling of toegewijd personeel in dienst die zich met het onderwerp bezighouden. Bij kleinere bedrijven is dat minder professioneel (of soms geheel niet) ingericht (Coventry e.a., 2014). In uitzonderlijke gevallen hoorden we van ondernemers zelfs dat ze niet wilden weten hoe hun bedrijf ervoor staat op het gebied van digitale veiligheid.[34]

Het kan ook zijn dat zijn dat regels niet gevolgd worden. We spreken dan over niet-adequate *information security policy compliance* (Cram e.a., 2019; Moody e.a., 2018). Hier kunnen verschillende redenen aan ten grondslag liggen. Medewerkers hebben bijvoorbeeld geen tijd of gebrek aan stimulans om het beleid te lezen, zijn gebrekkig geïnformeerd over waar het beleid te vinden is of snappen de instructies in het beleid simpelweg niet (Albrechtsen, 2007). Verder kan gedacht worden aan de balans tussen het opvolgen van een veiligheidsmaatregel versus de productiviteit. Mensen zijn vooral bezig met het behalen van doelen en uitvoeren van hun taak, en veiligheid is daarbij van secundair belang (Hielscher e.a., 2021). Een veel gehoord argument op de werkvloer is dat het weer iets is dat erbij komt, terwijl het al zo druk is. Ook kan het te maken hebben met de overload aan informatie die mensen op zich afgevuurd krijgen over hoe

[34] https://www.trouw.nl/economie/het-is-goed-hacken-in-een-land-vol-struisvogels~b71e92c8/

veilig om te gaan met digitale diensten en devices (Hielscher e.a., 2021). Daarnaast is het onderwerp niet tastbaar of grijpbaar; de dreiging is veelal niet direct zichtbaar, en dat geldt ook voor de (werking van) maatregelen (Renaud, 2021; Jansen, 2018). Ook kunnen mensen simpelweg fouten maken, bewust of onbewust (Groeneweg, 2018).

Tevens heeft het te maken met hoe burgers of organisaties met risico's omgaan. Aan het ene eind van het spectrum zien we dat mensen geneigd zijn zichzelf te overschatten als het aankomt op digitale veiligheid. Op het moment dat men denkt 'het overkomt mij niet', zal de motivatie laag zijn om iets aan een risico te doen. Dit wordt ook wel geduid met de psychologische term *optimism bias* (Alnifie & Kim, 2023; Pfleeger & Caputo, 2012). Aan het andere eind van het spectrum zien we mensen die er een fatalistische kijk (*rational fatalism*) op na houden (Crossland, 2022), wat we ook wel 'aangeleerde hulpeloosheid' noemen. Dit komt vermoedelijk doordat in communicatie rondom digitale veiligheid vaak wordt gezegd (en daar maak ik mij zelf ook schuldig aan): '100% security bestaat niet' en/of doordat mensen de verantwoordelijk voor veiligheid buiten zichzelf zoeken en die toedichten aan anderen, zoals dienstverleners of werkgevers, of toeleggen aan het lot.[35] Op het moment dat mensen de overtuiging hebben 'dit gebeurt toch wel', en dus het gevoel hebben er niets aan te kunnen doen, is de motivatie ook laag om actie te ondernemen om een risico te verminderen.[36]

Daarnaast zien we in onderzoek terug dat er sprake lijkt te zijn van een algemene risico-onderschatting: 'er valt bij mij niets te halen' of 'ik heb niets te verbergen'. Dit is onjuist, omdat burgers en organisaties wel degelijk iets te verliezen hebben. Denk bijvoorbeeld aan persoonlijke, financiële, klant- en productgegevens. Bovendien, vanuit een organisatieperspectief bekeken, is het nemen van maatregelen in sommige gevallen verplicht. Denk bijvoorbeeld aan de eerder beschreven AVG en de NIS(2) richtlijn. Maar ook burgers dienen goed na te denken over welke informatie ze delen online (en met wie), en welke ze beter niet kunnen delen. Verlies van controle en zeggenschap over data(verwerking) is eveneens een significant issue (Van Boheemen e.a., 2020).

Een belangrijke vraag – en waar we met het lectoraat hopen een antwoord op te kunnen geven – is: Hoe kunnen we eindgebruikers (i) voorbereiden op het herkennen van situaties die afwijken van het normale en (ii) ondersteunen bij het nemen van een bewuste beslissing om situaties te evalueren en waar nodig deze te beëindigen. Tijdens interviews die ik uitvoerde voor mijn promotieonderzoek met slachtoffers van phishing en malware hoorde ik vaak dat er tijdens de poging wel alarmbellen gingen rinkelen of het onderbuikgevoel ingaf dat er iets niet klopte, maar toch waren ze niet bij machte om de poging te stoppen en zijn ze uiteindelijk slachtoffer geworden (Jansen & Leukfeldt, 2016; 2018). In een van onze studies die we reeds met internationale partners aan het uitvoeren zijn, besteden we daar expliciet aandacht aan (zie par. 2.1).

[35] Dit wordt ook wel externe locus of control genoemd (Zie bijv. Jansen e.a., 2017).
[36] Er zijn nog meer heuristieken (vuistregels) en *biases* (systematische denk- en beoordelingsfouten) die van invloed zijn op ons gedrag. Voor een grafisch overzicht, zie: https://upload.wikimedia.org/wikipedia/commons/6/65/Cognitive_bias_codex_en.svg

Om de menselijke aspecten van digitale weerbaarheid aan te pakken, moeten we de factoren die van invloed zijn op menselijk gedrag allereerst goed begrijpen. Daar zijn verschillende theorieën en modellen voor. Denk bijvoorbeeld aan de protection motivation theory (PMT, Maddux & Rogers, 1983; Rogers, 1975), een van de best verklarende theorieën voor het nemen van beschermende maatregelen, en ook veelvuldig toegepast op het gebied van digitale veiligheid (Boehmer e.a., 2015; Boss e.a., 2015; Crossler, e.a., 2013; Haag e.a., 2021; Jansen & Van Schaik, 2017; 2018b), de reasoned action approach (RAA, Fishbein & Ajzen, 2010)[37], een gedragstheorie die verschillende typen gedrag kan verklaren, maar ook aan het capability, opportunity, motivation and behaviour (COM-B) model (Michie e.a., 2011; 2014), waar tevens praktische interventiefuncties aan gekoppeld zijn (i.e., behaviour change wheel).[38] Een determinant uit deze theorieën die op basis van een analyse van diverse empirische studies het sterkt voorspellend en meest consistent lijkt te zijn is zelfeffectiviteit c.q. gepercipieerde gedragscontrole (ENISA, 2019). Zelfeffectiviteit zegt iets over of personen geloven dat zij met succes het gedrag kunnen uitvoeren dat nodig is om een gewenst resultaat te behalen (Bandura, 1977).

Er wordt jaarlijks veel geld geïnvesteerd in bewustwordingscampagnes, gedragsinterventies en dergelijke, maar we zien slachtofferschap nog steeds toenemen.[39] Op het eerste oog lijkt het dan misschien dat we de wedstrijd aan het verliezen zijn. Immers, we investeren veel geld, maar het helpt niet. Echter, de realiteit is dat we nog niet genoeg weten over de effectiviteit van dergelijke campagnes en interventies. Anders gesteld, misschien waren de slachtofferpercentages wel nog hoger geweest wanneer we het zonder deze initiatieven hadden moeten stellen.

Wat cruciaal is wanneer we het hebben over beschermende maatregelen c.q. veilig gedrag is allereerst dat het type gedrag dat we willen bewerkstelligen (i.e., de doelgedraging) uitvoerbaar is door eindgebruikers (Sasse e.a., 2023). Dit lijkt logisch, maar volgens de auteurs worden vaak generieke producten of diensten afgenomen, zonder dat goed is nagedacht over de uitvoerbaarheid van de maatregel alsook de relevantie ervan in de specifieke context. Het is daarbij belangrijk dat het veilige gedrag onderdeel is van de dagelijkse praktijk. Dit betekent ook dat de maatregelen goed afgewogen moeten worden voor wie ze van belang zijn en de gebruiker daarbij zoveel mogelijk centraal stellen (user-centered design). Onderzoek laat zien dat wanneer dit niet het geval is, dat nadelige consequenties heeft voor de effectiviteit van de maatregel (Pollini e.a., 2022). Tevens moeten we ons ervan bewust zijn dat de factoren die een positieve uitwerking hebben op een bepaalde doelgedraging niet per se gelden voor andere doelgedragingen. Tot slot stellen zij dat het creëren van betrokkenheid waardevol is. Wanneer eindgebruikers actief betrokken worden en het gevoel hebben in regie te zijn (*agency*) dan leidt dat tot meer motivatie om aan zelfbeschermend gedrag te werken.

[37] De RAA is een doorontwikkeling van de theory of reasoned action (Fishbein & Ajzen, 1975) en de theory of planned behaviour (Ajzen, 1991). Deze theorieën zijn ook vaker toegepast op onderhavige context (Haag e.a., 2021; Jansen, 2018).
[38] Er zijn nog veel meer theorieën die toegepast kunnen worden op dit vakgebied. Zie bijvoorbeeld het artikel van Moody e.a. (2018) voor een overzicht.
[39] https://cybersecurityventures.com/security-awareness-training-report/

Deze denkrichting sluit aan bij wat ik in de paragraaf hierna bespreek, waarin de mens als oplossing wordt gezien voor het vergroten van digitale weerbaarheid in plaats van het probleem. Om winst te behalen lijkt co-creatie (voor het ontwikkelen van bijv. oplossingen en interventies) hier op zijn plek om te bespreken als interessante aanknopingspunt voor vervolgonderzoek. Er is nog relatief weinig bekend over hoe het participatieve ontwerpproces van digitale veiligheidsmaatregelen van invloed kan zijn op de doeltreffendheid en acceptatie van eindgebruikers voor een dergelijke maatregel. Een wat oudere studie van Albrechtsen en Hovden (2010) toont de waarde aan van werknemersparticipatie bij een informatiebeveiligingsinterventie. Ander onderzoek heeft het principe geïdentificeerd dat duurzame gedragsverandering in de richting van *buy-in* vereist dat mensen informatie verwerken die zij als persoonlijk relevant beschouwen (Uchendu e.a., 2021). De toegevoegde waarde van een dergelijke aanpak is dat het onderzoek direct in de organisatie wordt uitgevoerd en toegepast. Een van de onderzoeksprojecten die we recent toegekend hebben gekregen van Politie en Wetenschap past in dit beeld en wordt besproken in par. 2.3.

Daarnaast is het minstens zo belangrijk dat eindgebruikers worden gefaciliteerd of ondersteund om het gewenste gedrag daadwerkelijk toe te passen. Daar lijkt het momenteel vooral fout te gaan. Het veranderen van gedrag en het aanleren van nieuwe routines is geen sinecure en vergt inspanning. Hielscher e.a. (2021) en Sasse e.a. (2023) stellen dat om nieuw gedrag te laten beklijven, dit gedrag moet worden herhaald over een periode van ongeveer 28 dagen. Ander onderzoek toont dat het effect van security awareness- en educatieve programma's na zes maanden weer op het niveau zit van voor deze interventies (Reinheimer e.a., 2020). Anders gesteld; een eenmalige interventie werkt niet voor gedragsverandering. Hielscher en collega's (2021) presenteren in hun werk de security learning curve; een verdere uitwerking van het originele model van Beyer e.a. (2015; geciteerd in Hielscher e.a., 2021). Het gaat wat te ver om dit model hier geheel toe te lichten, maar het stelt basis-cyberhygiëne als ondergrens en loopt via verschillende stadia, zoals het vergroten van kennis en verbeteren van de houding, en het stimuleren van zelfeffectiviteit en aanleren van daadwerkelijke vaardigheden, door tot het ultieme doel, namelijk veilig gedrag.

Tot slot, als we het hebben over interventies dan is het van groot belang om deze te evalueren. Evaluatie heeft als doel zichtbaar te maken of interventies effectief zijn en of ze adequaat passen in werkprocedures. Continue verbetering van interventies (PDCA)[40] is belangrijk om gedragsverandering en de ontwikkeling van routines en veilig gedrag te ondersteunen (Sasse e.a., 2023). Momenteel is er een groeiende belangstelling voor zogenoemde evidence-based interventies. Dat wil zeggen dat wetenschappelijke inzichten worden toegepast op de ontwikkeling en evaluatie van beleid en praktijk. Wittebrood en Braak (2022) beschouwen dit in het licht van een verwetenschappelijking van beleid en praktijk.[41] Tevens geven zij aan dat momenteel discussie is over hoe strikt evidence-based werken opgevat moet worden; bijvoorbeeld dat er alleen sprake is van 'evidence-based' op het moment dat er randomized controlled trials (RTC) worden uitgevoerd. Hoewel zij bepleiten dat dit niet per se het geval hoeft te zijn, want ook de strikte wetenschappelijke benadering kent beperkingen (zoals de externe validiteit), kunnen we wellicht beter spreken van de term 'evidence-informed'. Dit wil zeggen dat een gedegen kennisbasis onmisbaar is (Wittebrood & Braak, 2022), bijvoorbeeld voor de ontwikkeling van interventies, maar dat tegelijkertijd ook ruimte is voor andere afwegingen.

Met het lectoraat dragen we ook bij aan evaluatiestudies. Twee voorbeelden zijn de evaluaties van de Cyberweerbaarheidsscan van het DTC (Hoekstra e.a., 2022) en een digitale veiligheid bewustwordingsprogramma voor burgers en bedrijven (Jansen & Stol, 2019). Ook evalueerden we 'evidence-informed' interventies middels (quasi)experimenteel onderzoek (Jansen & Van Schaik, 2018a; 2019). Op moment van schrijven zijn we, in opdracht van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) met een evaluatiestudie gestart naar diverse projecten die als doel hebben de digitale weerbaarheid van verschillende doelgroepen te vergroten (zie par. 2.1).

Niet alleen bewustzijn en gedrag verdienen overigens aandacht, ook de context en de behoeften van eindgebruikers moeten worden gekend en erkend om een succesvolle digitale weerbaarheidsstrategie te implementeren. Dit vergt echter een ander perspectief dan hoe nu tegen de menselijke factor wordt aangekeken.

1.4 Een ander perspectief op de mens in de digitale veiligheidsketen

In deze paragraaf zet ik uiteen dat een andere benadering van de mens nodig is die meer recht doet aan de complexe socio-technische context waarin wij ons begeven. In het huidige digitaal veiligheidsperspectief worden nogal eens negatieve associaties gemaakt met menselijke factoren, en wordt de mens zelfs algemeen beschouwd als de zwakste schakel. Hoewel ik erken dat de mens de *primary attack vector* is, ben ik het niet eens met die lezing zoals ik hier zal betogen. Het perspectief dat ik hier beschrijf gaat om het versterken van de mens, die ik dan ook beschouw als een essentiële en in potentie sterke schakel in de digitale veiligheidsketen. Dit perspectief plaatst de eindgebruiker in een positiever daglicht. Kortgezegd gaat het erom om de mens niet zozeer als (de veroorzaker van) het *probleem* te beschouwen, maar juist te beschouwen als een actor die bijdraagt aan de *oplossing*. Om het andere perspectief in context te plaatsen, beschrijf ik hier zowel het 'huidige' als het 'nieuwe' denken.

Een belangrijke inspiratiebron waarbij ik meer ben gaan nadenken over de positieve benadering van de mens komt uit het werk van Erik Hollnagel. Hollnagel is een pleitbezorger van het zogenoemde Safety-II

[40] PDCA, ook wel bekend als de kwaliteitscirkel van Deming, staat voor Plan, Do, Check, Act. De PDCA-cyclus is ontworpen om continue verbetering te bevorderen en een gestructureerde aanpak van het oplossen van problemen aan te moedigen (Spithoven e.a., 2022b).

[41] Andersom zien de auteurs ook de ontwikkeling van een vermaatschappelijking van de wetenschap. Dit is volgens hen ingegeven doordat kwalitatief hoogstaand onderzoek ook maatschappelijk nut moet hebben, bijvoorbeeld omdat onderzoek met publieke middelen wordt gefinancierd (Wittebrood & Braak, 2022).

denken. Het Safety-II perspectief is een benadering van veiligheid die zich richt op de capaciteiten en sterke punten van organisaties en individuen, in plaats van op hun zwakheden. De belangrijkste kenmerken van Safety-II (ten opzichte van Safety-I [Hollnagel, 2014, p.147]) zijn: (i) focus op successen (zoveel mogelijk goed doen, in plaats van zo weinig mogelijk fout doen), (ii) nadruk op aanpassingsvermogen (proactief verbeteren in plaats van reactief), (iii) focus op leren van successen en incidenten (de hoe-vraag in plaats van de schuldvraag beantwoorden), (iv) nadruk op de mens als mogelijke oplossing voor weerbaarheid (in plaats van het risico of de oorzaak van het probleem) en (v) belang van variabiliteit (het erkennen, monitoren en managen van variabiliteit in complexe systemen, in plaats van proberen alle variabiliteit te elimineren).

Beide benaderingen hebben als doel om een veilige werkomgeving te creëren, maar de benadering verschilt in hoe dit wordt bereikt. Safety-II is gericht op het begrijpen van wat er goed gaat en hoe het systeem goed functioneert, en op het bouwen van weerbaarheid en veerkracht om ervoor te zorgen dat het systeem zich kan aanpassen en verbeteren, waarbij Safety-I dus is gericht op het identificeren en beheersen van risico's om ongevallen te voorkomen. Een voorbeeld van Safety-II in digitale veiligheid is dat een organisatie een mechanisme implementeert om onregelmatigheden of potentiële veiligheidsincidenten te melden, zodat deze snel kunnen worden aangepakt en verbeterd, waarbij voor Safety-I eerder gedacht kan worden aan een organisatie die periodiek beveiligingsaudits uitvoert om potentiële zwakke plekken in het systeem te identificeren en deze te verhelpen om zodoende de veiligheid te verbeteren.

Hollnagel (2014) beschouwt de mens als beter in staat dan technologische systemen om gebreken en fouten te herkennen en te interpreteren, en om te bepalen wat er nodig is in specifieke situaties. De mens kan handelen door te detecteren, te corrigeren en in te grijpen voordat het erger wordt, door middel van zelf nadenken en reflectie in plaats van alleen de taak uit te voeren die van hem of haar wordt verwacht. Uiteraard moet dit – gezien de digitale context – samengaan met technische monitoring en detectie wat ook nodig is om de systemen en het dataverkeer te analyseren.

Binnen Safety-II wordt er overigens niet van uit gegaan dat mensen geen fouten maken. In plaats daarvan wordt erkend dat fouten en successen twee kanten van dezelfde medaille zijn en dat beide labels pas achteraf kunnen worden toegekend (Hollnagel, 2014). Ook ligt binnen Safety-II een nadruk op samenwerking. Voor het bereiken van veiligheid – alsook voor digitale weerbaarheid – geldt dat het een collectieve verantwoordelijkheid is (zie ook Pollini e.a., 2022). Door een cultuur van vertrouwen en open communicatie te bevorderen (bijv. voor het melden van [bijna-]incidenten zonder angst voor vergelding), kunnen organisaties hun veiligheidsprestaties verbeteren. Dit wordt ook wel aangeduid als Just Culture.

Een andere inspiratiebron betreft het werk van Sidney Dekker. Hij hangt een gedachtengoed aan dat hij Safety Differently noemt en heeft ook veel geschreven over Just Culture. Safety Differently stelt, net als Safety-II, traditionele opvattingen over veiligheid en ongevallenpreventie ter discussie (Dekker, 2012; 2014; Dekker & Conklin, 2022). Dit gedachtengoed beweegt weg van de traditionele veiligheidsbenadering van regels, procedures en naleving, maar benadrukt meer het belang van menselijke prestaties, complexiteit en systeeminteracties; mensen maken fouten, en deze fouten zijn niet noodzakelijkerwijs de oorzaak van ongevallen. Daarnaast ligt ook hier de focus op dat wat goed gaat, het *empoweren* van medewerkers en continu leren.

Beide benaderingen zijn ontstaan uit onvrede over hoe de praktijk omgaat met de veiligheidsvraagstukken van vandaag de dag. De huidige manier van denken is gebaseerd op een context die vrij stabiel, ontleedbaar en begrijpelijk is. Die context is echter niet meer accuraat, nu we ons bewegen in een complex socio-technisch systeem waarin zowel sociale c.q. menselijke (eindgebruikers en hun interactie met technologie), technische (hardware en software) en organisatorische (beleid en procedures) elementen met elkaar verweven zijn, door elkaar heen lopen en elkaar voortdurend beïnvloeden (Coventry e.a., 2020; Pollini e.a., 2022; Zimmermann & Renaud, 2019). Eveneens spelen externe factoren een rol, zoals bestuurlijke en wetgevende (waaronder ethische) elementen (Zimmermann & Renaud, 2019).

Bovendien wijst Hollnagel (2008; 2014) ons erop dat veiligheid over het algemeen niet wordt gemeten zoals het bedoeld is, omdat we geen successen meten, maar ons vooral richten op (het voorkomen van) incidenten en mislukkingen (zie ook Dekker, 2014). Deze focus op het bestuderen van mislukkingen en zwakheden kan echter resulteren in een beperkt begrip van wat ervoor zorgt dat dingen goed werken. Door successen te bestuderen, kunnen we inzicht krijgen in de factoren die hieraan bijdragen. Het is belangrijk om een evenwicht te vinden tussen het leren van mislukkingen en successen, en te erkennen dat beide waardevolle leermogelijkheden bieden.

Verder wordt gesteld dat de meeste dingen in de meeste gevallen 'gewoon' goed gaan.[42] We moeten dus de misvatting loslaten dat nul 'gebeurtenissen' het enige acceptabele veiligheidsresultaat is en dat elk incident of bijna-ongeval een duidelijke oorzaak heeft (Dekker & Conklin, 2022). Om deze redenen moeten we ook voor digitale weerbaarheid toe naar een 'nieuw' of beter gezegd 'aanvullend' veiligheidsperspectief. Ik wil niet bepleiten dat het ene perspectief boven de andere staat. Het moet vooral als een complementair perspectief worden beschouwd, waarbij het doel is om de mens in zijn kracht te benutten alsook te leren van dingen die goed gaan (Zimmermann & Renaud, 2019).

Voor digitale veiligheid hebben Zimmermann en Renaud (2019) de eerste stappen gezet om het aanvullende perspectief op papier te zetten. Zij stellen ook dat de huidige conceptualisering van de 'mens-als-probleem' gebrekkig is en moet verschuiven naar een 'mens-als-oplossing' benadering. Zij pleiten voor een zogenoemde Cybersecurity Differently benadering, waarbij de mens wordt gezien als iemand met goede intenties en als integraal en onmisbaar onderdeel van de oplossing. Zij zijn van mening dat de problemen die ontstaan met betrekking tot digitale veiligheid – net zoals in andere toepassingsgebieden – niet zijn geworteld in menselijk handelen, maar eerder in de complexiteit van de digitale omgeving.

[42] https://safetydifferently.com/why-do-things-go-right/

Zimmermann en Renaud (2019) beschrijven de belangrijkste principes van Cybersecurity Differently, waarbij de mens als oplossing wordt gezien. De hoofdlijnen zijn: (i) een focus op successen, (ii) het stimuleren van leren, communiceren en samenwerking, (iii) het uitgaan van iemands expertise en (iv) een balans vinden tussen tegenhouden (*resistance*) en weerbaarheid. De huidige tred, Cybersecurity Currently, die uitgaat van de mens als probleem is vooral gericht op: (i) het voorkomen van fouten, (ii) het uitsluiten, trainen, beheersen en beperken van mensen, (iii) de adequaatheid van beleid en (iv) de tegenhouden-modus.

Menselijke actoren zijn dus een belangrijke troef, maar ze moeten serieus worden genomen en worden gefaciliteerd om dit te doen. In de huidige praktijk wordt deze verantwoordelijkheid vaak neergelegd bij de chief information security officer (CISO). Voor een deel is dat begrijpelijk, omdat de CISO een belangrijke formele rol heeft aangaande informatiebeveiliging. Maar voor digitale weerbaarheid moet, zoals gezegd, de verantwoordelijkheid over de gehele organisatie worden verdeeld. Dit wordt ook onderschreven door Rothrock (2022) die stelt dat digitale weerbaarheid zowel van *top down* als *bottom up* bereikt kan worden. Wanneer elke individuele medewerker medeverantwoordelijk is voor digitale veiligheid, en aandacht besteedt aan mogelijke aanvallen en potentiële problemen, zal dat het competentie- en prestatieniveau naar verwachting doen laten stijgen. Dit wil overigens niet zeggen dat iedereen een cybersecurity-expert hoeft te worden.

Uiteindelijk zouden we toe moeten bewegen naar het ultieme doel, de stip op de horizon, en dat is het cultiveren van een cybersecuritycultuur; een cultuur waarin iedere medewerker medeverantwoordelijk is voor digitale veiligheid en procesoptimalisatie de standaard is geworden (Furnell & Vasileiou, 2019). Uchendu en collega's (2021) voerden een state-of-the-art onderzoek uit naar cybersecuritycultuur van organisaties. De twee meest genoemde factoren die hierop van invloed zijn die zij vonden in hun analyse van 58 artikelen zijn: de steun en het leiderschap van het topmanagement, en het hebben van duidelijk beleid en procedures. Beveiligingsbewustzijn en trainingsprogramma's zijn daarna de meest genoemde factor die van cruciaal belang is bij het cultiveren van een cybersecuritycultuur. Andere literatuuroverzichten over informatiebeveiligingscultuur (Glaspie & Karwowski, 2017; Nasir e.a., 2019) erkennen ook de drie hier genoemde kernpunten (zie ook Da Veiga, 2019), hoewel ze stellen dat er geen gemeenschappelijke overeenstemming bestaat over de factoren en dimensies die verband houden met dit concept.[43]

Een stap naar cybersecuritycultuur kan liggen in de adoptie van *secure routines* en het faciliteren daarvan zoals voorgesteld door Sasse en collega's (2023). Zoals besproken is de omgeving daarin van onmiskenbaar belang (Michie e.a., 2011). Dat dit soms ingewikkeld is illustreren Hielscher e.a. (2021) aan de hand van het promoten van VPN-gebruik[44]; een effectieve manier om privacy te beschermen. In een werkcontext blijkt het lastig om deze gedraging onderdeel te laten worden van de routine bij thuis- of op afstand werken, omdat verbinding maken met een VPN op het kantoor niet nodig is. Een interventie gericht op de omgeving of de dagelijkse routine brengt dan geen verandering. In plaats daarvan moeten de *cues* op de het apparaat zelf worden gewijzigd. Dit kunnen we ook deels als 'de omgeving' interpreteren. Hierbij zou *nudging*, het met zachte hand en in de gewenste richting beïnvloeden van gedrag, uit het domein van behavioural economics, een rol kunnen vervullen (Thaler & Sunstein, 2009). Door het toepassen van nudges kunnen eindgebruikers net dat subtiele duwtje krijgen waardoor ze 'als vanuit zichzelf' de meest veilige optie kiezen wanneer zij worden geconfronteerd met het moeten maken van een veiligheidsbeslissing.[45] Van Steen en De Busser (2021) hebben een bondige review geschreven over het toepassen van dergelijke principes in het ontwerp. Zij noemen dit security by behavioural design.

Hielscher e.a. (2021) noemen in de door hen gepresenteerde security learning curve (SLC) een interessant concept waar volgens hen nog onvoldoende aandacht aan wordt besteed in termen van gedragsverandering. Het gaat namelijk niet alleen om het aanleren van nieuw gedrag c.q. veilige routines, maar ook om het afleren of 'intentioneel

[43] In de literatuur worden de termen informatiebeveiligingscultuur en cybersecuritycultuur wisselend gebruikt. Ook wordt soms gesproken van veiligheids- of securitycultuur in relatie tot digitale veiligheid. Wiley e.a. (2020) tonen in hun onderzoek een positieve lineaire relatie aan tussen organisatie- en veiligheidscultuur, en laten zien dat veiligheidscultuur de relatie tussen organisatiecultuur en digitaal veiligheidsbewustzijn medieert.

[44] VPN staat voor Virtual Private Network en is een 'uitbreiding van een computernetwerk over een openbaar netwerk. Via die uitbreiding kunnen gebruikers vanaf elke plek veilig gegevens delen met het computernetwerk' (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.76).

[45] Zie de overzichtsstudie van Zimmerman en Renaud (2021) over de toepassing van nudging op cybersecurity.

vergeten' (*intentional forgetting*) van oud gedrag c.q. onveilige routines. Verder stellen ze dat een van de centrale acties in de SLC het stimuleren van zelfeffectiviteit is. Zoals eerder vermeld is zelfeffectiviteit een van de sterkste en meest consistente verklarende variabelen voor veilig gedrag. Zelfeffectiviteit wordt gestimuleerd door positieve feedback. Niet alleen gedurende een interventie, maar ook tijdens het dagelijkse werk (Sasse e.a., 2023). De aanvullende – positieve – benadering lijkt dus ook hiervoor een gunstig raamwerk te bieden.

Een concept dat tegen cybersecuritycultuur aan schuurt is organisational citizenship behaviour (OCB) (Sasse e.a., 2023). Yen e.a. (2008) laten een positieve relatie zien tussen OCB en *information systems success*, en daarmee potentieel ook voor digitale weerbaarheid. Het biedt in ieder geval een mooi perspectief voor nader onderzoek, waarbij het dan ook interessant is om te kijken in hoeverre het thuiswerken – dat we steeds massaler en frequenter doen[46] – van invloed is op OCB en daarmee op digitale veiligheid.

Uiteindelijk gaat het bij digitale weerbaarheid binnen organisaties erom dat men met elkaar moet leren, communiceren en samenwerken. Naar mijn mening kan het gesprek over digitale weerbaarheid op de werkvloer de eerste praktische stap zijn om hieraan te gaan werken. Dit kan door het bevorderen van de aanspreekcultuur, maar ook door het onderwerp op de agenda te zetten en gesprekken erover te faciliteren. Daar zijn verschillende mogelijkheden voor. Binnen NHL Stenden Hogeschool hebben we zogenoemde 'data protection counselors' in dienst, alsook 'digicoaches'. Dit zijn benaderbare collega's die op de werkvloer andere collega's kunnen ondersteunen bij vragen en problemen op digitaal gebied, waarbij de eerste vooral op strategisch niveau opereert (privacy en security) en de tweede meer op functioneel niveau. Andere voorbeelden zijn cybersecurity champion programma's die binnen organisaties worden uitgerold (Becker e.a., 2017) en digitale buurtambassadeurs die in wijken worden ingezet.[47] Om deze gesprekken zinvol te maken, is het echter belangrijk om een gemeenschappelijke taal te ontwikkelen en gebruiken die iedereen begrijpt. De taalbarrière – veelal veroorzaak door technisch jargon – moet worden weggenomen.

Hoewel de Safety-II en Safety Differently benaderingen interessant lijken, is empirisch bewijs – zowel buiten als binnen de digitale veiligheidscontext – vooralsnog beperkt voorhanden. Ook het werk van Zimmerman en Renaud (2019) wordt nog relatief weinig benut. Het 'andere' perspectief dat hier is besproken, werk ik op moment van schrijven theoretisch verder uit met collega's van het lectoraat Maatschappelijke Veiligheid van Saxion Hogeschool. Wij achten, gezien de instabiele en vijandige digitale omgeving waarin organisaties zich tegenwoordig bevinden, en die voortdurend veranderd, het cruciaal om digitale weerbaarheid holistisch te beschouwen. Deze redenering wordt ook door anderen ondersteund (Morgan e.a., 2020; Pollini e.a., 2022). Het creëren van een werkomgeving gebaseerd op openheid, vertrouwen en samenwerking, waarbij medewerkers gesteund en gefaciliteerd worden, is daarin een belangrijke randvoorwaarde (Sasse e.a., 2023). Daarbij verkennen we eveneens mogelijkheden om dit perspectief nader empirisch te onderzoeken.

[46] https://www.rijksoverheid.nl/actueel/nieuws/2021/07/14/onderzoek-wijst-uit-thuiswerken-is-een-blijvertje
[47] https://hetccv.nl/onderwerpen/cybercrime/database-lokale-cyberprojecten/digitale-buurtambassadeurs-in-breda/

Zodoende krijgen we een betere kijk op wat deze benadering betekent voor het digitale weerbaarheidsveld.

1.5 De rol van de politie in een digitaliserende samenleving

Wanneer het gaat over digitale veiligheid en digitale weerbaarheid is het allereerst van belang om zoveel mogelijk risico's te voorkomen. Vervolgens is het noodzakelijk om werkwijzen te hebben om de impact te reduceren en te herstellen wanneer dat nodig is. In die zin vormen burgers en organisaties de eerste verdedigingslinie tegen digitale onveiligheid. De politie komt aan bod op het moment dat burgers en organisaties 'er op eigen kracht niet meer uitkomen' (Stol, 2010, p.23). In deze paragraaf ga ik nader in op de uitdagingen die voor de politie spelen in een digitaliserende samenleving en hoe de politie daarmee kan omgaan. Ik beperk mij voor wat betreft het tweede deel tot waar de politie het meest mee worstelt c.q. de aspecten waaraan het lectoraat een bijdrage gaat leveren, namelijk digitale kennis en vaardigheden. De politieorganisatie (inclusief de Politieacademie waarvoor ik werkzaam ben) vormt een belangrijke omgeving voor het lectoraat, omdat we daarbinnen een groot deel van ons werk gaan doen; ons living lab.

1.5.1 Uitdagingen voor de politie

De afgelopen jaren hebben verschuivingen in het digitale landschap het politiewerk flink beïnvloedt (Van Lakerveld e.a., 2017; 2018; Schreuders e.a., 2018). Het gaat daarbij om veranderingen in de interne werkomgeving, zoals werkprocessen en informatievoorziening, alsook om de externe werkomgeving, zoals online communicatie en online criminaliteit. Met de verspreiding van technologie, sociale media en internet staat de politie voor nieuwe en complexe uitdagingen in de digitale wereld.

Deze uitdagingen zijn ingegeven door technische complexiteit, netwerkcomplexiteit, echtheidscomplexiteit en cyborgcomplexiteit (Stol, 2020; Stol & Bantema, 2021; Stol & Jansen, te verwachten). Technische complexiteit houdt in dat mensen niet gemakkelijk de digitale omgeving kunnen doorzien, wat kan leiden tot fouten en kwetsbaarheden. Netwerkcomplexiteit is het gevolg van de uitgebreide netwerken van aangesloten apparaten, waardoor het lastig is om goed zicht te krijgen op het geheel van verbindingen. Deze twee samen kunnen we beschouwen als onderdeel van het complexe socio-technische systeem waar ik het eerder over had (par. 1.4). Echtheidscomplexiteit ontstaat omdat het moeilijk kan zijn om te zeggen wat echt is en wat nep in de online wereld (Jansen e.a., 2019). Tot slot wordt cyborgcomplexiteit veroorzaakt door de 'versmelting' van technologie en het menselijk lichaam, wat kan leiden tot nieuwe en/of aangepaste vormen van misdaad en politie-uitdagingen (Borwell e.a., 2021a; Van der Wagen, 2018). Denk bij deze laatste bijvoorbeeld aan hoorapparaten, pacemakers en neuroprotheses (Stol & Jansen, te verwachten).[48]

[48] Verbeek (2011, p.14) benadrukt dat mens en technologie steeds verder verweven raken, 'zelfs zodanig dat het steeds lastiger wordt om een grens tussen beide te trekken'. Van Mensvoort (2019) onderkent dit en geeft daarbij aan dat technologie niet alleen onze omgeving verandert, maar ook de mens zelf. We merken dat al met mobiele telefoons die in relatief korte tijd de transitie maakten 'van onbekend naar vertrouwd naar onmisbaar' (Van Mensvoort, 2019, p.63). Hij stelt dat hoewel dit apparaat niet in ons lichaam zit, het een verlengstuk is geworden van onze hersenen en beleving.

Deze vier vormen van complexiteit zijn met elkaar verweven en kunnen niet van elkaar worden gescheiden, maar echtheidscomplexiteit is bijzonder zorgwekkend omdat dit het gevoel van waarheid en realiteit van mensen kan aantasten (Jansen e.a., 2019; Jansen & Stol, te verwachten). George Orwell beschrijft in zijn boek '1984' treffend dat onderscheid hierin kunnen maken cruciaal is voor individuele vrijheid en democratie. In een onderzoek van Accenture (2022) kwam naar voren dat 65% van de 24.000 ondervraagde consumenten weinig tot geen vertrouwen heeft in zichzelf bij het herkennen of identificeren van deepfake[49] video's of andere synthetische inhoud.[50] Aangezien digitalisering zich in hoog tempo blijft ontwikkelen, bijvoorbeeld op het gebied van kunstmatige intelligentie[51], moet de politie zich aanpassen aan deze complexiteiten om (online) criminaliteit effectief te bestrijden, gemeenschappen veilig te houden alsook om in verbinding te blijven staan met deze gemeenschappen.

Deze complexiteiten brengen diverse uitdagingen met zich mee voor de politie. Belangrijke uitdagingen zijn: online criminaliteit, openbare orde, communicatie met burgers, privacy en ethiek, en het opvijzelen van kennis en vaardigheden aangaande digitale aspecten van politiewerk (Stol & Jansen, te verwachten).[52] Daarbij moet de politie eveneens inspanningen verrichten om de eigen organisatie en medewerkers digitaal fit en weerbaar te maken én te houden.[53] Deze uitdagingen worden hierna beknopt toegelicht.

Een van de grootste uitdagingen waarmee de politie wordt geconfronteerd, is de opkomst van online criminaliteit. Kwaadwillenden gebruiken steeds vaker digitale technologieën om een breed scala aan misdaden te plegen, van identiteitsdiefstal en -fraude tot DDoS-aanvallen en online intimidatie (zie par. 1.2). Omdat criminaliteit is gedigitaliseerd, betekent dit dat ook het werkaanbod voor de politie is veranderd. Naast waakzaam en dienstbaar te zijn in de offline wereld, moet de politie dat ook zijn in de online wereld.[54] Omdat de online realiteit sterk is verweven met de fysieke realiteit, en daarmee met het dagelijks werk van politiemensen, kunnen we niet meer spreken van bijvoorbeeld 'regulier' of 'digitaal' politiewerk. Het is steeds moeilijker om dit te scheiden (De Vries & Henssen, 2018), omdat aspecten van deze realiteiten steeds meer door elkaar heen lopen.[55] Denk bijvoorbeeld aan smartphones die onderdeel zijn van de opsporing van traditionele criminaliteit. Het gaat dus gewoon om 'politiewerk'.

Terpstra en collega's (2021) stellen dat de kern van het politiewerk niet is veranderd. Politiemensen hebben – net zoals voorheen – veelal te maken met overlast, veelvoorkomende criminaliteit, en sociale en openbare ordeproblematiek. De politie moet echter wel goed thuis zijn in de nieuwe technologieën om dergelijke misdaden en problemen aan te pakken (voorkomen, verstoren/stoppen en gerechtelijk afdoen)[56], en bewust zijn van de consequenties van digitalisering. Ter illustratie, data kunnen enerzijds vluchtig zijn, waardoor snelle actie nodig is om digitale sporen veilig te stellen. Anderzijds kunnen data (bijv. afbeeldingen en video's) permanent rondzwerven op internet, waardoor slachtoffers continu aan een betreffend feit herinnerd worden; en het herstel van slachtofferschap daardoor moeizamer gaat.

Een uitdaging die speelt bij online criminaliteit is dat criminelen hun modus operandi steeds meer verfijnen en technologie gebruiken, zoals VPN, om hun identiteit en locatie te verhullen. De politie moet continu, binnen het juridisch kader, strategieën en werkwijzen bedenken om daar een antwoord op te vinden (Jansen e.a., 2020; 2023). Bovendien is het speelveld complex omdat verschillende actoren een rol spelen bij digitale veiligheidsproblemen. Ook vormt de internationale context een uitdaging. Dit maakt het voor de politie noodzakelijk – om effectief criminaliteit aan te pakken – om samen te werken met wetshandhavingsinstanties over de hele wereld. Dit vereist een hoog niveau van samenwerking evenals begrip van internationale wet- en regelgeving. Hoewel dit de nodige uitdagingen biedt, behaalt de politie ook regelmatig successen op dit terrein.[57,58]

Een illustratief voorbeeld is het opsporen van online aankoopfraude uit het buitenland (Jansen e.a., 2019). Hierbij zijn diverse actoren betrokken, zoals handel- en veilingsites, banken, payment service providers (bedrijven die online betaaloplossingen aanbieden, zoals iDeal), escrow-diensten (tussenpartijen die de belangen van kopers en verkopers behartigen), transportbedrijven, en natuurlijk consumenten, criminelen, hun eventuele handlangers, en (buitenlandse) politiediensten. In het geval van valse webshops komen daar nog internetserviceproviders en organisaties voor de registratie van domeinnamen bij. Een veiligheidsprobleem als online aankoopfraude laat zich lastig opsporen en dat kunnen we derhalve niet alleen over laten aan de politie, maar moet breder worden aangepakt. Zowel het voorkomen als het verstoren/stoppen van criminele handelingen die nodig zijn voor de realisatie van het delict horen daarbij (Jansen e.a., 2019; Leukfeldt & Jansen, 2020). Bovendien lijken die strategieën effectiever dan opsporing. Dit lukt overigens alleen wanneer publieke en private partijen integraal (ook internationaal) met elkaar samenwerken (CSR, 2021). Een moeilijkheid hierbij

[49] Een deepfake betreft 'inhoud (video, audio of anderszins) die volledig of gedeeltelijk is verzonnen of bestaande inhoud (video, audio of anderszins) dat is gemanipuleerd' (Van der Sloot & Wagensveld, 2022, p.1, vertaald uit het Engels).
[50] Deepfakes worden met ransomware en cybercrime-as-a-service bestempeld als grote risico's voor de komende tijd. Zie: https://www.agconnect.nl/artikel/deepfakes-ransomware-en-cybercrime-service-grote-risicos-voor-2023
[51] Ter illustratie zie het artikel van Europol over het criminele gebruik van ChatGPT: https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models
[52] Er zijn nog veel meer onderwerpen en uitdagingen die verband houden met digitalisering. Denk bijvoorbeeld aan informatiegestuurd politiewerk en technologische innovatie. Omdat dit buiten het bereik van het onderzoek van het lectoraat valt, ga ik daar niet op in. Dergelijke onderwerpen worden overigens wel expliciet behandeld binnen het kenniscentrum Digitalisering, Opsporing en Technologie van de Politieacademie (zie par. 3.1).
[53] https://www.politie.nl/nieuws/2020/december/1/politie-investeert-in-digitale-fitheid.html
[54] Artikel 3 van de Politiewet stelt: 'De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'
[55] https://open.overheid.nl/documenten/ronl-a850d2e1-5355-4ef3-aeaf-48f2f9ce5e71/pdf
[56] Deze drie interventies hebben betrekking op gelegenheidsstructuren, (potentiële) daders en (potentiële) slachtoffers.
[57] https://www.politie.nl/nieuws/2023/februari/3/politie-leest-opnieuw-mee-met-criminelen.html
[58] https://www.politie.nl/nieuws/2023/april/5/operation-cookiemonster-nl.html

is dat informatie-uitwisseling in de praktijk soms lastig blijkt, maar ook dat sommige partijen niet mee willen (of kunnen) werken.

Hoewel al snel de link wordt gelegd met de internationale dimensie, immers online criminaliteit is niet gebonden aan (lands)grenzen, moeten we de lokale context niet vergeten. De meeste online criminaliteit waarvan inwoners van Nederland slachtoffer worden, wordt 'gewoon' door andere inwoners van Nederland gepleegd (Roks & Monshouwer, 2022). Deze bevinding en de hoge slachtoffercijfers van online criminaliteit vertellen ons dat de politie (en haar partners) lokaal steeds vaker met online criminaliteit in aanraking komt (Spithoven e.a., 2022a; Terpstra e.a., 2021). Lokaal kunnen politiemensen samen met veiligheidspartners een waardevolle rol vervullen om online criminaliteit aan te pakken (Leukfeldt e.a., 2020b; Stol e.a., 2013; Terpstra e.a., 2021). Immers, een lokaal veiligheidsprobleem vergt een lokale aanpak (RBPO Noord-Nederland, 2023). Ook in het buitenland wordt de lokale aanpak beschouwd als een benadering die heel waardevol kan zijn (Brunner, 2020; Hadlington e.a., 2018; Hull e.a., 2018; Holt & Bossler, 2012). Tegelijkertijd hebben we in een recent onderzoek geconstateerd dat het kennisniveau van digitale aspecten van politiewerk op lokaal niveau (basisteams) juist het minst aanwezig is (Jansen e.a., 2020; Van Valkengoed, 2017). Dit is nadelig, omdat dit de eerste plek is waar slachtoffers zich komen melden en waar wijkagenten signalen kunnen waarnemen (bijv. activiteiten van geldezels en hun ronselaars).

Bovenstaande uitdagingen gelden eveneens voor fenomenen als polarisatie en desinformatie, die zijn meegegroeid met de opkomst van social media, die voor toenemende maatschappelijke spanningen kunnen zorgen. Daarbij speelt ook het handhaven van de *fysieke* openbare orde een rol. Stol (2020; 2021) beschrijft dat burgers hedendaags beschikken over meer 'organisatievermogen' alsook 'informatievermogen' dankzij digitalisering. Burgers kunnen digitale middelen namelijk gebruiken om zich te organiseren (bijv. demonstraties, rellen en vechtpartijen).[59] Fenomenen die hier betrekking op hebben zijn zogenoemde online aangejaagde ordeverstoringen (De Vries & Bantema, 2022), maar ook een cybercrisis kan leiden tot openbare ordeproblemen (zie par. 1.2). Omdat informatie snel opduikt en wordt verspreid via internet, en bovendien deels voor de politie is afgeschermd, kan dat volgens Terpstra e.a. (2021) ook nog eens leiden tot een 'informatieachterstand'. Hoe het zit met de openbare orde *online* is nog onduidelijk, maar het lijkt een kwestie van tijd dat daar vanuit politie en partners (zoals gemeenten) nadrukkelijker naar wordt gekeken en acties op worden ondernomen (Stol & Jansen, te verwachten). Daarbij is het de vraag in hoeverre er verschil zou moeten zijn tussen fysieke en online openbare orde.

De communicatie met burgers is ook een aandachtsgebied voor de politie dat onder andere door gebruik van social media is veranderd (Van Lakerveld e.a., 2017; Van Steden e.a., 2021; Terpstra e.a., 2021). Uit een onderzoek van Van Steden en collega's (2021) over politie en sociale media blijkt dat de politie sociale media vooral gebruiken voor het zenden van informatie, maar ook dat veel onduidelijkheid bestaat over de effectiviteit van politie-initiatieven. De politie onderzoekt hoe in een digitale samenleving gewerkt kan worden aan de relatie politie-publiek, waarbij digitale wijkagenten een sleutelrol spelen. De politie zet stappen in webcare (het onderhouden van contact met burgers en organisaties) en dienstverlening via digitale middelen. Voorbeelden hiervan zijn chatbot Wout[60] en de internetaangifte (Borwell, e.a., 2020). De ontwikkeling bevindt zich echter nog in de beginfase en er is meer onderzoek nodig om de effectiviteit van deze manier van werken te onderzoeken (Stol & Jansen, te verwachten). Naast digitale aanwezigheid blijven fysieke nabijheid en benaderbaarheid overigens noodzakelijk (Terpstra e.a., 2021), iets wat onder druk kan komen te staan door toedoen van de digitalisering van politiewerkzaamheden (Van Lakerveld, 2018).

Ook zorgen rondom privacy en ethiek voor het eigen optreden spelen om uiteenlopende redenen een rol voor de politie. Dit geldt temeer naarmate de politie gebruik maakt van digitale technologieën, zoals drones[61] en gezichtsherkenningssoftware[62], vergaande analysemogelijkheden toepast waarbij verschillende datasystemen aan elkaar gekoppeld worden (i.e., big data; Van Lakerveld e.a., 2018) of bijvoorbeeld gaat monitoren op social media als informatiebron om potentiële dreigingen te identificeren (Bantema e.a., 2021).

Uiteraard moet de politie ook investeren in de digitale weerbaarheid van de eigen organisatie en haar personeel om de digitale infrastructuur en data te beschermen tegen digitale dreigingen en risico's. Ook het beheer en verwerken van data horen daarbij, wat tevens onder de juiste juridische voorwaarden moet geschieden, transparant en controleerbaar moet zijn. De enorme hoeveelheden digitale gegevens die de politie verzamelt en opslaat – denk aan persoonsgegevens en digitaal bewijs – kunnen immers ook leiden tot privacyvraagstukken, bijvoorbeeld wanneer deze onjuist verwerkt worden of worden gelekt/gestolen. Kortom, door het verbeteren van de digitale kennis en vaardigheden van politiemensen wordt niet alleen het digitale handelingsrepertoire, de digitale weerbaarheid en de digitale veiligheid van individuele politiemensen vergroot (bijv. het voorkomen van doxing[63] en het oplossen van een onderzoek naar online criminaliteit), maar verbetert ook de digitale weerbaarheid van de hele politieorganisatie (bijv. het voorkomen van datalekken).

1.5.2 Inzet op kennis en vaardigheden

Om de uitdagingen in het effectief handelen door de politie aan te pakken, moeten politiediensten investeren in de nodige middelen en trainingen om het snel veranderende digitale landschap bij te houden (Cockcroft e.a., 2018; Jansen e.a., 2020; POR, 2020; Schreuders e.a., 2018). Dit omvat de uitbreiding van gespecialiseerde eenheden en personeel dat is opgeleid in bijvoorbeeld digitaal forensisch onderzoek en hightech cybercriminaliteit, maar het

[59] Burgers kunnen zich natuurlijk ook ten positieve organiseren via digitale middelen. Een voorbeeld daarvan betreft WhatsApp BuurtPreventie (WABP). Een opmerkingen daarbij is dat aan WABP ook enkele nadelen kunnen kleven (Stol & Bantema, 2021).

[60] https://www.politie.nl/onderwerpen/wout.html

[61] https://nos.nl/artikel/2399774-chinese-drones-van-rijkswaterstaat-en-politie-mogelijk-onveilig

[62] https://www.volkskrant.nl/nieuws-achtergrond/nederlandse-politie-gebruikte-controversiele-gezichtsherkennings-software-minimaal-vijftig-keer~b6aa77d4/

[63] Doxing is 'het proces waarbij vertrouwelijke informatie over een persoon of organisatie publiek wordt gemaakt. Dit gebeurt doorgaans via het internet. Deze informatie wordt verkregen via open bronnen, social engineering of via (vaak ongeautoriseerde) toegang tot gesloten systemen' (Cybersecurity Alliantie & Cyberveilig Nederland, 2021, p.33). Doeleinden van doxing omvatten afpersing en beschaming.

vereist ook het ontwikkelen van personeel in de bredere politieorganisatie (Stol, 2018; Jansen e.a., 2020). Ook hierin worden al initiatieven ontplooid, zoals onder meer te lezen is in het rapport van Schiks en collega's (2022) en in scripties die politiemensen van basisteams schrijven over hoe hun basisteam stappen kan zetten op digitaal gebied.[64] Daarnaast moeten we kijken welke kennis in hoofden van politiemensen moet zitten en welke gevonden kan worden in – of just-in-time aangeboden kan worden door – systemen (i.e., performance support; Jansen e.a., 2020; Van Valkengoed, 2021). Dit vereist tevens goed kennismanagement.

De politie heeft de afgelopen jaren op landelijk, regionaal en lokaal niveau goede stappen gezet om online criminaliteit aan te pakken. Denk bijvoorbeeld aan het landelijke Team High Tech Crime (THTC)[65], het Landelijk Operationeel Cybercrime Overleg (LOCO), het Landelijk Meldpunt Internetoplichting (LMIO) en aan het publiek-private samenwerkingsverband Electronic Crimes Taskforce (ECTF). Op lokaal niveau zien we steeds vaker digitaal wijkagenten actief worden (Boelens & Landman, 2021) en heeft inmiddels iedere eenheid een cybercrime-team en specialisten in dienst op het gebied van digitaal rechercheren.

Online criminaliteit komt inmiddels dusdanig veel voor dat het niet alleen aan specialisten kan worden overgelaten, maar dat ook collega's in de basisteams hier invulling aan moeten geven. Een goede opvolging begint namelijk al bij de melding of aangifte. Bovendien moet 'eenvoudige' online criminaliteit ook door een crimeteam (i.e., opsporingsteam binnen de basisteams) opgepakt kunnen worden. Daarnaast zien we dat naast online criminaliteit politiemensen ook veel te maken krijgen met 'criminaliteit met een digitale component'. Dit omvat delicten waarbij digitale sporen (zoals metadata, audioberichten en beeldmateriaal) kunnen bijdragen aan het oplossen ervan, zoals een gefilmde mishandeling.

Om tot de kern te komen is het allereerst van belang dat politiemensen beschikken over een adequaat 'digitaal' kennis- en vaardighedenniveau. Ruwweg hebben we het dan over (i) kennis aangaande digitalisering (Waar hebben politiemensen mee te maken?) en (ii) kennis van handelingen die de politie kan verrichten in het kader van voorkomen, verstoren/stoppen en opsporen (Wat kunnen politiemensen doen?). Belangrijk is dat politiemensen vervolgens voldoende digitaal geïnformeerd, vaardig en weerbaar blijven; welke digitale kennis politiewerk vereist, verandert continu en vergt meebewegen (Jansen e.a., 2020; 2023).

In relatie tot kennis en digitalisering werd lange tijd geschreven dat de politie een tekort aan operationele kennis zou hebben (Stol e.a., 1999; Toutenhoofd e.a., 2009). Er was echter nooit onderzocht waaruit dat tekort zou bestaan, en waar in de organisatie dit zich voordeed. Om deze kennislacune op te vullen, deden wij hier onderzoek naar (Jansen e.a., 2020). Wij onderzochten, in opdracht van de politie, het kennisniveau van politiemensen aangaande digitale aspecten van politiewerk. Daarvoor stelden wij eerst kennisnormen vast waaraan het kennisniveau van politiemensen kon worden getoetst. Dit deden we aan de hand van literatuuronderzoek, expertinterviews en focusgroepen.

Een kennisnorm geeft aan over welke 'digitale' kennis politiemensen moeten beschikken om effectief invulling te geven aan politiewerk in een gedigitaliseerde samenleving. De normen hebben betrekking op bewustzijn over online criminaliteit, handelingen op en rondom een plaats delict die met 'digitaal' te maken hebben, digitale sporen, informatiegaring op internet, online communicatie met burgers en aangiften van online criminaliteit. De kennisnormen omvatten ook juridische componenten en verschillen per functiegroep. Een voorwaarde is dat politiemensen beschikken over de meer generieke digitale vaardigheden c.q. digitaal geletterd zijn, weten wat er speelt in de (digitale) samenleving en beschikken over voor het politievak relevante vakspecifieke digitale kennis en vaardigheden (De Vries & Henssen, 2018; Huisman e.a., 2016; Jansen e.a., 2020; POR, 2020; Van Valkengoed, 2021). Belangrijk is om bewust te zijn dat kennisnormen dynamisch moeten zijn.

Op basis van die normen ontwikkelden wij een vragenlijst die 402 agenten en rechercheurs hebben ingevuld. Dit deden we om in kaart te brengen welke kennis politiemensen in de praktijk hebben. De uitkomsten laten zien dat verbetering van kennis in de breedte en diepte noodzakelijk is. Uit een nadere analyse viel op dat de verschillen niet leeftijdgebonden zijn. Dit betekent dat het kennistekort niet vanzelf wordt opgelost wanneer oudere politiemensen uitstromen en nieuwe, jongere politiemensen instromen. Wel lijken opleiding en ervaring met 'digitale' zaken positief samen te hangen met het kennisniveau van politiemensen. Ook viel op dat rechercheurs over meer digitale kennis beschikken dan politiemensen uit andere functiegroepen, zoals agenten op straat ('blauw') of politiemedewerkers die aangiften opnemen. Dit betekent dat om een goede slag te slaan in het bestrijden van het kennistekort, belangrijke winst geboekt kan worden op basisteamniveau.

Ons onderzoek – met als hoofdtitel Level-Up! – heeft veel impact gehad. Het rapport heeft goed zijn weg gevonden en blijft deze vooralsnog vinden binnen de politieorganisatie. Zo heeft de Politieonderwijsraad veel van onze aanbevelingen overgenomen in haar rapport (POR, 2020), wordt het onderzoek binnen het Expertise Centrum Digitale Opsporing (ECDO) van de politie als basis gebruikt bij de vormgeving van ontwikkeltrajecten binnen de politie (Van Valkengoed, 2021), en worden we regelmatig benaderd door politiemensen en politiestudenten uit verschillende eenheden om kennis te delen over het onderwerp en daarover te sparren.

Het werken aan kennis en vaardigheden moet structureel gebeuren; op organisatorisch niveau alsook op het niveau van het individu. Dit is echter niet eenvoudig te bewerkstelligen. Capaciteitsproblemen en de ervaren werkdruk die bij de politie erg groot is spelen daarin een belemmerende rol (De Snoo e.a., 2021; Inspectie Justitie en Veiligheid, 2017; Jansen e.a., 2023; Terpstra e.a., 2021). Capaciteitsgebrek heeft daarnaast ook zijn weerslag op de aanpak. De grote hoeveelheid aan online criminaliteitszaken kan al snel leiden tot overvraging.

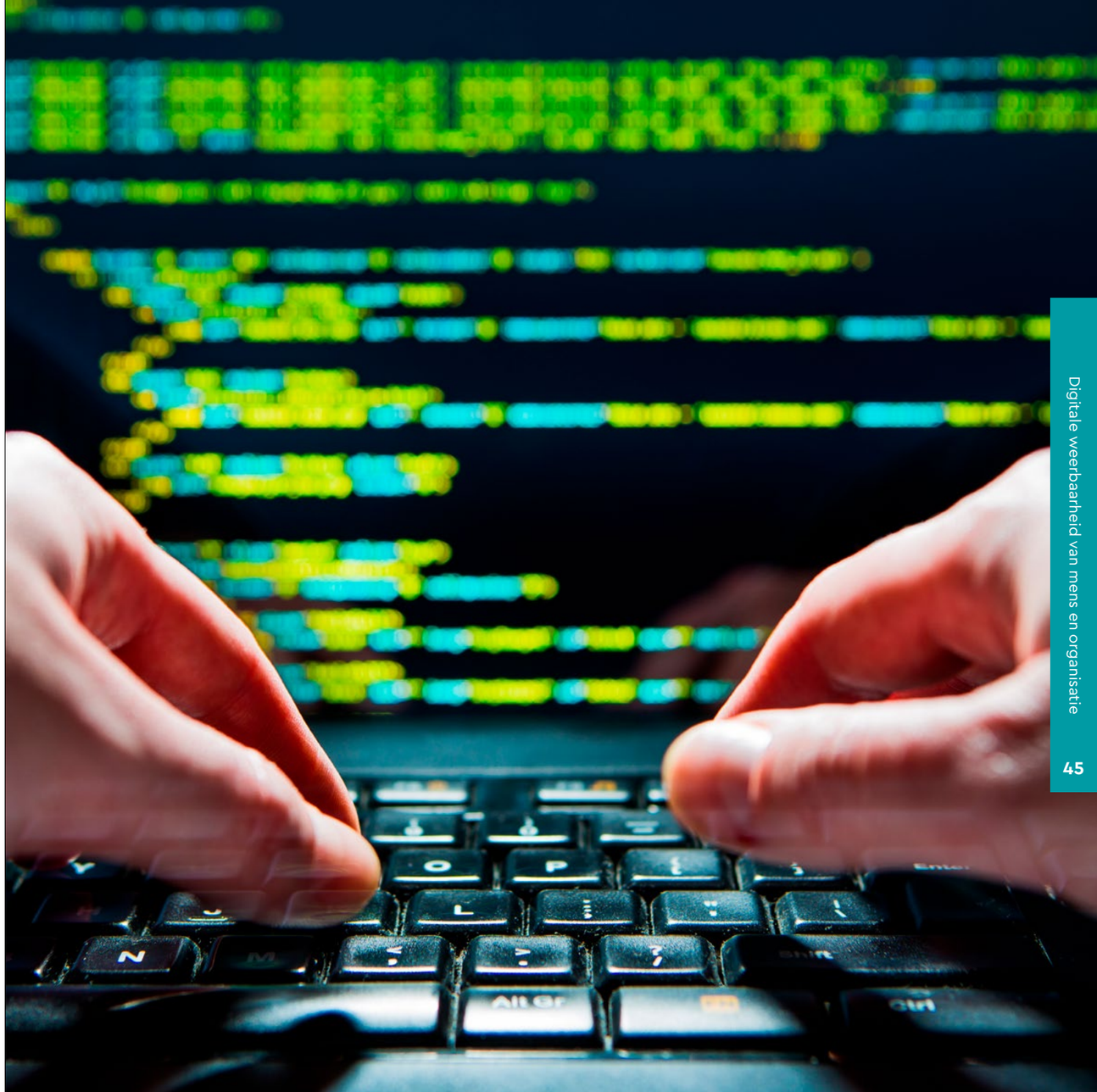
[64] https://cybersciencecenter.nl/kennisplatform-ggp-digitalisering/introductie/

[65] Een initiatief dat hier onder valt is het in 2020 opgerichte landelijke daderpreventieteam COPS (Cyber Offender Prevention Squad). Zie: https://magazines.cybersecurityraad.nl/csrmagazine/2022/01/16.-waarom-wachten-tot-het-fout-gaat-ook-daderpreventie-is-cybersecurity

Daarnaast hebben we te maken met een grote organisatie waar meer dan 60.000 mensen werken. Bovendien is het lastig voor veel politiemensen om de snelheid van deze ontwikkelingen bij te benen (Hadlington e.a., 2018). Wel hebben wij en anderen hiervoor suggesties gedaan (Jansen e.a., 2020; POR, 2020), zoals performance support by design (i.e., een systematische benadering voor het creëren en implementeren van performance support oplossingen) en learning-on-the-job, en geven we hier invulling aan via een recent, door Politie en Wetenschap, gehonoreerd onderzoeksproject (zie par. 2.3).

Kortom, het digitale tijdperk heeft de politie nieuwe en complexe uitdagingen gebracht. Bovenstaande illustreert dat de politie actief stappen onderneemt om deze uitdagingen aan te gaan. Het verder aanpakken van deze uitdagingen vereist een gezamenlijke inspanning van de politie, beleidsmakers en andere publieke en private partners en belanghebbenden. Immers, de politie staat er niet alleen voor als we het hebben over het werken aan digitale veiligheid. De werkelijkheid is daarvoor te complex en de politie is niet de enige verantwoordelijke partij. De politie speelt echter wel een essentiële rol en moet daarom meegaan in deze ontwikkelingen om midden in de samenleving te blijven staan. Dat vergt dus meebewegen.

Hoe dat meebewegen eruit moet zien, daar willen we met het lectoraat aan bijdragen. Wij zullen ons voornamelijk focussen op de veranderopgave voor een digitaal vaardige (en weerbare) politie (POR, 2020). Het gaat daarbij niet alleen om de ontwikkeling van defensieve kennis en vaardigheden (om fouten en slachtofferschap te beperken), maar ook om offensieve kennis en vaardigheden (voor het benutten van de mogelijkheden van digitalisering voor politiewerk). Een goed startpunt hiervoor zijn de basisteams. Zij hebben te maken met de grootste kennislacune, zijn het eerste aanspreekpunt voor burgers en moeten de lokale aanpak vormgeven (Jansen e.a., 2020; Terpstra e.a., 2021). Zij zoeken reeds naar oplossingen, maar kunnen daar verdere ondersteuning – via onderzoek én onderwijs – goed bij gebruiken (zie ook CEPOL, 2022).



Hoofdstuk 2

Onderzoekslijnen en -thema's

De twee leidende focusgebieden binnen de onderzoeksgroep Cybersafety zijn: (i) digitale weerbaarheid van mens en organisatie en (ii) bestuur in een digitaliserende samenleving. Deze focusgebieden – en de gelijknamige lectoraten – zijn aanvullend aan elkaar en vormen in zekere zin een continuüm. In dit hoofdstuk worden de onderzoekslijnen en -thema's gepresenteerd van het lectoraat Digitale Weerbaarheid van Mens en Organisatie (par. 2.1-2.3). Per lijn zijn één hoofdvraag en drie deelvragen geformuleerd, en zijn twee onderzoeksprojecten beschreven die reeds worden uitgevoerd. Daarnaast zijn enkele ideeën opgenomen waar we in de huidige lectoraatsperiode (2022-2026) werk van willen maken. De onderzoekslijnen en -thema's van het lectoraat Bestuur in een Digitaliserende Samenleving zijn te lezen in het werk van Bantema (2023).

De activiteiten van het lectoraat dragen bij aan de verschillende doelen die we hebben geformuleerd op het gebied van kennis, beroepspraktijk en onderwijs. Het gaat daarbij om bij te dragen aan (i) kennisontwikkeling en het delen van kennis, (ii) oplossingen voor de beroepspraktijk en maatschappelijke vraagstukken en (iii) de kwaliteit en toekomstbestendigheid van onderwijs en professionalisering. De activiteiten van het lectoraat sluiten aan bij het hogeschoolbeleid en bij regionale, landelijke en internationale thema's en agenda's. Voorbeelden zijn de Strategische Onderzoeksagenda voor de Politie (SOAP) 2019-2022 (Politieacademie, 2019)[66], de Kennis- en Innovatieagenda Veiligheid (missie 'cyberveiligheid')[67], de Nationale Wetenschapsagenda ('Hoe garanderen wij onze digitale veiligheid?')[68], de NCSC Onderzoeksagenda 2023-2026[69] en de Agenda Digitale Veiligheid 2020-2024 van de Vereniging van Nederlandse Gemeenten (VNG)[70].

Zoals in de inleiding al opgemerkt gaan de ontwikkelingen op het gebied van digitalisering razend snel. Het is daarom van belang dat de onderzoeksgroep daar zicht op houdt, om deze zodoende beter te begrijpen. Niet alleen om relevant onderzoek te kunnen blijven doen, maar ook om het werkveld daarover te informeren en studenten erin op te leiden. Het kan daarbij gaan om het duiden van ontwikkelingen (Wat speelt nu?) alsook het anticiperen op nieuwe uitdagingen (Wat komt er op ons af?). Ons onderzoek is dus zowel trendvolgend als trendsettend. Continue, overstijgende onderzoeksvragen waar de onderzoeksgroep zich op richt zijn:

1. Welk effect heeft digitalisering op de veiligheid (problemen, dreigingen, risico's) van de maatschappij?

2. Welke veiligheidsuitdagingen spelen op het gebied van digitalisering?

3. Hoe zorgen we samen (onderwijs, overheid, ondernemers) voor digitale veiligheid?

[66] De nieuwe SOAP is in ontwikkeling en zal later dit kalenderjaar (2023) worden gepubliceerd.
[67] https://www.nwo.nl/sites/nwo/files/assets/KIA%20Veiligheid%20-%2020191015%20definitief_0.pdf
[68] https://vragen.wetenschapsagenda.nl/cluster/hoe-garanderen-we-onze-digitale-veiligheid
[69] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/11/ncsc-onderzoeksagenda-2023---2026/Onderzoeksagenda+2023+-+2026+NCSC_NL_comp..pdf
[70] https://vng.nl/sites/default/files/2020-02/vng_agenda_digitale_veiligheid_2020-2024_def_0.pdf

Deze vragen zijn breed en algemeen geformuleerd voor de onderzoeksgroep als geheel. Het onderzoek binnen een hogeschool kenmerkt zich door het toegepaste en praktijkgerichte karakter ervan. Daarom concretiseer ik de scope van de activiteiten van het lectoraat hierna in drie afgebakende onderzoekslijnen en bijbehorende onderzoeksvragen. Let op dat in ons onderzoek altijd wordt gekeken naar ethische en juridische kaders, waaronder privacy; zowel voor de uitvoering – door in ieder geval de richtlijnen en gedragsnormen te volgen die gelden voor hoogwaardig praktijkgericht onderzoek – als voor de implicaties van de resultaten voor de praktijk. Hierbij kan gedacht worden aan niet alleen de vraag te stellen of iets *kan*, maar ook of iets *mag* en in hoeverre het *wenselijk* is. Of zoals het in het rapport van Pijpers e.a. (2020, p.11) wordt verwoord: 'Het uitgangspunt "als het mag is het goed" is misschien juridisch in de haak, maar niet per se ethisch.' Naast wetten en regels zijn normen en waarden dus ook van belang (Van Mensvoort, 2019). Ethiek is een vanzelfsprekend onderdeel in de onderzoeken die wij uitvoeren en wordt om die reden hier niet als een op zichzelf staand onderwerp behandeld.

2.1 Digitale weerbaarheid van burgers

Voor wat betreft digitale weerbaarheid richt het lectoraat zich in de eerste plaats op de digitale weerbaarheid van burgers; ofwel eindgebruikers die in een privésetting gebruik maken van digitale middelen en diensten. Zoals in hoofdstuk 1 is te lezen zien we dat relatief veel burgers in Nederland slachtoffer worden van online criminaliteit en dat de slachtofferaantallen blijven stijgen. Het is belangrijk om deze stijging een halt toe te roepen door daarvoor inspanningen te leveren. Dat kan op verschillende terreinen waar verschillende partijen aan kunnen en moeten bijdragen. Vanuit het lectoraat richten we ons op thema's als bewustwording, risicoperceptie, maar vooral op (verandering van) gedrag. Immers, bewustwording is slechts de eerste stap voor digitale weerbaarheid. Uiteindelijk gaat het om actie. De hoofdvraag binnen de burger-lijn luidt als volgt: Hoe kunnen we burgers helpen om zichzelf structureel te beschermen tegen digitale risico's? De deelvragen waar we ons als lectoraat op richten zijn:

1. Hoe kunnen we het gedrag van burgers begrijpen, verklaren en verbeteren/faciliteren, zodat zij zichzelf (en anderen) effectief beschermen tegen (toekomstige) digitale risico's?

2. Wat zijn de werkzame elementen van (gedrags) interventies voor burgers gericht op het minimaliseren van digitale veiligheidsrisico's, en hoe effectief zijn deze (op korte en lange termijn)?

3. Hoe kan communicatie over digitale risico's beter toegesneden worden op het kennisniveau en referentiekader van burgers, rekening houdend met individuele verschillen?

Om deze vragen te beantwoorden is allereerst goed inzicht nodig in de problemen die op burgers af komen en hoe die zich ontwikkelen (Wat is er aan de hand?). Vervolgens is zicht nodig op de specifieke burgerdoelgroepen die het betreft (Voor wie is het relevant?), wat de achterliggende oorzaken zijn (Hoe komt het?) en welke kennis en vaardigheden zij hebben

(Wat weten/kunnen ze wel en niet?)[71]. Een goede informatiepositie is essentieel. Pas dan kan gericht worden gewerkt aan oplossingen (Wat kan eraan worden gedaan?). Ook weten we nog onvoldoende over welke (gedrags) interventies werken in welke situaties, onder welke condities, voor welke doelgroep, en voor hoelang. Daarmee gaan we aan de slag.

We kunnen echter niet op iedere vraag tegelijk inspringen. Hierna beschrijf ik een tweetal onderzoeksprojecten die we momenteel uitvoeren. De eerste heeft betrekking op online fraudepreventie (kader 2.1) en de tweede op diverse digitale weerbaarheidsprojecten en de evaluatie daarvan (kader 2.2). Daarna beschrijf ik een aantal onderwerpen die we graag in deze lectoraatsperiode willen oppakken.

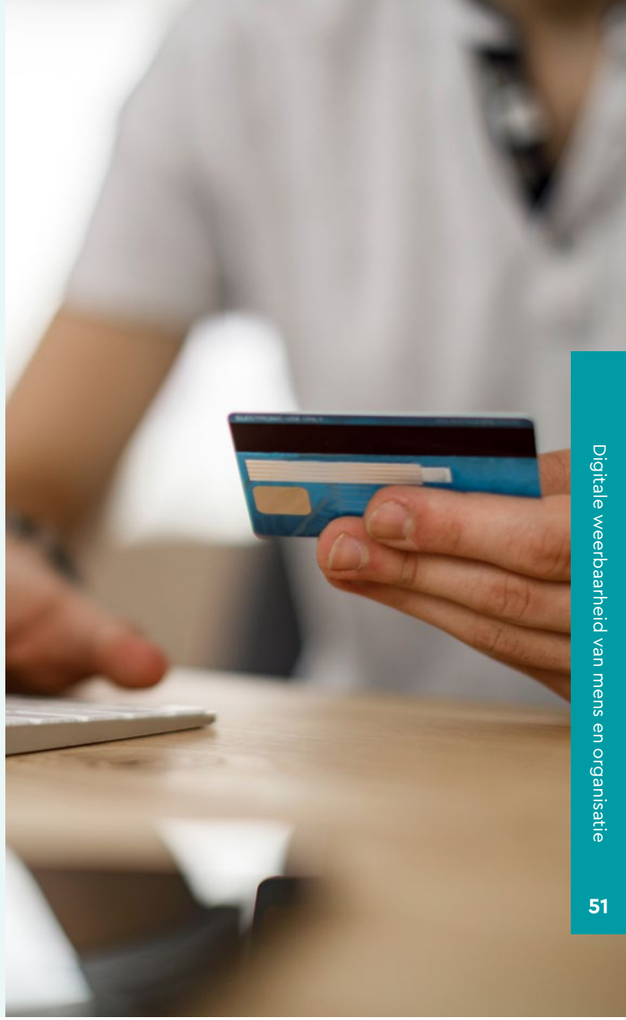
Kader 2.1: Veiligheid van internetbankieren vanuit gebruikersperspectief (lopend)

Op basis van mijn proefschrift, en ervaring met het toepassen van de protection motivation theory (PMT), ben ik benaderd door een van de grootbanken uit het Verenigd Koninkrijk om samen te werken aan een onderzoek met als doel eindgebruikers te beschermen tegen online bankfraude. De betreffende medewerkers van deze bank – beide gedragswetenschappers – zijn geïnteresseerd in hoe eindgebruikers ondersteund kunnen worden om betere beslissingen te nemen die ten gunste komen van de veiligheid om zodoende fraude te voorkomen. Hiervoor werken we tevens samen met een onderzoeker van Michigan State University (VS).

Het theoretische model dat we hebben ontwikkeld en de hypothesen die we hebben opgesteld, leunen op drie theoretische perspectieven. De eerste twee zijn het Systeem-1 en Systeem-2 denken van Kahneman (2011) en het perspectief van mentale modellen.[72] Daarbij is de vraag: Hoe krijgen we eindgebruikers van het automatische Systeem-1 handelen (*fast thinking*; waarbij eindgebruikers doorgaans een 'niet-verdacht' mentaal model hebben), naar een rationele probleem-evaluatiemodus in Systeem-2 (*slow thinking*; waarbij eindgebruikers overschakelen naar een 'verdacht' mentaal model, en hun ratio gebruiken om zodoende goede beslissingen te nemen).

In het ideale geval maken eindgebruikers actief gebruik van hun mentale checklist om tekenen van fraude op te sporen, in dit geval phishing. Om die ratio praktisch in te vullen, gebruiken we de belangrijkste elementen uit de PMT; het derde theoretische perspectief.

Aan de hand van vragenlijstdata proberen we de mentale modellen van de respondenten (i.e., klanten van banken die gebruik maken van internetbankieren) te construeren en in kaart te brengen hoe de besluitvormingsmodus van een individu eruit ziet (*sense making*) en bewijs te verzamelen voor mogelijkheden (*tipping point*) om daarin eventueel een verschuiving te bewerkstelligen (*goal shift*). We kijken daarbij zowel naar positieve uitkomstvariabelen (i.e., adaptieve coping; dat men [on]bewust de phishing poging stopt) alsook negatieve uitkomstvariabelen (i.e., maladaptieve coping; dat men meegaat in de phishing poging). Op moment van schrijven bevindt deze studie zich in de data-analysefase.



[71] Denk ook aan andere eigenschappen van de doelgroep, zoals hoe de doelgroep informatie verwerkt (Petty & Cacioppo, 1986), eerdere ervaringen en persoonlijkheidskenmerken die mogelijk van invloed zijn op slachtofferschap en het nemen van beschermende maatregelen (Borwell e.a., 2018; Floyd e.a., 2000).

[72] Mentale modellen zijn cognitieve representaties van de externe werkelijkheid (Jones e.a., 2011).

Kader 2.2: Evidence-based werken aan lokale cyberweerbaarheid (tweejarig project, lopend)

In opdracht van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) voeren we, samen met de Haagse Hogeschool en Saxion Hogeschool, een project uit dat is getiteld 'Evidence-based werken aan cyberweerbaarheid'. Dit project bestaat uit een aantal werkpakketten. De eerste, waar we op moment van schrijven concreet invulling aan geven, is een zogenoemde procesevaluatiestudie. Dit houdt in dat alle projecten uit de City Deal Lokale Cyberweerbaarheid Cybercrime[73] worden geëvalueerd op proces (Hoe is de uitvoering van het project verlopen?) en potentiële werkzame bestanddelen (Werkt het project en waarom?). Door middel van procesevaluaties streven we naar het verkrijgen van inzicht in de essentiële voorwaarden die nodig zijn om een beoogd project over digitale weerbaarheid naar het gewenste succes te leiden en het eventueel op te schalen naar andere delen van het land. Tevens zullen de evaluaties de gepercipieerde opbrengsten van de projecten aan het licht brengen. De andere werkpakketten omvatten onder andere effectevaluatiestudies en een studie naar de positieve benadering van digitale weerbaarheid (mens-als-oplossing). Het project bevindt zich op moment van schrijven in de beginfase.

Naast deze concrete projecten is er een aantal thema's op de burger-lijn waar we verder onderzoek naar willen doen. Waar we allereerst mee aan de slag willen is om betrouwbare gedragsdata te verzamelen over veilig online gedrag en beschermende maatregelen. Dit kan bijvoorbeeld middels observaties en logs. 't Hoff-de Goede en collega's (2019) keken naar (daadwerkelijk) gedrag door vignetten voor te leggen en respondenten concrete risicosituaties te laten ondergaan. In het gros van de gevallen wordt echter nog veel geleund op vragenlijstonderzoek. Dit biedt veel inzicht en kennis, maar vooral op het gebied van percepties en intenties. Het vakgebied is klaar om de volgende stap te zetten. Er zit potentieel veel ruis op de lijn tussen intentie en gedrag dat moet worden aangepakt.[74] Dat geldt tevens voor het meten van 'daadwerkelijke kennis en vaardigheden', waar vooralsnog zeer weinig onderzoek naar is verricht (Haag e.a., 2021). Voor dit laatste punt hebben we op moment van schrijven een paper in review. Dit paper is gebaseerd op het afstudeeronderzoek van Kimberly Bluhm (2023).

Omdat het aantal succesvolle digitale aanvallen blijft toenemen is het belangrijk voor individuele burgers om hun apparaten te beveiligen. Hoe dit te doen is onmiskenbaar een uitdaging (Jansen, 2018; Nicholson e.a., 2019; Renaud, 2021).

[73] https://hetccv.nl/onderwerpen/cybercrime/city-deal-lokale-weerbaarheid-cybercrime/
[74] Deze kritiek wordt ook wel aangeduid als de *intention-behaviour gap* (Boss e.a., 2015; Crossler e.a., 2013; Sheeran, 2002). Dit wil zeggen dat (rationele) intenties niet altijd worden opgevolgd door daadwerkelijk gedrag.

Overheden erkennen dit, maar beschouwen zichzelf niet langer als 'shepherds protecting their flocks, as they used to some decades ago' (Renaud, 2021, p.12). Hoewel de landelijke overheid zich wel degelijk met het grotere plaatje bezig houdt[75], lijkt de overheid de handen er vanaf te trekken op het moment dat het concreter moet worden, terwijl ze van oudsher wel is belast met het werken aan 'de veiligheid en gezondheid van iedereen in Nederland'[76]. De landelijke overheid zit zo gezien meer op de lijn dat burgers zelf verantwoordelijkheid moeten dragen, en dat ze dat prima kunnen doen met de adviezen die ze krijgen (Renaud e.a., 2020).

Waar organisaties uit de vitale sector en de Rijksoverheid kunnen terugvallen op het NCSC en overige organisaties op het DTC, is voor burgers geen dergelijk expertisecentrum ingericht. In westerse samenlevingen worden doorsnee-burgers die als internetgebruikers geen specialistische kennis over digitale veiligheid hebben, geacht zelf verantwoordelijkheid te nemen om zich tegen deze dreigingen te beschermen. Dit heet *responsibilization* (Renaud, 2021; Renaud e.a., 2020), ofwel 'het stimuleren van de eigen verantwoordelijkheid'.

De aanname die daaronder ligt is dat burgers een adequate perceptie hebben van risico's en nauwkeurig advies krijgen en daarmee uit de voeten kunnen (Renaud, 2021). Echter, voor doorsnee-burgers is het moeilijk te bepalen tegen welke dreigingen zij zich moeten beveiligen en welke beschermende maatregelen het meest effectief zijn (Jansen, 2018; Renaud, 2021). De adviezen die worden gegeven zijn vaak one-size-fits-all en weinig concreet. Als bijvoorbeeld wordt geadviseerd om een VPN-dienst of een wachtwoordmanager te gebruiken, hoe kunnen niet-specialisten hierin een goede keuze maken wanneer zij worden geconfronteerd met een groot aanbod aan gratis en betaalde diensten? Bovendien is over de adviezen die worden gegeven geen consensus en zijn deze soms tegenstrijdig (Reeder e.a., 2017; Redmiles e.a., 2020). Daarnaast is voor handelen meer nodig dan alleen kennis, houding en motivatie (Jansen & Van Schaik, 2018a; 2019; Michie e.a., 2011; Van Deursen & Helsper, 2021), en weten we dat mensen over het algemeen slecht in staat zijn om risico's te begrijpen (Siegrist & Árvai, 2020). Het nemen van verantwoordelijkheid voor de eigen digitale veiligheid is dus geen sinecure.

Waar Renaud (2021) vooral pleit voor toegankelijkere en *usable* cybersecurity, door hier in het ontwerpproces rekening mee te houden, maakt zij ook een zaak om de lijn te verkennen van *de-responsibilization*; dus meer advisering en ondersteuning vanuit de overheid. We zien in Nederland dat gemeenten hier wel een rol pakken door activiteiten te organiseren voor hun doelgroepen en ze zodoende te stimuleren om hun digitale weerbaarheid te vergroten.[77] In hoeverre dat voldoende is behoeft echter meer onderzoek. Een interessante weg om te verkennen is die van beslissingsondersteuning bij het nemen van beschermende maatregelen. De vraag die centraal staat is hoe internetgebruikers concreet en praktisch ondersteund kunnen worden bij het nemen van beschermende maatregelen en

[75] https://www.rijksoverheid.nl/actueel/nieuws/2022/03/08/digitaliseringsstrategie-meer-regie-en-publieke-waarden-centraal
[76] https://www.rijksoverheid.nl/onderwerpen/gezonde-en-veilige-leefomgeving/bewust-omgaan-met-veiligheid
[77] https://hetccv.nl/onderwerpen/cybercrime/documenten/lokale-cyberwegenkaart/

het maken van beslissingen ten behoeve van de eigen digitale veiligheid, en welke rol de overheid (met partners, zoals ondernemersverenigingen, bibliotheken en scholen) daarin kan of moet vervullen.

2.2 Digitale weerbaarheid van organisaties

Het lectoraat richt zich in de tweede plaats op de digitale weerbaarheid van organisaties. Alle organisaties moeten digitaal weerbaar worden, omdat ze vroeg of laat het doelwit zullen zijn van een cyberaanval (Rothrock, 2022). Alles is met alles en iedereen verbonden en de kansen van digitalisering en vrijheid van informatie-uitwisseling zijn hoger geplaatst dan veiligheid. Daarom moeten organisaties digitale (rest)risico's accepteren en digitale weerbaarheid integraal onderdeel maken van hun bedrijfsvoering. Het organiseren van digitale weerbaarheid gebeurt op het niveau van mens, techniek en organisatie, waarop onder andere bestuurlijke en juridische krachten van invloed zijn (Renaud & Zimmerman, 2019). Vanuit het lectoraat hebben we primair aandacht voor de menselijke aspecten van digitale weerbaarheid. We richten ons, gezien onze positionering binnen de Thorbecke Academie, in eerste plaats (maar niet uitsluitend) op publieke organisaties. De hoofdvraag binnen de organisatie-lijn luidt als volgt: Hoe kunnen we organisaties en medewerkers helpen zich structureel te beschermen tegen digitale risico's?
De deelvragen waar we ons als lectoraat op richten zijn:

1. Hoe kunnen we het gedrag van medewerkers begrijpen, verklaren en verbeteren/faciliteren, zodat zij zichzelf (en anderen) effectief beschermen tegen digitale risico's?

2. Wat zijn de werkzame elementen van (gedrags) interventies voor medewerkers gericht op het minimaliseren van digitale risico's en impact, en hoe kunnen we de effecten meetbaar maken?

3. Hoe kunnen we leren van (bijna-)incidenten én van de dingen die goed gaan in de dagelijkse praktijk aangaande digitale veiligheid?

Een project waar we op moment van schrijven mee bezig zijn is het NUL-EEN project (zie kader 2.3). Een ander langlopend project dat we binnen deze lijn uitvoeren is het onderzoek naar meldgedrag (zie kader 2.4). Dit project sluit voor een groot deel aan bij het mens-als-oplossing perspectief (par. 1.4). Een ander project dat binnen deze lijn genoemd kan worden is het recent opgestarte SPRONG-project. Dit project staat beschreven in par. 3.1. Ook hoort het eerder besproken 'evidence-based' project hier voor een deel thuis (par. 2.1). De City Deal Lokale Cyberweerbaarheid Cybercrime bevat naast projecten voor verschillende burgerdoelgroepen namelijk ook projecten die gericht zijn op organisaties.[78]

[78] https://hetccv.nl/onderwerpen/cybercrime/database-lokale-cyberprojecten/

Kader 2.3: Digitale weerbaarheid in de regio Noordoost-Fryslân (tweejarig project, lopend)

Vanuit de Versnellingsagenda Noordoost-Fryslân zijn we als lectoraat actief in het project NUL-EEN. Samen met partners – Stichting Cybersafety Noord-Nederland, ROC Friese Poort en IntegriPro – helpen we ondernemers in de regio Noordoost-Fryslân om digitaal weerbaar te worden. Zo organiseren we bijvoorbeeld regelmatig (algemene) bijeenkomsten en (verdiepende) masterclasses in de regio. Tijdens algemene bewustwordingsbijeenkomsten worden diverse thema's behandeld, zoals de nieuwste trends en ontwikkelingen op het gebied van digitalisering en veiligheid, en uitleg over privacy en de AVG. Tijdens verdiepende sessies wordt vaak een specifiek thema behandeld, zoals hoe te beschermen tegen en te handelen tijdens een cyberincident of cybercrisis.

Met de Cyber Starter, een beroepsproduct dat we vanuit het lectoraat hebben ontwikkeld, helpen we ondernemers om de voor hen belangrijkste digitale risico's in kaart te brengen. Met een korte vragenlijst inventariseren we tevens de mate waarin een ondernemer al bezig is met digitale veiligheid. Op basis van zijn of haar antwoorden komen studenten langs om samen met de ondernemer de mogelijke maatregelen te bespreken. Deze studenten worden geworven via het leerbedrijf Digitalisering en Veiligheid (zie par. 3.2) of voeren dit als opdracht uit binnen het reguliere onderwijsprogramma van NHL Stenden Hogeschool. De student zorgt vervolgens, samen met een medewerker van het lectoraat, voor een op maat gemaakte rapportage met praktische aanbevelingen. Uiteindelijk willen we dit ook opvolgen, zodat we inzicht krijgen wat ondernemers hiermee doen en welk effect hiermee wordt bereikt. Tevens willen we bereiken dat na afloop van het project, als de financiering is gestopt, iets duurzaams achterblijft in de regio, waardoor ondernemers blijvend gefaciliteerd kunnen worden bij het vergroten van hun digitale weerbaarheid. Voor meer informatie over het project, zie de projectwebsite: nul-een.frl

Kader 2.4: Meldgedrag (promotieonderzoek, lopend)

Om de digitale weerbaarheid te vergroten binnen organisaties, moeten we niet alleen vertrouwen op tijdige controles en audits, maar moeten we hier ook proactief mee aan de slag. Een manier om dit te doen is door een goedwerkend rapportagesysteem te implementeren en dito processen (bijv. in termen van opvolging, feedback en begeleiding). Het promotieonderzoek 'Exploring and Enhancing Data Breach Reporting Behaviour' gaat over het melden van digitale incidenten en bijna-incidenten. Een specifiek vraagstuk waarnaar wordt gekeken is het toenemende probleem van datalekken.[79] Een datalek is een beveiligingsincident of bijna-incident waarin (potentieel) toegang is verkregen tot informatie zonder autorisatie. Het gaat hierbij om zowel externe dreigingen (zoals een cyberaanval) als interne dreigingen (zoals onzorgvuldigheid van een medewerker). De impact van datalekken loopt uiteen van financiële en juridische consequenties naar negatieve gevolgen op het gebied van reputatie.[80,81]

De hoofdvraag van dit promotieonderzoek is: Welke organisatorische kenmerken faciliteren of remmen meldgedrag van digitale (bijna-)incidenten? Het onderzoek kent een mix van kwalitatieve en kwantitatieve methoden. Het gaat daarbij om de wetenschappelijke state-of-the-art in kaart te brengen, inzichten uit de praktijk op te halen, factoren te identificeren die meldgedrag verklaren, en uiteindelijk interventies te ontwikkelen om meldgedrag bewezen effectief te bevorderen. We hopen binnenkort het eerste artikel over dit onderzoek te publiceren. Het promotieonderzoek wordt uitgevoerd door Sander Ebbers en begeleid door Wouter Stol (promotor) en ondergetekende (copromotor).

[79] Ter illustratie, zie: https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen
[80] https://www.ibm.com/downloads/cas/OJDVQGRY
[81] https://autoriteitpersoonsgegevens.nl/

Ik denk dat er veel te winnen valt door gericht onderzoek te doen naar het mens-als-oplossing perspectief. Hoewel er anekdotisch bewijs bestaat dat deze aanpak werkt in de praktijk van traditionele veiligheidssituaties, is er weinig empirisch bewijs (zowel voor traditionele veiligheidsstudies als voor digitale veiligheid) om deze beweringen te onderbouwen (Cooper, 2022; Rae e.a., 2020). Cooper geeft aan dat het onzeker is of de nieuwe aanpak leidt tot meer veiligheid en/of minder incidenten. Een van de kritieken van Rae en collega's is dat er in de veiligheidswetenschap een gebrek is aan kwalitatief hoogstaande interventiestudies. Dit betekent dat toekomstig onderzoek zich op deze benadering moet richten en moet proberen uit te vinden of deze benadering inderdaad van waarde is.

Een manier om dit te doen is door het toepassen van micro-experimenten. Dekker en Conklin (2022), die pleiten voor een Safety Differently benadering, adviseren ook om micro-experimenten uit te voeren. Rae e.a. (2020, p.2) introduceren de term reality-based safety science: 'waar de theorie is gebaseerd op rigoureuze observaties van de bestaande praktijk, en waar de praktijk is gebaseerd op gevestigde theorie.' Ze benadrukken dat empirisch onderzoek zich zou moeten richten op hoe werk wordt gedaan (*work as done*) in plaats van hoe werk wordt voorgesteld (*work as imagined*), wat wordt onderschreven door Dekker en Conklin (2022). Het is ook belangrijk om te begrijpen wat de uitkomst van een bepaalde praktijk veroorzaakt, om theorie op te bouwen en evidence-informed en -based praktijk te verbeteren. Gevalideerde en gestandaardiseerde schalen en methoden voor het opzetten en evalueren van micro-experimenten zouden het veld verder verbeteren, omdat het vergelijken dan gemakkelijker wordt. Hier liggen ook interessante kansen met het onderwijs, bijvoorbeeld door daarvoor een experimenten-lab op te zetten.

Naast micro-experimenten op korte termijn moet het veld profiteren van goede empirische studies. Deze studies hebben baat bij het meten van het feitelijke gedrag van eindgebruikers, bijvoorbeeld door middel van (participerende) observaties en technische logs – wat nu nog vaak ontbreekt in studies over digitale veiligheid. Bovendien zijn studies met een longitudinaal karakter welkom. Hierdoor is het mogelijk om te ontdekken in hoeverre gevonden effecten stabiel zijn in de tijd (Jansen & Van Schaik, 2019; Milne e.a., 2002) en om trends te signaleren (Uchendu e.a., 2021).

In aansluiting op deze lijn van redenatie willen we vanuit het lectoraat verder verkennen hoe we structureel kunnen bijdragen aan veranderbereidheid en verandermanagementprocessen in ruimere zin (Da Veiga, 2019; Van 't Wout, 2019). Verandermanagement in onderhavige context wordt door Da Veiga en Martins (2015, p.251) beschreven als 'the perceptions about change and the willingness of users to change in order to protect information.' Uchendu e.a. (2021) zien dit onderwerp ook als een interessante kans voor toekomstig onderzoek. Bij onderzoek hiernaar is het van belang om rekening te houden met organisatorische factoren zoals de omvang van een organisatie. Hoe kunnen kleinere organisaties dit perspectief bijvoorbeeld toepassen en de vruchten ervan plukken? Mkb'ers worden bijvoorbeeld blootgesteld aan vergelijkbare digitale risico's als grotere publieke of private organisaties, maar missen vaak de nodige middelen, zoals budget, tijd, kennis en vaardigheden om zich hier adequaat tegen te weren (Da Veiga, 2019; Jansen e.a., 2016).

2.3 Digitale weerbaarheid van politie

Een bijzondere rol in het verhaal rondom een digitaal veilige en weerbare samenleving is weggelegd voor de politie. Daarom krijgt deze actor ook een prominente rol binnen de werkzaamheden van het lectoraat. Zoals in par. 1.5 besproken zijn er legio uitdagingen op het gebied van digitalisering en politiewerk. Om het onderzoek gefocust te houden is nadere afbakening gewenst. Het doel van het onderzoek binnen de politie-lijn is voor een belangrijk deel gestoeld op ons Level-Up! onderzoek (Jansen e.a., 2020) en is tweeledig. Het onderzoek draagt bij aan het versterken van (i) kennis inzake politiewerk in een digitale samenleving en (ii) het handelingsrepertoire van politiemensen (attituden, vaardigheden en gedrag). Het bovenliggende doel is dat de politie meegaat met de ontwikkelingen op het gebied van digitalisering en daarmee midden in de samenleving blijft staan en hiervan profiteert voor een effectieve aanpak van online criminaliteit. Het onderzoek van het lectoraat draagt bij aan de ontwikkel- en veranderopgave voor een digitaal vaardige (en weerbare) politie; gericht op (digitaal) vakmanschap (POR, 2020). De hoofdvraag binnen de politie-lijn luidt als volgt: Hoe kunnen we politiemensen ondersteunen om kennis en vaardigheden aan te leren aangaande digitale aspecten van politiewerk en helpen om zichzelf structureel te beschermen tegen digitale risico's? De deelvragen waar we ons als lectoraat op richten zijn:

1. Welke parate digitale kennis en vaardigheden zijn nodig op welk niveau, en welke moeten 'vindbaar' zijn (in groepen, netwerken, systemen)?

2. Welke interventies leiden tot bewezen verbeteringen van digitale kennis en vaardigheden van politiemensen?

3. Hoe kan ervoor worden gezorgd dat de digitale kennis en vaardigheden aangaande digitale aspecten van politiewerk bij politiemensen actueel blijven, rekening houdend met snelle ontwikkelingen?

In kader 2.5 wordt een project besproken dat kortgeleden is toegekend. Dit project gaat over de intensivering van de lokale aanpak van online criminaliteit. In kader 2.6 wordt het onderzoek naar de rol van encryptie in de opsporing besproken dat onlangs is opgeleverd (Jansen e.a., 2023).

Kader 2.5: Expeditie Lokaal Digitaal: Naar een interventie voor de intensivering van de lokale aanpak van gedigitaliseerde criminaliteit (tweejarig project, toegekend)

Het onderzoek of, misschien beter gezegd, de expeditie Lokaal Digitaal is een langlopend actie-onderzoek dat gezamenlijk met onderzoekers van Saxion Hogeschool en de Haagse Hogeschool is aangevraagd bij, en wordt uitgevoerd, voor Politie en Wetenschap. Het onderzoek heeft als doel om een effectieve interventie te ontwikkelen voor een zelfverzekerde, lokale aanpak van gedigitaliseerde criminaliteit. Dit onderzoek wordt uitgevoerd bij – en samen met – basisteams van de eenheden Noord- en Oost-Nederland, het Digitaal Platform Drenthe en het cybercrime-team van de eenheid Oost-Nederland. Tevens wordt aangesloten bij de Agenda Gebiedsgebonden Politie en de Agenda Digitalisering & Cybercrime. De hoofdvraag van het onderzoek luidt: Hoe kunnen basisteams hun personeel voorbereiden op een effectieve en zelfverzekerde intensivering van de lokale aanpak van gedigitaliseerde criminaliteit? Het onderzoek gaat september 2023 van start.

Kader 2.6: De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden (afgerond)

Bij verschillende vormen van criminaliteit wordt steeds vaker gebruik gemaakt van encryptie, ofwel de versleuteling van gegevens. De aanleiding tot dit onderzoek is een dilemma dat gepaard gaat met encryptie. Een voorbeeld van dit dilemma is te vinden in de resolutie over versleuteling die op 14 december 2020 werd aangenomen door de Europese Raad.[82] Encryptie beschermt enerzijds grondrechten en digitale veiligheid, maar bemoeilijkt anderzijds de wettelijke bevoegdheden van politie en het Openbaar Ministerie. Het doel van het onderzoek is om inzicht te bieden in de rol van encryptie in opsporingsonderzoeken. Dit inzicht kan worden benut bij de gedachtevorming aangaande het genoemde dilemma.

Het onderzoek, waarin werd samengewerkt met onderzoekers van de Politieacademie en de Open Universiteit, omvatte een combinatie van deskresearch – literatuuronderzoek, media-analyse en analyse van rechterlijke uitspraken – en fieldresearch. Fieldresearch bestond uit zestien interviews met negentien experts die werkzaam zijn bij de politie, het Nederlands Forensisch Instituut, het Openbaar Ministerie en de Rechterlijke Macht, en een survey die door 177 operationeel specialisten van de politie volledig is ingevuld (responsepercentage 20%).

Het onderzoek laat zien dat encryptie in opsporingsonderzoeken een prominente rol inneemt. Deze rol werkt twee kanten uit. Aan de ene kant vormt encryptie een belemmering voor de politie, omdat het bewijs niet direct toegankelijk is, wat gevolgen kan hebben voor de identificatie en lokalisatie van verdachten. Aan de andere kant kan encryptie, vooral wanneer het gekraakt of omzeild is, juist praktisch van nut zijn en een zaak versnellen, criminele netwerken onthullen en leiden tot nieuwe opsporingsonderzoeken.

Het was lastig om vast te stellen hoeveel zaken niet worden opgelost of hoeveel tijd verloren gaat door encryptie, en evenzo hoeveel zaken extra worden opgelost of hoeveel tijd er wordt gewonnen dankzij gekraakte encryptie. De complexiteit van opsporingsonderzoeken, die afhankelijk zijn van diverse factoren en omstandigheden, maakt dit moeilijk meetbaar. Al met al geeft het onderzoek een genuanceerd beeld van de rol van encryptie in opsporingsonderzoeken. Het onderzoek werd op 11 april 2023 gepresenteerd aan de Tweede Kamer.

[82] https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

Daarnaast draagt het lectoraat bij aan een lopend project omtrent politiestraatwerk en informatiegebruik. Dit meerjarige project wordt uitgevoerd voor Politie en Wetenschap en geleid door Wouter Stol en betreft, net als het encryptieonderzoek, een samenwerking tussen NHL Stenden Hogeschool, de Politieacademie en de Open Universiteit. Kortgezegd gaat dit onderzoek over de doorwerking van informatietechnologie op het politiewerk op straat. Met het onderzoek wordt het gebruik en de waarde van het (meestal digitale) informatieaanbod in politiestraatwerk geëvalueerd. De dataverzameling voor dit onderzoek was uniek, daar mijn collega's en ik een aantal diensten meeliepen met de noodhulp van een drietal politiebasisteams en deze observeerden. Een bijzondere en waardevolle ervaring om het politiewerk van zo dichtbij mee te maken. Op moment van schrijven bevindt het onderzoek zich in de data-analysefase. De verwachting is dat het rapport aan het eind van dit kalenderjaar (2023) wordt opgeleverd.

Een ander onderzoek waar het lectoraat aan bijdraagt voor de politie-lijn is het promotieonderzoek 'Slachtofferimpact Cybercrime' van Jildau Borwell. In dit promotieonderzoek wordt onderzocht hoe de impact van online criminaliteit op slachtoffers zich verhoudt tot de impact van traditionele criminaliteit en wat dit betekent voor de rol van de politie. De effecten van online criminaliteit lijken vaak te worden onderschat, terwijl verschillende onderzoeken laten zien dat slachtoffers ernstige impact kunnen ervaren (o.a. Jansen & Leukfeldt, 2018). Online criminaliteit kent enkele unieke kenmerken, zoals besproken in hoofdstuk 1. Ten tijde van de start van het promotieonderzoek was onduidelijk in hoeverre deze kenmerken van invloed zijn op de impact van slachtofferschap. Bovendien heeft nooit een uitgebreide vergelijking plaatsgevonden tussen de impact van verschillende vormen van online criminaliteit en traditionele criminaliteit. Het promotieonderzoek heeft al verschillende publicaties opgeleverd (Bluhm e.a., 2022; Borwell e.a., 2021a; 2021b), de nodige impact gehad[83] en bevindt zich op moment van schrijven in het laatste jaar. Het promotieonderzoek wordt begeleid door Wouter Stol (promotor) en ondergetekende (copromotor).

Daarnaast willen we een aantal nieuwe onderzoeken opstarten binnen de politie-lijn. Zo willen we state-of-the-art, evaluatief en experimenteel onderzoek doen naar hoe politiemensen het meest effectief kennis kunnen opdoen over en getraind kunnen worden in digitale aspecten van politiewerk. Immers: 'Voor politiewerk is diepgaande kennis over bijvoorbeeld "wijk, web en wereld" onmisbaar om te kunnen begrijpen wat en waarom iets gedaan moet worden' (POR, 2020, p.6). Voor het politieonderzoek is het van cruciaal belang om de vragen die spelen op het gebied van politiewerk en digitalisering continu te inventariseren (en daar vervolgens antwoorden op te formuleren). Dat kan naast (internationaal) literatuuronderzoek het beste door goed met de doelgroep – de politie én de Politieacademie – in contact te blijven staan. Met de actieve

[83] Deze impact omvat lokale aanpassing in prioritering van online criminaliteit, onderbouwing voor pilots op het gebied van dienstverlening en slachtofferzorg na online criminaliteit, en inspiratie voor een grootschalig onderzoek naar tevredenheid na aangifte van de portefeuille Dienstverlening.

verbinding die we hebben met de Politieacademie en de goede contacten die we onderhouden met verschillende politieonderdelen (zie hoofdstuk 3) hebben we daar reeds een goede basis voor gelegd.

Vanuit het in oprichting zijnde kenniscentrum Digitalisering, Intelligence en Opsporing van de Politieacademie (zie par. 3.1), waarvan ik deel uitmaak, ligt een interessante verbinding tussen de bij dat kenniscentrum betrokken lectoraten op het gebied van digitale transformatie. Ons lectoraat kan bijdragen door kennis en expertise op het terrein van human factors in te brengen. Immers, ook bij digitale transformatie, wat onder andere bestaat uit het ontwerpen, ontwikkelen en implementeren van nieuwe digitale producten en werkprocessen, draait het voor een belangrijk deel om de mens (Davis, 1989; Van Mensvoort, 2019; Venkatesh e.a., 2003), in dit specifieke geval dus politiemensen. Ook daar liggen mooie kansen voor nieuw onderzoek.

Hoofdstuk 3

De kracht van verbinding

Onderzoek draait om het beter begrijpen, verklaren en verbeteren van de wereld om ons heen. Het gaat ook om met een bepaalde lens kritisch naar situaties en problemen te kijken, deze te duiden en het gesprek daarover te voeren. Een van de kernresultaten dat onderzoek moet opleveren is het op systematische wijze ontwikkelen van nieuwe kennis en oplossingen. Deze kennis en oplossingen moeten niet alleen ten bate komen aan de wetenschap, maar ook relevant zijn voor het werkveld en maatschappij, en meerwaarde hebben voor het onderwijs.

Voor de ontwikkeling van kennis en oplossingen voor digitale veiligheidsvraagstukken, is een belangrijke taak van het lectoraat om duurzame verbindingen te zoeken met verschillende actoren. De vraagarticulatie voor de onderzoeken die we uitvoeren komt rechtstreeks uit de praktijk. In sommige gevallen werken we ook direct samen met de praktijk in deze onderzoeken. Hoe dan ook zijn de uitkomsten die we opdoen met ons onderzoek toepasbaar voor de praktijk. Dit betekent dat de verbinding met het werkveld inherent is aan ons werk (par. 3.2). Aan de onderzoeken werken zowel docent-onderzoekers als studenten mee. De resultaten werken daardoor – direct en indirect – door in het onderwijs en dragen bij aan de professionalisering van docent-onderzoekers. Daarmee is ook de verbinding met onderwijs geborgd (par. 3.3). Waar mogelijk en daar waar het meerwaarde heeft, staan we nauw in verbinding met kennispartners. Hiermee trap ik dit hoofdstuk af (par. 3.1). In de praktijk lopen onderzoeks- en onderwijsactiviteiten door elkaar heen en kunnen verschillende actoren diverse rollen aannemen. Voor de duidelijkheid van het verhaal bespreek ik ze hier los van elkaar.

3.1 Verbinding met kennispartners

Digitale weerbaarheid vereist samenwerking. Een van de doorlopende doelen van het lectoraat is het opzetten en onderhouden van een netwerk van kennis- en werkveldpartners c.q. de gebruikers van kennis op het terrein van digitale weerbaarheid. Een belangrijke kennispartner waarmee we een duurzame verbinding zijn aangegaan is de Politieacademie. Ook hebben we onlangs middelen toegekend gekregen om het netwerk en onderhouden daarvan verder te professionaliseren; via de zogenoemde SPRONG-subsidie (kader 3.1).

De samenwerking met de Politieacademie krijgt vooralsnog gestalte door middel van een aanstelling van de lector voor een dag in de week bij de sector Kennis en Onderzoek. Op moment van schrijven zijn we aan het verkennen om dit te verruimen en om het lectoraat Digitale Weerbaarheid van Mens en Organisatie vorm te gaan geven als een gezamenlijk lectoraat van NHL Stenden Hogeschool én de Politieacademie. Hierdoor kunnen de huidige activiteiten, zoals bijdragen aan onderwijs, de nieuwe SOAP en het in oprichting zijnde kenniscentrum Digitalisering, Intelligence en Technologie (kcDIT) structureler worden en worden uitgebouwd. Daarbij wordt eveneens verkend hoe de verdere uitwisseling tussen de kenniskring van docent-onderzoekers van NHL Stenden Hogeschool en de Politieacademie eruit komt te zien.

Binnen het in wording zijnde kcDIT wordt samengewerkt met collega's van team Kennis en team Onderzoek. Voor team Onderzoek onder meer met de lector Intelligence en de lector Technologies for Criminal Investigation. Op moment van schrijven is het kcDIT nog volop in ontwikkeling (o.a. aanscherpen van missie, visie en doelen).

Daarom is het nog wat te prematuur om op de details in te gaan. Een aantal kernelementen van de in oprichting zijnde kenniscentra komt voort uit intern politiebeleid om omvat: (i) het verenigen van de sector Kennis en Onderzoek in een gemeenschappelijke opdracht om tot bundeling van krachten, expertise en kennis te komen, (ii) co-creatie van kennis met behoeftestellers uit de operatie, onderwijs, onderzoek en andere kennisinstellingen en (iii) werken vanuit een kwaliteitskader voor kennisontwikkeling en kennisontsluiting.

Kader 3.1: SPRONG Expertisenetwerk Cyberweerbaar Nederland (achtjarig project, lopend)

Steeds vaker krijgen we vanuit provincies, gemeenten en bedrijven de vraag om mee te denken over hun digitale weerbaarheid en die van de doelgroepen die zij bedienen. Samen met de Haagse Hogeschool en Saxion Hogeschool hebben we onlangs voor acht jaar een SPRONG-subsidie toegekend gekregen om publieke en private organisaties daarbij te helpen. De focus van de SPRONG-groep ligt, net als ons lectoraat, op de menselijke aspecten van digitale weerbaarheid.

De kick-off van het project vond medio februari 2023 plaats te Utrecht. De kernactiviteiten zijn gericht op het opbouwen van een duurzaam expertisenetwerk ten behoeve van continue vraagarticulatie en kennisdisseminatie, het organiseren van professionaliseringsactiviteiten voor praktijkgerichte onderzoekers, het leveren van bijdragen aan het onderwijs, het opbouwen en onderhouden van een landelijke monitor van digitale veiligheidsincidenten, en het uitvoeren van experimenten en simulaties gericht op het gedrag van individuen binnen organisaties. De ambitie van de SPRONG-groep is om het toonaangevende expertisenetwerk te worden op het gebied van digitale weerbaarheid binnen publieke en private organisaties en hoogwaardige, relevante en praktisch toepasbare kennis te ontwikkelen op dit onderwerp. Dit met als doel om de digitale weerbaarheid in Nederland te bevorderen.

Tot slot zijn we ook op andere wijze verbonden met kennispartners. Zo maken we deel uit van verschillende (internationale) werkgroepen aangaande digitale veiligheid en worden we bijvoorbeeld benaderd om zitting te nemen in klankbord-, lees- en adviescommissies. Ook worden we gevraagd om mee te denken over de inhoud van onderzoeksagenda's en subsidiecalls op het gebied van digitale veiligheid. Tevens worden we geregeld benaderd om artikelen te reviewen voor diverse (internationale) tijdschriften en heb ik bijvoorbeeld als gastredacteur meegewerkt aan het themanummer 'Lokale aanpak van cybercriminaliteit' van het Tijdschrift voor Veiligheid (Spithoven e.a., 2022a).

3.2 Verbinding met werkveld

Een elementaire taak van het lectoraat is om relevant onderzoek uit te voeren. De vragen uit het werkveld zijn daarbij bepalend. Een belangrijk criterium daarvoor is om in goede verbinding te staan met het werkveld. Het lectoraat onderhoudt daarom contact met diverse netwerken. Twee voorbeelden daarvan zijn reeds benoemd in par. 3.1. Aangaande digitale weerbaarheid is naast de relevante landelijke netwerken ook veel contact met lokale netwerken en partners. Naast kennisinstellingen betreft dat bijvoorbeeld professionals van gemeenten, zoals ambtenaren Openbare Orde en Veiligheid (OOV) en CISO's. Aangaande de politie wordt eveneens contact onderhouden met lokale, regionale en landelijke politieprogramma's, afdelingen en teams op het gebied van digitalisering.

Dit gaat overigens verder dan onderzoek alleen. Soms gaat het ook om het praktisch helpen bij vraagstukken. Zo hebben we de politie (eenheid Noord-Nederland) bijvoorbeeld geholpen om basisteams mee te nemen in de ontwikkelingen omtrent cybercrises door ze erover te informeren en ermee te laten oefenen. Een korte beschrijving van dit bewustwordingsinitiatief is te lezen in de publicatie van Schiks e.a. (2022). Op moment van schrijven borduren we verder op dit thema en worden in samenwerking met onderwijs (minor Crisisbeheersing) aanvullende activiteiten ontplooid. Door ons onderzoek, in dit geval naar cybercrises (Ebbers e.a., 2021), weet het werkveld ons te vinden, en kunnen we 'nieuwe' thematiek laten landen in c.q. overdragen naar het onderwijs.

We staan dus niet alleen via ons onderzoek in verbinding met het werkveld, maar ook via het onderwijs. Studenten spelen daarin een belangrijke rol. Studenten voeren in verschillende jaargangen onderzoeken uit die te maken hebben met digitalisering en veiligheid (zie par. 3.3). Een initiatief dat ik hier wil noemen, dat is ontstaan uit de samenwerking tussen onderzoek en onderwijs van de Thorbecke Academie en ten bate komt aan het werkveld (alsook studenten en alumni), is het leerbedrijf Digitalisering en Veiligheid (kader 3.2). Met name Saskia Westers en Monique van Dijk hebben een onmisbare rol vervuld in de realisatie hiervan.

Kader 3.2: Leerbedrijf Digitalisering en Veiligheid

Het leerbedrijf Digitalisering en Veiligheid zag het licht in 2021 en is een platform waar studenten/alumni en het werkveld elkaar kunnen vinden. Het doel van het leerbedrijf is tweeledig: (i) om studenten/alumni (extra) kansen te geven om relevante werkervaring op te doen, hun netwerk uit te breiden en hun plek te vinden op de arbeidsmarkt, en (ii) om het werkveld te helpen bij snel ontwikkelende vraagstukken op het gebied van digitalisering en veiligheid. Op de website van het leerbedrijf kunnen studenten/alumni zich aanmelden en worden opdrachten geplaats van opdrachtgevers. Het leerbedrijf kan zowel faciliteren bij de uitvoering van opdrachten binnen de curricula van de Thorbecke Academie, als los daarvan. In principe worden de studenten begeleid door de opdrachtgever, maar indien een extra kwaliteitsslag gewenst is, kunnen ook docent-onderzoekers van de onderzoeksgroep (onder voorwaarden) bijdragen met kennis, expertise en eventueel aanvullende begeleiding. Een mooie opbrengst van het leerbedrijf voor ons lectoraat (en onderwijs) is dat we via dit platform een talentvolle docent-onderzoeker hebben kunnen aannemen. Interesse in de mogelijkheden die het leerbedrijf biedt? Bezoek dan de website: https://leerbedrijfdigitaliseringenveiligheid.nl

Een werkveldpartner die heel erg voor de hand ligt, maar waar we nog maar relatief kort actief zaken mee doen, is NHL Stenden Hogeschool. De hogeschool biedt een inspiratievolle omgeving om allerlei onderzoek te doen op het gebied van digitale weerbaarheid. Onderwijsorganisaties hebben te maken met een open omgeving en worden ook geconfronteerd met diverse digitale dreigingen en risico's, zoals ransomware-aanvallen en datalekken (SURF, 2022). Denk bijvoorbeeld aan de aanval op de Universiteit van Maastricht[84] en ROC Mondriaan[85].

Dergelijke incidenten beginnen doordat er bijvoorbeeld op een verkeerd linkje is geklikt, slecht wachtwoordbeleid is gevoerd of omdat een geïnfecteerd bestand is gedownload. Ook zien we dat kwetsbaarheden in software voor problemen kunnen zorgen, zoals in 2021 het geval was door de Apache Log4j software.[86] Dit betekent dat de digitale weerbaarheid van deze sector dus ook verder omhoog moet (SURF, 2022; Inspectie van het Onderwijs, 2021). Voor zover bekend is NHL Stenden Hogeschool (nog) niet getroffen door een grootschalig incident, maar dat neemt niet weg dat dit in de toekomst kan gebeuren. Het is dus belangrijk om zoveel mogelijk te voorkomen dat dergelijke incidenten zich zullen voordoen (cybersecurity) en wanneer deze zich voordoen de impact zo laag mogelijk te houden (weerbaarheid). Een van de manieren om dat te doen – en waar het lectoraat aan bijdraagt – is via bewustwording. Zo hebben we bijvoorbeeld ten tijde van Covid-19 webinars

[84] https://nos.nl/artikel/2321732-hackers-universiteit-maastricht-zaten-maanden-in-netwerk-200-000-euro-betaald
[85] https://nos.nl/artikel/2401109-roc-mondriaan-vergoedt-identiteitsbewijzen-na-hack
[86] https://www.digitaleoverheid.nl/nieuws/53875/

gegeven en een infographic ontwikkeld met praktische handvatten voor veilig thuiswerken, en zijn we recent betrokken bij een bewustwordingsprogramma voor medewerkers (zie kader 3.3).

Ook biedt deze samenwerking veel kansen om de kennis en expertise die we opbouwen, terug te laten komen in het beleid van NHL Stenden Hogeschool. Zo zijn kenniskringleden van de onderzoeksgroep onder andere uitgenodigd om mee te denken over en/of mee te werken aan het digitaliseringsbeleid, het cyberawareness programma en de digitale agenda van de hogeschool, en hebben we recent bijvoorbeeld een training verzorgd voor de Raad van Toezicht. Ook is een van de kenniskringleden, Sander Ebbers, actief als data protection counselor. Het stemt positief dat digitale veiligheid serieus wordt genomen en digitale weerbaarheid stevig wordt omarmd binnen de hogeschool. Ook is het een mooie erkenning van het werk dat het lectoraat heeft gerealiseerd dat we worden uitgenodigd om hieraan bij te dragen.

Daarnaast proberen we zoveel mogelijk aan te haken bij bredere programma's die vanuit NHL Stenden Hogeschool worden georganiseerd en aangeboden aan het werkveld. Immers, digitalisering speelt overal een rol, en zou daarom overal aandacht moeten krijgen. Op het gebied van digitale veiligheid zien we echter dat er nog een wereld te winnen is. De ervaring leert dat om effectief te zijn niet per se zelf dingen georganiseerd te hoeven worden, maar dat het soms beter is om aan te sluiten bij bestaande initiatieven. Een voorbeeld daarvan is het programma Veerkrachtig Ondernemen van het Center for Entrepreneurship waarvoor wij een sessie over digitale weerbaarheid hebben verzorgd. Het lectoraat werkt bij dergelijke initiatieven graag samen met interne partners op het gebied van digitale veiligheid en privacy, waaronder de CISO en de Functionaris Gegevensbescherming (FG).

Kader 3.3: Awareness van medewerkers van NHL Stenden Hogeschool (meerjarenproject, lopend)

Binnen NHL Stenden Hogeschool worden diverse maatregelen genomen om hacks en andere digitale aanvallen te voorkomen en de impact daarvan te minimaliseren. Hierbij kan gedacht worden aan technische maatregelen, zoals de implementatie van multifactorauthenticatie (MFA), het scannen op phishingmails en het monitoren van het dataverkeer. Daarnaast worden organisatorische maatregelen getroffen, zoals het ontwikkelen van beleid en maatregelen (richtlijnen, gedragsregels en protocollen), het simuleren van phishing-aanvallen en het oefenen met cybercrisisscenario's (incident response). Ook wordt samengewerkt met partijen zoals SURF (een coöperatieve vereniging van Nederlandse onderwijs- en onderzoeksinstellingen), bijvoorbeeld op het gebied van informatie-uitwisseling.

In het kader van bewustwording werkt het lectoraat nauw samen met interne en externe partners. Een project waar nu aan wordt gewerkt is het ontwikkelen van een e-learning programma. Hoewel in de inleiding het beeld wordt geschetst dat een one-size-fits-all benadering voor bewustwording en gedragsverandering niet de meest efficiënte oplossing is, is onze aanpak anders in die zin dat het betreffende programma niet een standaard aangekocht geheel is, maar deze specifiek op de situatie van NHL Stenden Hogeschool is toegesneden. Eveneens zorgen we door middel van een trapsgewijze aanpak over meerdere jaren heen voor de nodige verdieping en hebben we aandacht voor concrete doelgedragingen en continue verbetering. Vanuit het lectoraat leveren we de inhoud en stemmen deze af met de CISO, FG en medewerkers van team Privacy en Security. De tooling wordt extern ontwikkeld. Dit project begeeft zich ten tijde van schrijven in de lanceringsfase van de eerste serie van een grotere bewustwordingsreeks.

3.3 Verbinding met onderwijs

Een andere fundamentele taak van het lectoraat – naast kennisontwikkeling en -deling en oplossingen bedenken voor de beroepspraktijk en maatschappelijke vraagstukken – is de doorwerking van de ontwikkelde kennis (en oplossingen) in het onderwijs. Het lectoraat wil dan ook de wisselwerking en samenhang met het onderwijs op dit specifieke onderwerp verder uitbouwen binnen NHL Stenden Hogeschool en de Politieacademie. Het lectoraat heeft reeds een goede verbinding met het onderwijs van NHL Stenden Hogeschool. Het thema digitale weerbaarheid is verankerd in de Thorbecke Academie opleiding Integrale Veiligheidskunde (IVK) en bij HBO-Rechten worden diverse activiteiten ontplooid. Het lectoraat staat open voor samenwerking met andere opleidingen.

Een concreet voorbeeld van de verbinding tussen het lectoraat en onderwijs betreft de Engelstalige minor van IVK: Cyber Resilience of Citizens and Organisations (CROCO). Deze minor staat open voor (internationale) studenten van verschillende opleidingen, binnen en buiten NHL Stenden Hogeschool. In deze minor wordt gefocust op menselijke en organisatorische maatregelen die burgers en organisaties kunnen nemen om digitaal weerbaar te worden én te blijven. Het gaat hierbij zowel om preventie als repressie. Vragen die centraal staan zijn: Hoe zorg je voor bewustwording? Hoe maak je beleid en procedures? Hoe gaan cybercriminelen te werk? Hoe bereid je je voor op en hoe herstel je van cyberincidenten? En: Hoe gaan we om met de steeds grotere afhankelijkheid van digitale middelen? Binnen de minor gaan studenten aan de slag met real-life opdrachten uit het werkveld. Het werkveld speelt ook een belangrijke rol in het verzorgen van het minor-onderwijs door middel van het geven van workshops en verzorgen van gastcolleges. Dus ook op dat vlak wordt een mooie verbinding gerealiseerd. Het werkveld is dusdanig enthousiast dat ze jaarlijks wil terugkeren om studenten te vertellen over hun werkzaamheden.

Om studenten die zich willen verbreden naar andere 'cyber'-disciplines (een veel gehoorde behoefte tijdens evaluaties van het 'cyber'-onderwijs) daarin te faciliteren, zijn we een vruchtbare samenwerking aangegaan met HBO-ICT en het Maritiem Instituut Willem Barentz van NHL Stenden Hogeschool. Dit heeft geresulteerd in een gezamenlijk 'Cyber Safety & Security' minoren-aanbod, waarbij ook de Engelstalige minoren Certified Ethical Hacking, Secure Programming en Hack@Sea worden aangeboden. We hebben per periode een gezamenlijke kick-off en afsluiting, en studenten kunnen naar gelang hun eigen leerbehoefte shoppen bij deze vier minoren, om zodoende een 'op maat' gemaakt programma te volgen. Mogelijk kunnen in de nabije toekomst hier nog andere minoren bij aansluiten.

Een voordeel van deze samenwerking – alsook het openstellen van de minor voor studenten met diverse achtergronden (cultuur en domein) – is dat studenten zich gedurende de minor niet alleen verbreden op het onderwerp, maar ook worden aangemoedigd om met verschillende perspectieven naar complexe vraagstukken te kijken en oplossingen te bedenken. Dit is voor IVK-studenten extra belangrijk, omdat zij vaak met professionals uit verschillende domeinen c.q. expertisegebieden in contact staan en een verbindende rol spelen in de organisaties waarvoor zij gaan werken.[87] Studenten leren – via samenwerking – om zich te verplaatsen in de belevingswereld van bijvoorbeeld ICT- en rechtenstudenten. Dit geldt andersom ook natuurlijk. Het helpt studenten elkaars taal te begrijpen en wederzijds begrip te vergroten.

Hierna licht ik een voorbeeld uit van een project dat studenten voor ons hebben uitgevoerd (kader 3.4). Het is niet zo dat het lectoraat alleen kennis komt brengen naar de opleidingen. Een waardevolle verbinding ligt ook in het ophalen van kennis. Waar mogelijk proberen we studenten – van NHL Stenden Hogeschool en de Politieacademie – aan te laten sluiten bij de projecten die we uitvoeren. Dat kan bijvoorbeeld via minoren, atelier, leerbedrijf of door ze als afstudeerder te verbinden aan het lectoraat. Soms zien we ontwikkelingen die zich in de maatschappij voordoen, en die we belangrijk achten, maar waar we bijvoorbeeld zelf (nog) geen onderzoek naar hebben lopen. Studenten helpen ons dan om dergelijke onderwerpen nader te onderzoeken.[88] Dit levert vaak interessante beroepsproducten op waar we gelijk wat mee kunnen en/of goede inzichten die we kunnen toepassen in nieuwe subsidieaanvragen.

Kader 3.4: Digitale weerbaarheidsmonitor (lopend)

In periode 2 van de derdejaars minor CROCO (2022-2023) is een groep van drie studenten aan de slag gegaan om een digitale weerbaarheidsmonitor te ontwikkelen. Het doel erachter is dat in Nederland geen structurele aandacht is voor het meten van digitale weerbaarheid. Dit in tegenstelling tot bijvoorbeeld slachtofferschap van online criminaliteit in de Veiligheidsmonitor. De monitor moet een beperkt aantal kernthema's bevatten waarmee inzicht kan worden verkregen in de digitale weerbaarheid van burgers. Dat de thema's beperkt moeten worden, komt voornamelijk doordat de monitor op straat moet worden afgenomen. Er moet een vaste set met vragen komen, zodat vergelijkingen over de tijd mogelijk zijn. Daarbij moet een kort flexibel deel worden ingevoegd waarmee ruimte ontstaat om vragen te stellen over actuele thema's. Deze studentengroep heeft op basis van bovenstaande criteria een concept monitor ontwikkeld. Zij hebben daarvoor de HAIS-Q-vragenlijst (Parsons e.a., 2014; 2017) en de SeBIS-schaal (Egelman & Peer, 2015) als primaire bronnen gebruikt.

[87] https://www.verenigingenhogescholen.nl/system/profiles/documents/000/000/083/original/AA_Schets_IVK_Bedrijfsprofiel_2019.pdf?1572365401

[88] Voorbeelden van onderwerpen zijn: veilig gebruik van huishoudelijke IoT-apparatuur, evaluatie van gemeentelijk veiligheidsbeleid (a.d.h.v. de lokale cyberwegenkaart), implicaties van nieuwe normenkaders (ISO27001:2022), digitaal nalatenschap en de impact van de NIS2 richtlijn.

Aan de hand van dit concept zijn op moment van schrijven (periode 3 en 4) drie vierdejaars Atelier-studenten aan de slag om dit door te ontwikkelen tot een eindproduct dat toegepast kan worden in het tweedejaars onderwijs van de opleiding IVK. Dit betekent dat waar de eerste studentengroep zich vooral richtte op de inhoud, de tweede groep zich voornamelijk richt op de praktische invulling ervan. Wat zijn bijvoorbeeld de behoeften en requirements die vanuit het onderwijs (vakinhoudelijke docenten en onderzoeksdocenten) gelden en belangrijk worden geacht?

Uiteindelijk gaan tweedejaars IVK-studenten dit instrument gebruiken om hun onderzoeksvaardigheden te ontwikkelen en uit te breiden. Studenten kunnen – in samenwerking met docent-onderzoekers – tevens ervaring opdoen om over de resultaten en conclusies te publiceren. Doordat met een gestandaardiseerde set vragen wordt gewerkt kunnen na verloop van tijd ook trends worden beschreven. De verwachting is dat deze monitor vanaf komend studiejaar (2023-2024) wordt geïntroduceerd in het IVK-onderwijs. Een mooi voorbeeld van een verbinding van het lectoraat – via studenten – met het onderwijs.

Naast de minor CROCO is er binnen de opleiding IVK een afstudeerrichting 'cybersafety', waarbij studenten die vanaf het derde studiejaar de 'cyber' richting kiezen en erin afstuderen een aantekening krijgen op hun diploma. Ook komen diverse elementen van het thema terug in verschillende onderwijseenheden van IVK, zoals in het eerstejaars vak Bedrijf en Veiligheid en het vierdejaars Atelier Veiligheid en Recht. Dit wordt gerealiseerd door docent-onderzoekers van zowel binnen als buiten het lectoraat. Ook biedt het lectoraat afstudeerplekken aan. Bij HBO-Rechten fungeert het lectoraat als opdrachtgever bij de minor Recht en Digitaal Ondernemen. Daarnaast wordt door middel van gastcolleges een bijdrage geleverd aan het onderwijs van andere opleidingen en academies. In een ideale wereld wordt *cyber* – al spreek ik liever van *digitaal* – standaard onderdeel binnen alle (relevante) vakken en modules. Immers, digitalisering en digitale veiligheid zijn overal van belang. Echter, zo lang dit nog niet het geval is, schenken we op deze manier er op zijn minst aandacht aan.

Naast bachelor-onderwijs kijken we als onderzoeksgroep verder. Zo verzorgen we bijvoorbeeld divers cursusaanbod. Dit geldt met name op het moment dat zich specifieke ontwikkelingen op het gebied van digitale veiligheid voordoen, zoals in 2018 met de AVG, of als werkveldpartners daar specifiek om vragen. Dit kan gaan om meerdaagse programma's, maar ook om kortere programma's van bijvoorbeeld een dagdeel. Een voorbeeld is een meerdaagse cursus die we in 2021 samen met de Academie ICT & Creative Technologies (ICT&CT) verzorgenden in het kader van het programma I-Partnerschap.[89]

[89] https://www.rijksorganisatieodi.nl/i-partnerschap

Tevens wil ik hier de ontwikkeling van de deeltijdopleiding Ad Cyber Safety & Security noemen die eind 2022 is goedgekeurd. Dit resultaat komt op het conto van de vruchtbare samenwerking tussen de academies: Thorbecke en ICT&CT, die sinds 2019 steeds structureler is geworden, alsook de ondersteunende diensten die daarin van onschatbare waarde zijn geweest. Dergelijke programma's zijn essentieel in een tijd waarin cyber-expertise schaars is (CSR, 2021; Furnell, 2021; NCSC, 2022).

De komende jaren proberen we de verbinding met het onderwijs te versterken, zowel binnen NHL Stenden Hogeschool als de Politieacademie. De doorontwikkeling van curricula staat daarbij centraal, maar ook de professionalisering van docent-onderzoekers. De ambitie is dan ook om meer met docent-onderzoekers (van beide instellingen) samen te werken in onderwijs en onderzoek. Bovendien kan een mooie uitwisseling ontstaan door collega's van beide instellingen aan elkaar te verbinden. Ook kan de bijdrage aan het onderwijs van de Politieacademie structureler worden neergezet. Momenteel is de inzet ad hoc[90], maar onder andere via het in oprichting zijnde kcDIT proberen we die relatie te verduurzamen. Daarbij kan bijvoorbeeld worden gedacht aan onderwijsontwikkeling (op bachelor- en masterniveau). Een belangrijke impuls die het lectoraat tot slot wil geven is aan het professionaliseren van docent-onderzoekers. Dit gebeurt door docent-onderzoekers te laten participeren in onderzoek, bijvoorbeeld in termen van het bijhouden van literatuur, het ontwikkelen en/of uitbouwen van onderzoeksvaardigheden, het publiceren over onderzoek en het presenteren ervan op (internationale) conferenties. Daarmee is ook direct de doorwerking naar het onderwijs geborgd. Via het SPRONG-project zullen we hier ook nader invulling aan geven. Het is daarnaast mogelijk om aan promotieonderzoek te werken binnen het lectoraat (zie hoofdstuk 2).

[90] Voorbeelden omvatten scriptiebegeleiding en het verzorgen van gastcolleges en workshops bij de Politiekundige bachelor, de Master of Policing (een gemeenschappelijke master van de Politieacademie en de Canterbury Christchurch University) en andere onderwijsuitingen, zoals de Integrale Vervolg Opleiding Opsporing (IVOO).

Hoofdstuk 4

Lectoraat Digitale Weerbaarheid van Mens en Organisatie

In de vorige hoofdstukken is de context gepresenteerd en zijn de grootste knelpunten en uitdagingen waarvoor we staan aangaande digitale veiligheid besproken. Daarnaast is uiteengezet hoe we met het lectoraat – samen met onderwijs, werkveld en partners – invulling geven om deze knelpunten en uitdagingen aan te pakken. Belangrijke uitgangspunten hierbij zijn dat we de mens centraal moeten stellen in het vergroten van de digitale weerbaarheid, de mens daarbij moeten beschouwen als een actor die bijdraagt aan de oplossing, en dat we moeten investeren in goede samenwerking. In dit laatste hoofdstuk presenteer ik de kerngroep van het lectoraat Digitale Weerbaarheid van Mens en Organisaties. Samen gaan we de uitdaging aan om onze ambities te verwezenlijken. Het hoofdstuk eindigt met een slotwoord.

Jurjen Jansen

Jurjen Jansen (1983) heeft Communication & Multimedia Design gestudeerd aan NHL Stenden Hogeschool (2001-2005). Daarna heeft hij zijn master gehaald in Communication Studies aan de Universiteit Twente (2005-2007). Aansluitend is hij als wetenschappelijk onderzoeker gaan werken aan de Universiteit Twente bij de vakgroep Media, Communication and Organisations. In 2010 maakte Jurjen de overstap naar de onderzoeksgroep Cybersafety van NHL Stenden Hogeschool. In 2018 is hij gepromoveerd op het terrein van human-centered cybersecurity. Dit deed hij aan de Open Universiteit op het proefschrift 'Do you bend or break? Preventing online banking fraud victimization through online resilience'. Zijn promotieonderzoek richtte zich op het versterken van de digitale weerbaarheid van gebruikers van internetbankieren. Sinds 2022 is Jurjen als lector verbonden aan de onderzoeksgroep Cybersafety. Hij is verantwoordelijk voor de aansturing en ontwikkeling van het lectoraat Digitale Weerbaarheid van Mens en Organisatie van de onderzoeksgroep alsook voor acquisitie, en de uitvoering en kwaliteitsbewaking van het onderzoek. Jurjen is tevens verbonden aan de Politieacademie, sector Kennis en Onderzoek. Daar houdt hij zich primair bezig met de ontwikkel- en veranderopgave voor een digitaal vaardige politie. Jurjen heeft veel ervaring met hoogwaardig praktijkgericht onderzoek op het gebied van digitalisering en veiligheid. Naast diverse presentaties op uiteenlopende conferenties, symposia en themabijeenkomsten in binnen- en buitenland, heeft hij meerdere (wetenschappelijke) publicaties op zijn naam staan. Tot slot is hij actief betrokken bij het ontwikkelen van onderwijs op het gebied van veiligheid en digitalisering. Zo heeft hij samen met collega's de minor Cyber Resilience of Citizens and Organisations opgezet (Bachelor) en de deeltijdopleiding Cyber Safety & Security (Ad) ontwikkeld.

Saskia Westers

Saskia Westers (1991) heeft in 2017 de masters Rechtspsychologie aan de Maastricht Universiteit en Forensische Criminologie aan de Universiteit Leiden afgerond. Ze heeft extra onderzoekservaring opgedaan als student-assistent bij beide universiteiten. Als werknemer bij de ING Fraudedetectie heeft zij praktijkervaring opgedaan in het opsporen en aanpakken van cybercriminaliteit in de financiële sector. Saskia is sinds 2018 werkzaam als docent-onderzoeker bij de onderzoeksgroep Cybersafety en opleiding Integrale Veiligheidskunde van NHL Stenden Hogeschool. Bij de onderzoeksgroep ligt haar focus op digitale weerbaarheid en de politie in de digitale samenleving. Saskia werkte mee aan diverse onderzoeksprojecten, zoals naar de rol van encryptie in de opsporing, politiestraatwerk onder Corona, toekomstige cybercriminele verdienmodellen en online aankoopfraude vanuit het buitenland. Tevens voerde zij samen met collega's effectstudies uit naar het gebruik van bodycams en automatische kentekenherkenning (ANPR). Als docent is Saskia coördinator geweest van derde- en vierdejaars minoren Cybersafety. Nu coördineert ze de vierdejaars minor Atelier Veiligheid en Recht, en begeleidt ze studentgroepen bij onderzoeken met een digitaal veiligheidsvraagstuk en bij hun afstudeertraject. Tevens is ze oprichter van het leerbedrijf Digitalisering en Veiligheid.

Sander Ebbers

Sander Ebbers (1989) studeerde in 2015 af in de master Arbeids-, Organisatie- en Personeelspsychologie aan de Rijksuniversiteit Groningen. Daarna werkte hij als adviseur Informatiebeveiliging & Security Awareness bij Insite Security. Sander kwam in januari 2020 in dienst als docent-onderzoeker bij de onderzoeksgroep Cybersafety en de opleiding Integrale Veiligheidskunde. Zijn specialisatiegebied is gedrag en digitale veiligheid binnen organisaties. Zo werkt Sander bijvoorbeeld aan een project om ondernemers in de regio Noordoost-Fryslân digitaal weerbaarder te maken en is hij betrokken bij de ontwikkeling van een e-learning-programma voor medewerkers van NHL Stenden Hogeschool. Daarnaast is Sander per september 2022 gestart met een promotieonderzoek. Dit onderzoek gaat over het verkennen en versterken van meldgedrag van digitale (bijna-)incidenten. Hij is daarvoor als buitenpromovendus verbonden aan de Open Universiteit. Sander is eveneens actief het onderwijs. Hij coördineert en doceert in de minor Cyber Resilience of Citizens and Organisations, begeleidt studenten bij afstudeertrajecten en ondersteunt het leerbedrijf Digitalisering en Veiligheid. Tot slot is Sander werkzaam als data protection counselor, waarbij hij ondersteuning biedt aan team Privacy en Security van NHL Stenden Hogeschool.

Maike Berkenpas

Maike Berkenpas (1996) heeft in de zomer van 2020 de opleiding Integrale Veiligheidskunde afgerond aan NHL Stenden Hogeschool, waarbij zij zich vanaf het derde studiejaar is gaan specialiseren in cybersafety. Maike is sinds december 2020 werkzaam als docent-onderzoeker bij de onderzoeksgroep Cybersafety en sinds augustus 2021 bij de opleiding Integrale Veiligheidskunde. Maike heeft waardevolle bijdragen geleverd aan onderzoeksprojecten zoals de evaluatie van de Basisscan Cyberweerbaarheid van het Digital Trust Center (DTC) en het onderzoek naar de rol van encryptie in de opsporing dat in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) is uitgevoerd. Maike is trots op het feit dat ze aan maatschappelijk relevante en betekenisvolle projecten werkt die op allerlei manieren te maken hebben met het bevorderen van de digitale weerbaarheid van burgers en organisaties. Zij is daarnaast ook actief in het onderwijs. Zij doceert in de minor Cyber Resilience of Citizens and Organisations en begeleidt studenten die stagelopen in het derde studiejaar. Begin 2023 is Maike gestart met een premaster met als doel om door te stromen naar de master Governance & Law in Digital Society van de Rijksuniversiteit Groningen.

Kimberly Bluhm

Kimberly Bluhm (1996) heeft in de zomer van 2019 de bachelor Integrale Veiligheidskunde afgerond aan NHL Stenden Hogeschool. In het laatste jaar van deze bachelor heeft zij zich gespecialiseerd in cybersafety en de bijbehorende aantekening op haar diploma gekregen. Hierin heeft zij zich onder andere gefocust op criminele activiteiten die plaatsvinden op sociale mediaplatformen. Vervolgens is zij in 2020 gestart met de master Psychology of Conflict, Risk & Safety aan de Universiteit Twente en in maart 2023 heeft zij deze opleiding met succes afgerond. Om extra onderzoekservaring op te doen tijdens de master, is zij via het leerbedrijf Digitalisering en Veiligheid in contact gekomen met de onderzoeksgroep Cybersafety, waarvoor ze sinds november 2022 werkzaam is. Zij heeft meegewerkt aan het promotieonderzoek van Jildau Borwell waarbij de impact van cybercrime is vergeleken met de impact van traditionele criminaliteit. Dit heeft geresulteerd in een publicatie in het Tijdschrift voor Veiligheid en een aanstelling bij de onderzoeksgroep. Momenteel werkt Kimberly aan een evaluatieonderzoek van diverse digitale weerbaarheidsprojecten.

Slotwoord

Met deze laatste alinea sluit ik het boekwerk af dat ik heb geschreven ter gelegenheid van mijn lectorale rede (30 mei 2023). Mocht u tijdens of na het lezen van dit werk interessante ideeën hebben gekregen voor onderzoek en samenwerking, dan nodig ik u uit om contact op te nemen met het lectoraat Digitale Weerbaarheid van Mens en Organisaties. Wij staan altijd open voor nieuwe 'verbindingen' en verkennen graag de mogelijkheden om samen te werken aan een samenleving die digitaal weerbaar is én blijft.

Referenties

Accenture (2022). *Technology vision 2022 – Meet me in the metaverse: The continuum of technology and experience, reshaping business*. Via: https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/_acnmedia/thought-leadership-assets/pdf-5/Accenture-Meet-Me-in-the-Metaverse-Full-Report.pdf

Ahmad, T. (2020) Corona virus (Covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *SSRN*. doi.org/10.2139/ssrn.3568830

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*, 276–289.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*, 432–445.

Alnifie, K.M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis. *Journal of Information Security, 14*, 93–110.

AP (2021). *Smart Cities: Onderzoeksrapport bescherming van persoonsgegevens in de ontwikkeling van Nederlandse Smart Cities*. Autoriteit Persoonsgegevens.

Arachchilage, N.A.G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304–312.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191–215.

Bantema, W. (2023). *Bestuurlijk koorddansen in een digitale samenleving*. NHL Stenden Hogeschool.

Bantema, W., Westers, S., Hoekstra, M., Herregodts, R., & Munneke, S, (2021). *Black box van gemeentelijke online monitoring: Een wankel fundament onder een stevige praktijk*. Sdu (Politie en Wetenschap).

Becker, I., Parkin, S., & Sasse, M.A. (2017). Finding security champions in blends of organizational culture. In *Proceedings of the 2nd European Workshop on Usable Security* (pp. 1–11). Internet Society.

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

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M.A., & Passingham, N. (2015). *Awareness is only the first step*. Hewlett Packard.

Bluhm, K. (2023). *Ready, set, know: The race against cybercrime and the importance of actual knowledge*. Universiteit Twente (master scriptie).

Bluhm, K., Borwell, J., & Stol, W.Ph. (2022). De slachtofferimpact van cybercrime versus traditionele criminaliteit: Aanknopingspunten voor slachtofferzorg en preventieprioriteiten. *Tijdschrift voor Veiligheid, 21*(3–4), 13–31.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology, 10*(34), 1022–1035.

Boelens, M., & Landman, W. (2021). *Pionieren in gebiedsgebonden politiewerk: Een onderzoek naar de digitaal wijkagent in het basisteam.* Politie Nederland / TwynstraGudde.

Boheemen, P. van, Munnichs, G., Kool, L., Diercks, G., Hamer, J., & Vos, A. (2020). *Cyberweerbaar met nieuwe technologie: Kans en noodzaak van digitale innovatie*. Rathenau Instituut.

Borwell, J., Jansen, J., & Stol, W.Ph. (2018). Human factors leading to online fraud victimisation: Literature review and exploring the role of personality traits. In J. McAlaney, L.A. Frumkin en V. Benson (red.), *Psychological and behavioral examinations in cyber security* (pp. 26–45). IGI Global.

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

Borwell, J., Jansen, J. & Stol, W.Ph. (2021b). The psychological and financial impact of cybercrime victimization: A novel application of the shattered assumptions theory. *Social Science Computer Review, 40*(4). doi.org/10.1177/0894439320983828

Borwell, J., Schuppers, K., Rooyakkers, J., & Harteveld, A. (2020). Het cybercrimebeeld van de Nederlandse politie: Van algemeen beeld naar verdiepende analyse en aanpak. *Cahiers Politiestudies, 56*, 39–62.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864.

Brouwer, N., & Mil, J. van (2023). Cybersecurity in Europa: De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS2). *Nederlands Juristenblad, 10*, 748–757.

Bruine, H. de (2018). Organiseren van veiligheid. In F. Guldenmund (red.), *Gedrag en Veiligheid* (pp. 153-168). Vakmedianet.

Brunner, M. (2020). Challenges and opportunities in state and local cybercrime enforcement. *Journal of National Security Law & Policy, 10*, 563–582.

Bullée, J.-W. (2017). *Experimental social engineering: Investigation and prevention*. Universiteit Twente (proefschrift).

CEPOL (2022). *European Union strategic training needs assessment 2022–2025*. Via: https://www.cepol.europa.eu/api/assets/European_Union_Strategic_Training_Needs_Assessment_2022_2025_EUSTNA.pdf

CBS (2021). *Cybersecuritymonitor 2020*. Centraal Bureau voor de Statistiek.

CBS (2022). *Veiligheidsmonitor 2021*. Centraal Bureau voor de Statistiek.

Cockcroft, T.W., Shan-A-Khuda, M., Schreuders, C., & Trevorrow, P. (2018). Police cybercrime training: Perceptions, pedagogy and policy. *Policing: A Journal of Policy and Practice, 15*(1), 15–33.

Collier, B., Horgan, S., Jones, R., & Shepherd, L.A. (2020). *The implications of the covid-19pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations*. Scottish Institute for Policing Research.

Cooper, M.D. (2022). The emperor has no clothes: A critique of Safety-II. *Safety Science*. doi.org/10.1016/j.ssci.2020.105047

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In *Proceedings of the International Conference on Human-Computer Interaction* (pp. 105–122). Springer.

Coventry, L., Briggs, P., Blythe, J.M., & Tran, M. (2014). *Using behavioural insights to improve the public's use of cyber security best practices*. Government Office for Science.

Cram, W.A., D'arcy, J., & Proudfoot, J.G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525–554.

Crossland, G. (2022). *Using psychological theories and usable security to understand cyber-security perceptions and behaviours within an organization: A case study of a law firm*. Royal Holloway, University of London (proefschrift).

Crossler, R.E., Bélanger, F., & Ormond, D. (2019). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers, 21*(2), 343-357.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.

CSR (2021). *Adviesrapport – Integrale aanpak cyberweerbaarheid: Een integrale aanpak om de open, vrije en welvarende Nederlandse samenleving structureel cyberweerbaar te maken en (digitale) kansen te verzilveren*. Cyber Security Raad.

Cybersecurity Alliantie & Cyberveilig Nederland (2021). *Cybersecurity woordenboek 2021: Van cybersecurity naar Nederlands*. Via: https://www.cybersecurityalliantie.nl/ ecp_images/2021/12/Cybersecurity-Woordenboek-2021_ZonderSpreads.pdf

Davis, F.D. (1989). Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Quarterly, 13*(3), 319–340.

Dekker, S. (2012). *Just Culture: Balancing safety and accountability*. Ashgate Publishing.

Dekker, S. (2014). Employees: A problem to control or solution to harness. *Professional Safety, 58*(8), 32–36.

Dekker, S., & Conklin, T. (2022). *Do Safety Differently*. Pre Accident Media.

Deursen, A.J.A.M. van, & Helsper, E.J. (2021). *Mediawijsheid: conceptualisering en belang in een gemedieerde samenleving: Lacunes in bestaand onderzoek en beleid*. Universiteit Twente.

Dijk, J.A.G.M. van (2012). *The network society* (third edition). SAGE Publications.

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

Ducheine, P. (2018). Het bevorderen en beschermen van nationale belangen in een democratische rechtsstaat in het informatietijdperk (pp. 26–46). In *Ordening in de dreiging: Beschouwingen over internationale veiligheid en de toekomst van de liberale democratie* (pp. 26–46). Mr. Hans van Mierlo Stichting.

Duin, M. van, & Maan, J. (2018). Cyberaanval op Maersk. In M. van Duin, V. Wijkhuijs en W. Jong (red.), *Lessen uit crises en mini-crises 2017* (pp. 119-129). Boom bestuurskunde.

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

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual Conference on Human Factors in Computing Systems* (pp. 2873–2882). ACM.

ENISA (2019). *Cybersecurity culture guidelines: Behavioural aspects of cybersecurity*. Via: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

ENISA (2022). *ENISA threat landscape 2022*. Via: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Europol (2020). *Internet organised crime threat assessment (IOCTA) 2020*. Via: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020#downloads

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley.

Fishbein, M., & Ajzen, I. (2010). *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis.

Floyd, D.L., Prentice-Dunn, S., & Rogers, R.W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407–429.

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security, 100*. https://doi.org/10.1016/j.cose.2020.102080

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security, 31,* 983–988.

Furnell, S., & Vasileiou, I. (2019). A holistic view of cybersecurity education requirements. In I. Vasileiou en S. Furnell (red.), *Cybersecurity education for awareness and compliance* (pp. 1–18). IGI Global.

Glaspie H.W., & Karwowski W. (2017). Human factors in information security culture: A literature review. In *Proceedings of the International Conference on Applied Human Factors and Ergonomics* (269-280). Springer.

Groeneweg, J. (2018). Beslissingen en fouten. In F. Guldenmund (red.), *Gedrag en Veiligheid* (pp. 57-72). Vakmedianet.

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *Data Base for Advances in Information Systems, 52*(2), 25–67.

Hadlington, L., Lumsden, K., Black, A., & Ferra, F. (2018). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice, 15*(1), 34–43.

Hallas, B. (2018). *Rethinking the human factor: A philosophical approach to information security awareness, behaviour and culture*. The Hallas Institute.

Hoekstra, M., Vries, S. de, Berkenpas, M., & Jansen, J. (2021). *De werking van de Basisscan Cyberweerbaarheid: Een kwalitatief onderzoek naar het gedrag van ondernemers*. Cybersafety Research Group.

Hielscher, J., Kluge, A., Menges, U., & Sasse, M.A. (2021). "Taking out the trash": Why security behavior change requires intentional forgetting. In *Proceedings of the New Security Paradigms Workshop* (pp. 108–122). ACM.

Hoff-de Goede, S. 't, Kleij, R. van der, Weijer, S. van de, & Leukfeldt, E.R. (2019). *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*. De Haagse Hogeschool / NSCR.

Hollnagel, E. (2008). Risk + Barriers = Safety? *Safety Science, 46*(2), 221–229.

Hollnagel, E. (2014). *Safety-I and Safety-II: The past and future of safety management*. CRC Press.

Holt, T.J., & Bossler, A.M. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 464–472.

Holt, T.J., & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.

Huisman, A., Princen, M., Klerks, P., & Kop, N. (2016) *Handelen naar waarheid: Sterkte- en zwakteanalyse van de opsporing*. Politieacademie.

Hull, M., Eze, T., & Speakman, L. (2018). Policing the cyber threat: Exploring the threat from cyber crime and the ability of local law enforcement to respond. In *Proceedings of the European Intelligence and Security Informatics Conference* (pp. 15–22). IEEE.

IBD (2022). *Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 2023 – 2024*. Informatiebeveiligingsdienst.

Inspectie van het Onderwijs (2021). *Binnen zonder kloppen: Digitale weerbaarheid in het hoger onderwijs*. Ministerie van Onderwijs, Cultuur en Wetenschap.

Inspectie Justitie en Veiligheid (2017). *Modernisering van de gebiedsgebonden politiezorg: Afsluitend onderzoek naar de vorming van de nationale politie*. Ministerie van Justitie en Veiligheid.

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Open Universiteit (proefschrift).

Jansen, J., & Leukfeldt, E.R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79–91.

Jansen, J., & Leukfeldt, E.R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology, 6*(2), 205–228.

Jansen, J., & Schaik, P. van (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security, 25*(2), 165–180.

Jansen, J., & Schaik, P. van (2018a). Persuading end users to act cautiously online: A fear appeals study on phishing. *Information & Computer Security, 26*(3), 264–276.

Jansen, J., & Schaik, P. van (2018b). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior, 87*, 371–383.

Jansen, J., & Schaik, P. van (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human – Computer Studies, 123*, 40–55.

Jansen, J., & Stol, W.Ph. (2019). *Cyber-to-Go roadshow: Evaluatie van een methodiek om cyberweerbaarheid te vergroten.* Cybersafety Research Group (niet openbaar).

Jansen, J., Kop, N., & Stol, W.Ph. (2017). *Internetbankieren: Veiligheidspercepties van gebruikers. Tijdschrift voor Veiligheid, 16*(1), 36–51.

Jansen, J., Valkengoed, van T., Veenstra, S., & Stol, W.Ph. (2020). *Level-Up! Kennis voor politiewerk in een digitale samenleving.* Cybersafety Research Group.

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W.Ph. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology, 35*(5), 368-379.

Jansen, J., Westers, S., Schreurs, W., Berkenpas, M., Alpár, G., & Stol, W.Ph. (2023). *De rol van encryptie in de opsporing: Belemmeringen en mogelijkheden.* Cybersafety Research Group.

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

Jones, N.A., Ross, H., Lynam, T., Perez, P., & Leitch, A. (2011). Mental models: An interdisciplinary synthesis of theory and methods. *Ecology and Society 16*(1). https://www.jstor.org/stable/26268859

Kahneman, D. (2011). *Thinking, fast and slow.* Penguin Group.

Kaouass, A., & Zannoni, M. (2017). *De veiligheidsregio en cyberagenda 2017–2020: Voorbereid, betrokken en betrouwbaar.* COT: Instituut voor Veiligheids- en Crisismanagement.

Kaur, M., Eeten, M. van, Janssen, M., Borgolte, K., & Fiebig, T. (2021). *Human factors in security research: Lessons learned from 2008–2018.* TU Delft.

Kemp, S., Buil-Gil, D., Miró-Llinares, F., & Lord, N. (2021). When do businesses report cybercrime? Findings from a UK study. *Criminology & Criminal Justice*. doi.org/10.1177/17488958211062359

Kerpershoek, E., Westers, S., Burghouwt, P., Jansen, J., Bantema, W., & Spruit, M. (2022a). *Risicomanagement en digitale veiligheid bij smart cities – Casus 1: Systeem van intelligente verkeersregelinstallaties*. De Haagse Hogeschool / NHL Stenden Hogeschool (niet openbaar).

Kerpershoek, E., Bartels, A., Burghouwt, P., Jansen, J., Bantema, W., & Spruit, M. (2022). *Risicomanagement en digitale veiligheid bij smart cities – Casus 2: Systeem van slimme camera's voor druktemeting.* De Haagse Hogeschool / NHL Stenden Hogeschool (niet openbaar).

Kleij, R. van der, & Leukfeldt, E.R. (2019). Cyber resilient behavior: Integrating human behavioral models and resilience engineering capabilities into cyber security. In *Proceedings of the International Conference on Applied Human Factors and Ergonomics* (pp. 16–27). Springer.

Lakerveld, J. van, Gussen, I., & Pardon, Y. van (2018). *Visies op de politiefunctie.* PLATO (Universiteit Leiden).

Lakerveld, J.A. van, Gussen, I.W.M., Stoutjesdijk, F.D., Tönis, I.C.M., & Zoete, J. de (2017). *Maatschappelijke ontwikkelingen en hun implicaties voor Gebiedsgebonden politiewerk: Een verkenning.* PLATO (Universiteit Leiden).

Leukfeldt, E.R. (2016) *Cybercriminal networks: Origin, growth and criminal capabilities.* Eleven International Publishers (proefschrift).

Leukfeldt, E.R., & Jansen, J. (2020). Financial cybercrimes and situational crime prevention. In E.R. Leukfeldt en T. Holt (red.), *The human factor of cybercrime* (pp. 216–239). Routledge.

Leukfeldt, E.R., Notté, R.J., & Malsch, M. (2020a). Exploring the needs of victims of cyber-dependent and cyber-enabled crimes. *Victims & Offenders, 15*(1), 60–77.

Leukfeldt, E.R., Spithoven, R., & Misana-ter Huurne, E.F.J. (2020b). De lokale aanpak van cybercrime: Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In C. de Poot, E. Lievens, W.Ph. Stol en L. de Kimpe (red.), *Politie en cybercrime* (pp. 203–222). Gompel&Scavina.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 394–413.

Maddux, J.E., & Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469–479.

Mensvoort, K. van (2019). *Next nature: Waarom technologie onze natuurlijke toekomst is*. Maven Publishing.

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

Michie, S., Atkins, L., & West, R. (2014). *The behaviour change wheel: A guide to designing interventions*. Silverback Publishing.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106–143.

Moody, G.D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285–311.

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. In *Proceedings of the International Conference on Human-Computer Interaction* (pp. 206–216). Springer.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems, 29*(3), 306–321.

Nasir, A., Arshah, R.A., Hamid, M.R.A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12–22.

NCSC (2022). *Nederlandse Cybersecuritystrategie 2022 – 2028: Ambities en acties voor een digitaal veilige samenleving*. Nationaal Cyber Security Centrum.

NCTV (2022). *Cybersecuritybeeld Nederland (CSBN) 2022*. Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Nicholson, J., Coventry, L., & Briggs, P. (2019). "If it's important it will be a headline": Cybersecurity information seeking in older adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems,* (pp. 1–11). ACM.

Notté, R., Slot, L., Hoff-de Goede, S. van, & Leukfeldt, E.R. (2019). *Cybersecurity in het mkb: Nulmeting*. De Haagse Hogeschool.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Petty, R.E., & Cacioppo, J.T. (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (red.), *Advances in experimental social psychology* (pp. 123–205). Academic Press.

Pfleeger, S.L., & Caputo, D.D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*, 597–611.

Pijpers, R., Bomas, E., Dondorp, L., & Ligthart, J. (2020). *Waarden wegen: Een ethisch perspectief op digitalisering in het onderwijs*. Kennisnet.

Politieacademie (2019). *Strategische onderzoeksagenda voor de Politie 2019 – 2022: Voor een effectievere politie en een veiligere samenleving*. Moduli Print.

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*, 371–390.

POR (2020). *Let's get digital! Een solide basis voor een digitaalvaardige politie*. Politieonderwijsraad.

Rae, A., Provan, D., Aboelssaad, H., & Alexander, R. (2020). A manifesto for Reality-based Safety Science. *Safety Science*. doi.org/10.1016/j.ssci.2020.104654

RBPO Noord-Nederland (2023). *Online criminaliteit in Noord-Nederland*. Regionaal Informatie en Expertise Centrum (RIEC) Noord-Nederland.

Redmiles, E.M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R., & Mazurek, M.L. (2020). A comprehensive quality evaluation of security and privacy advice on the web. In *Proceedings of the 29th USENIX Security Symposium* (pp. 89–108). USENIX.

Reeder, R.W., Ion, I., & Consolvo, S. (2017). 152 simple steps to stays safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy 15*(5), 55–64.

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., & Duezguen, R. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. In *Proceedings of the 16th Symposium on Usable Privacy and Security* (pp. 259–284). USENIX.

Renaud, K. (2021). Accessible cyber security: The next frontier? In *Proceedings of the 7th International Conference on Information Systems Security and Privacy* (pp. 9–18). SciTePress.

Renaud, K., Orgeron, C., Warkentin, M., & French, P.E. (2020). Cyber security responsibilization: An evaluation of the intervention approaches adopted by the Five Eyes countries and China. *Public Administration Review, 80*(4), 577–589.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.

Roks, R., & Monshouwer, N. (2020). F-gamers die 'mapsen', 'swipen' en 'bonken': Een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger. *Justitiële Verkenningen, 2*, 44–58.

Rothrock, R.A. (2022). *Digital resilience: Is your company ready for the next cyber attack*. HarperCollins Leadership.

SANS (2022). *SANS 2022 security awareness report: Managing human risk*. Via: https://www.sans.org/blog/sans-2022-security-awareness-report/

Sasse, M.A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122–131.

Sasse, M.A., Hielscher, J., Friedauer, J., & Buckmann, A. (2023). Rebooting IT security awareness: How organisations can encourage and sustain secure behaviours. In *Proceedings of the ESORICS 2022 International Workshops* (pp. 248–265). Springer.

Schaik, P. van, Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior, 78*, 283–297.

Schaik, P. van, Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547–559.

Schaik, P. van, Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *Computers & Security, 90*. doi.org/10.1016/j.cose.2019.101651

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

Schreuders, Z.C., Cockcroft, T.W., Butterfield, E.M., Elliott, J.R., Soobhany, A.R., & Shan-A-Khuda, M. (2018). Needs assessment of cybercrime and digital evidence in a UK police force. Via: https://eprints.leedsbeckett.ac.uk/id/eprint/5076/

Sheeran, P. (2002). Intention-behavior relations: A conceptual and empirical review. *European Review of Social Psychology, 12*(1), 1–36.

Siegrist, M., & Arvai, J. (2020). Risk perception: Reflections on 40 years of research. *Risk Analysis*. doi.org/10.1111/risa.13599

Sloot, B. van der, & Wagensveld, Y. (2022). Deepfakes: Regulatory challenges for the synthetic society. *Computer Law & Security Review, 46*, 1–15.

Smit, P.R., Ghauharali, R., Veen, H.C.J. van der, Willemsen, F., Steur, J., Velde, R.A. te, Vorst, T. van der, & Bongers, F. (2018). *Tasten in het duister: Een verkenning naar bronnen en methoden om de aard en omvang van de criminaliteit te meten (deel 2: Technische rapport)*. WODC.

Snoo, T.-P. de, Wennekes, S., & Smit, A. (2021). De politie een zorg (voor later?)... In G. Meershoek, J. Nap en L. van Spijk (red), *In naam der wat? Reflecties op politie en politiewerk* (pp. 97–106). Boom criminologie.

Spithoven, R., Jansen, J., Drenth, A., & Leukfeldt, E.R. (2022a). Wijk + web: De noodzaak van een lokale aanpak van cybercriminaliteit. *Tijdschrift voor Veiligheid, 21*(3–4), 3–12.

Spithoven, R., Schoonenberg, K., & Land, M. van der (2022). De IVK-handelingscyclus. In R. Spithoven e.a. (red.), *Basisboek integrale veiligheid* (pp. 175-191). Boomcriminologie.

Steden, R. van, Anholt, R., & Koetsier, R. (2021). *De kracht van gebiedsgebonden politiewerk: Een internationale literatuurstudie*. Politie Nederland.

Steen, T. van, & Busser, E. de (2021). *Security by behavioural design: A rapid review*. Universiteit Leiden.

Stol, W.Ph. (2010). *Cybersafety overwogen: Een introductie in twee lezingen*. Boom Juridische Uitgevers.

Stol, W.Ph. (2018). Politiewerk is.... Werken in een digitale samenleving. *Tijdschrift voor de Politie, 80*(5), 22–25.

Stol, W.Ph. (2020). Digitalisering en criminaliteit: Een beknopte inleiding op cybercrime. *Cahier Politiestudies, 3*, 13–22.

Stol, W.Ph. (2021). Digitalisering en de maatschappelijke rol van de politie: Naar politie als 'autoriteit fatsoenlijke rechtshandhaving'. In G. Meershoek, J. Nap en L. van Spijk (red.), *In naam der wat? Reflecties op politie en politiewerk* (pp. 29–38). Boom criminologie.

Stol, W.Ph., & Bantema, W. (2021). *Lokaal bestuur in een digitaliserende samenleving – Essay over een stap in de ontwikkeling: Een handelingskader*. Cybersafety Research Group.

Stol, W.Ph., & Jansen, J. (te verwachten). Politie in een digitaliserende samenleving. In *Politiehandboek*.

Stol, W.Ph., & Strikwerda, L. (2017). *Strafrechtspleging in een digitale samenleving*. Boom Juridisch.

Stol, W.Ph., Leukfeldt, E.R., & Klap, H. (2013). Politie in een digitale samenleving: Stand van zaken anno nu. In W.Ph. Stol en J. Jansen (red.), *Cybercrime en de politie* (pp.63–76). Boom Lemma Uitgevers.

Stol, W.Ph., Treeck, R.J. van, & Ven, A.E.B.M. van der (1999). *Criminaliteit in cyberspace: Een praktijkonderzoek naar aard, ernst en aanpak in Nederland*. Elsevier.

SURF (2022). *Cyberdreigingsbeeld onderwijs en onderzoek 2021–2022*. Via: https://www.surf.nl/files/2022-06/cyberdreigingsbeeld-onderwijs-en-onderzoek-2021-2022-lr.pdf

Terpstra, J., Salet, R., Duijneveldt, I. van, & Havinga, T. (2021). *Gebiedsgebonden politiewerk in ontwikkeling: Onderzoek naar basisteams in een digitale en superdiverse samenleving*. Sdu (Politie en Wetenschap).

Thaler, R.H., & Sunstein, C.R. (2009). *Nudge: Improving decisions about health, wealth and happiness*. Penguin Group.

Toutenhoofd, M.H., Veenstra, S., Domenie, M.M.L., Leukfeldt, E.R., & Stol, W.Ph. (2009). *Politie en cybercrime: Intake en eerste opvolging*. Cybersafety Research Group.

Uchendu, B., Nurse, J.R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security, 109*. doi.org/10.1016/j.cose.2021.102387

Valkengoed, T. van (2017). *Competentieonderzoek cybercrimeopsporing*. Politie Nederland (bachelor scriptie).

Valkengoed, T. van (2021). *Infographic digitaal vaardige politie* (versie 0.31). Politie Nederland (niet openbaar).

Veiga, A. da (2019). Achieving a security culture. In I. Vasileiou en S. Furnell (red.), *Cybersecurity education for awareness and compliance* (pp. 72-100). IGI Global.

Veiga, A. da, & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Computer Security, 31*, 243–256.

Venkatesh, V., Morris, M.G., Davis, G.B., & Davis, F.D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Verbeek, P.-P. (2011). *De grens van de mens: Over techniek, ethiek en de menselijke natuur*. Lemniscaat.

Verweijen, B. (2022). Leren van cyberincidenten: Een meta-analyse van evaluatierapporten ten behoeve van organisatorisch leren. *Tijdschrift voor Veiligheid, 21*(3–4), 89–108.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H.R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576–586.

Vries, H. de, & Henssen, M. (2018). *Podium voor goed politiewerk: Ontwikkelagenda GGP*. Politie Nederland.

Vries, S. de, & Bantema, W. (2022). *Aanpak in kaart: Inzicht in een regionale aanpak van online aangejaagde ordeverstoringen*. Cybersafety Research Group.

Wagen W. van der (2018). *From cybercrime to cyborg crime: An exploration of high-tech cybercrime, offenders and victims through the lens of actor-network theory*. Rijksuniversiteit Groningen (proefschrift).

Wagen, W. van der, Zand-Kurtovic, E.G. van 't, Matthijsse, S.R., & Fischer, T.F.C. (2019). *Cyberdaders – uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin*. Erasmus Universiteit Rotterdam / Universiteit Leiden.

Weijer S.G.A. van de, Leukfeldt, E.R., & Zee, S. van der (2021). Cybercrime reporting behaviors among small- and medium-sized enterprises in the Netherlands. In M. Weulen-Kranenbarg, E.R. Leukfeldt (red.), *Cybercrime in context: Crime and justice in digital society* (pp. 303–325). Springer.

Wiley, A., McCormac, A., & Calic, D (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security, 88*. doi.org/10.1016/j.cose.2019.101640

Winter, B. de (2019). *Door het oog van de naald: Analyse van het beveiligingsincident in Lochem*. Via: https://www.lochem.nl/fileadmin/internet-doc/Bestuur-Organisatie-Nieuws/Nieuws/2019/hack/Duidingsrapportage_Lochem-WHITE.pdf

Winter, B. de (2021). *Te goed van vertrouwen? Duidingsrapportage ransomware-aanval Hof van Twente*. Via: https://www.hofvantwente.nl/fileadmin/files/hofvantwente/inwoners/actueel/Te-goed-van-vertrouwen.pdf

Wittebrood, K., & Braak, R. (2022). *Onderzoeksgedoe: Hoe kan je als wetenschappelijk onderzoeker integer omgaan met complexe druk*. Boom bestuurskunde.

WEF (2022). *The global risks report 2022* (17th edition). Via: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

WEF (2023a). *Global cybersecurity outlook 2023: Insight report*. Via: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

WEF (2023b). *The global risks report 2023* (18th edition). Via: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2023.pdf

Wout, C. van 't (2019). Develop and maintain a cybersecurity organisational culture. In *Proceedings of the 14th International Conference on Cyber Warfare and Security* (pp. 457–466). Stellenbosch University.

WRR (2019). *Voorbereiden op digitale ontwrichting*. Wetenschappelijke Raad voor het Regeringsbeleid.

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407–427.

Yen, H.R., Li, E.Y., & Niehoff, B.P. (2008). Do organizational citizenship behaviors lead to information system success? *Information & Management,* 45(6), 394–402.

Zimmerman, 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.

Zimmerman, V., & Renaud, K. (2021). The nudge puzzle: Matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction, 28*(1). https://doi.org/10.1145/3429888

Digitale weerbaarheid van mens en organisatie

De kracht van verbinding

Dr. Jurjen Jansen is lector Digitale Weerbaarheid van Mens en Organisatie aan NHL Stenden Hogeschool. Het lectoraat is gepositioneerd binnen de Onderzoeksgroep Cybersafety van de Thorbecke Academie. Daarnaast is hij als senior onderzoeker verbonden aan de sector Kennis & Onderzoek van de Politieacademie.