Nu veiligheid er niet meer is

Naar een aanpak van cyberrisico's die *wel* werkt

Lectorale rede

Dr. Rick van der Kleij

8 mei 2025

Centre of Expertise
Veiligheid & Veerkracht
Een initiatief van avans

avans hogeschool

Nu veiligheid er niet meer is

Naar een aanpak van cyberrisico's die *wel* werkt

Dr. Rick van der Kleij
Lectoraat Cyberweerbare Organisaties

Lectorale rede in verkorte vorm uitgesproken bij de publieke aanvaarding van de functie van lector Cyberweerbare Organisaties aan het Centre of Expertise Veiligheid & Veerkracht, Avans Hogeschool op 8 mei 2025

Inhoudsopgave

Hoofdstuk 1

Een groot digitaal dilemma

'Wat zijn de uitdagingen van cybersecurity incidentresponsteams?'

Deze vraag was mijn eerste kennismaking met het cyberdomein in 2017. Ik werkte bij de unit Defensie en Veiligheid van TNO, de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, aan het thema nationale veiligheid. Als psycholoog onderzocht ik het functioneren van teams die werken onder uitdagende omstandigheden. Het was dan ook niet vreemd dat die vraag bij mij en mijn collega's terechtkwam. Het cyberdomein was sterk in opkomst. We besloten om een verkennend onderzoek te doen naar incidentresponsteams in dit opkomende veld.

We huurden een ervaren consultant in van een cybersecuritybedrijf om ons te helpen contacten te leggen met deze teams. Niet veel later stonden we in een kleine kamer met vier computerwerkplekken in een kantoorgebouw in Den Haag. Hier werkte de Informatiebeveiligingsdienst (IBD), een onderdeel van de Vereniging van Nederlandse Gemeenten. De IBD ondersteunt gemeenten bij het verbeteren van hun informatiebeveiliging en helpt hen met incidentrespons. Taken die het kleine team al behoorlijk boven het hoofd begonnen te groeien. We spraken ook met leden van de cybersecurity incidentresponsteams van Defensie, Thales, Northwave en Fox-IT. Dit leverde mijn collega's en mij, naast relevante inzichten en de start van een nieuwe onderzoekslijn, uiteindelijk een mooi artikel op over de behoeften aan ondersteuning van deze teams in het academische tijdschrift *Frontiers in Psychology*.[1]

Al snel na deze verkenning ontdekte ik dat niet alleen de teams die zich beroepsmatig met cybersecurity bezighouden uitdagingen ondervinden. Ook bedrijven ondervinden uitdagingen. Zij staan voor een *groot digitaal dilemma* (zie ook Van Rijsewijk, 2016, p.33). De Nederlandse samenleving is in hoge mate gedigitaliseerd. Volgens recente gegevens van de Wereldbank over 2023 maakt 97% van alle inwoners gebruik van het internet.[2] Digitale processen en technologieën zorgen voor veel gemak. Volgens de jaarlijkse Digital Economy and Society Index (DESI) van de Europese Unie (EU) heeft Nederland zelfs

[1] Van der Kleij, R. Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology*. doi: 10.3389/fpsyg.2017.02179.
[2] https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=NL

een van de beste digitale infrastructuren van Europa (Europese Unie, 2022). Het heeft voordelen om overal met elkaar in verbinding te staan en toegang tot veel informatie te hebben. Bij bedrijven staat digitalisering dan ook hoog op de agenda. En daar waar ik het heb over bedrijven in deze rede, kunt u natuurlijk ook denken aan organisaties, instellingen, instanties of individuen. Maar zoals we nu weten, opende digitalisering tegelijk nieuwe 'deuren' voor cybercriminelen. Digitalisering vergroot ook de kwetsbaarheid van bedrijven.

Een effectieve verdediging tegen een veelheid aan potentiële cyberdreigingen zou vereisen dat bedrijven geen toegang meer tot het internet hebben. Dit isoleren van systemen biedt bescherming tegen allerlei cyberdreigingen, vooral in omgevingen waar de beveiliging van cruciaal belang is, zoals militaire netwerken en medische apparatuur. Voor de meeste bedrijven is een evenwicht tussen beveiliging en functionaliteit echter noodzakelijk. Hierbij is connectiviteit, en dus het internet, onmisbaar. Ziehier het dilemma dat veel bedrijven onder ogen moeten komen. Hoe vind je als ondernemer een goede balans? Want je wilt als ondernemer gebruik kunnen maken van de digitale infrastructuur die Nederland rijk is, zonder je bedrijf helemaal op slot te moeten zetten.

Dit groot digitaal dilemma gaat niet vanzelf weg. De dreigingen nemen alleen maar toe, met kans op grote schade, zelfs met faillissement tot gevolg. Dreigingen zijn bovendien steeds minder voorspelbaar. De klassieke aanpak van cyberrisico's (hierna: cybersecurity) vereist dat risico's kunnen worden geïdentificeerd *ex ante*. Maar door de snelle ontwikkelingen in het dreigingslandschap ontstaan telkens nieuwe dreigingen die op voorhand niet kunnen worden voorzien of zelfs niet kunnen worden voorkomen. Cybersecurity legt de focus op veiligheid. Deze aanpak richt zich op het versterken van kwetsbare onderdelen van het bedrijf om voorspelbare dreigingen te kunnen weerstaan. Een aanpak die vaak de metafoor oproept van een kasteel met hoge muren en diepe slotgrachten: een ondoordringbare barrière tegen externe aanvallen. Maar bovenal een aanpak van cyberrisico's die niet langer voldoet, want het aantal incidenten en de impact ervan neemt alleen maar toe.

Het idee dat bedrijven weerbaar moeten zijn als reactie op cyberrisico's is de afgelopen jaren opgekomen en populair geworden. We noemen deze nieuwe kijk op de aanpak van cyberrisico's ook wel cyberweerbaarheid.

Het managen van cyberweerbaarheid omvat niet alleen een aanpak gericht op het voorkomen van schade. Het omvat ook het vermogen om onverwachte, positieve mogelijkheden te benutten om de veiligheid te verbeteren en te kunnen reageren op, te herstellen van, en zich aan te passen aan ongunstige gebeurtenissen of activiteiten. Het is een dynamischer concept dan cybersecurity, omdat het erkent dat absolute veiligheid niet haalbaar is, vandaar de titel van deze rede: *Nu veiligheid er niet meer is*. Bedrijven moeten dus handelen vanuit de aanname dat er aanzienlijke cyberincidenten zullen plaatsvinden op regelmatige basis.

Maar hoe helpt dit idee de bedrijven met hun dilemma? Cyberweerbaarheid is een complex begrip dat lastig te implementeren is. De uitdaging is hoe je als organisatie open en verbonden kan zijn, gebruik kan maken van de kansen die digitalisering brengt, en tegelijkertijd kan vertrouwen op het vermogen om weerbaar te zijn tegen cyberrisico's (Van Rijsewijk, 2016). Dit idee is niet geheel nieuw, maar het vereist een andere kijk op veiligheid. Een doorbraak naar een nieuw paradigma is nodig. Het is tijd voor een aanpak van cyberrisico's die *wel* werkt.

Dat dit idee niet nieuw is, wil niet zeggen dat we alles al weten. Ik geef in deze rede dan ook geen blauwdruk voor cyberweerbaarheid. Op veel vragen over weerbaarheid weten we het antwoord gewoonweg nog niet, omdat het onderzoek ernaar nog in de kinderschoenen staat. Mijn taak als lector is om op zoek te gaan naar de antwoorden door praktijkgericht onderzoek. Dit zorgt voor oplossingen die direct toepasbaar zijn en aansluiten bij de behoeften van de praktijk. Praktijkgericht onderzoek is naar mijn mening dan ook doorlopend nodig. Zo creëren we een situatie waar bedrijven voldoende geïnformeerd zijn om de juiste besluiten te kunnen nemen over het toepassen van de laatste stand van kennis over cyberweerbaarheid in hun bedrijfspraktijken.

Hoofdstuk 2

Het belang van cyberweerbaarheid

De veiligheidssituatie in Europa

In de ons land goed gezinde internationale context was weerbaarheid geen zorg meer, zo valt te lezen in een recent rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR, 2024, p. 14). Sinds het einde van de Koude Oorlog inde Nederland het vredesdividend en bezuinigde fors op veiligheid. Die tijd is voorbij. Veel Nederlanders hebben echter nog niet of nauwelijks een voorstelling van de fundamentele veranderingen die mondiaal gaande zijn. Ze zijn er niet van doordrongen dat vitale publieke voorzieningen, onze levensstandaard en mogelijk zelfs onze vrijheid daadwerkelijk op het spel komen te staan (WRR, 2024).

De veiligheidssituatie in Europa is in rap tempo drastisch verslechterd. Door geopolitieke spanningen en verschuivende internationale machtsverhoudingen neemt ook de dreiging tegen Nederland toe.[3] Het gaat dan vooral om de oorlog tegen Oekraïne, de strijd tussen Israël en Hamas en de rol van China op het wereldtoneel (Nationaal Coördinator Terrorismebestrijding en Veiligheid [NCTV], 2024a). Nederland kan weer in oorlog raken. Lang leek dat ondenkbaar, maar door de rivaliteit tussen de grootmachten is dat een scenario dat ook ons land nu serieus moet nemen. Zelfs NAVO-baas Rutte vindt het tijd om ons geestelijk voor te bereiden op oorlog.[4] De fragmentatie van tonelen van machtsuitoefening maakt bovendien dat oorlog allerlei vormen kan aannemen. Zelfs nu al zijn er dagelijks talloze pogingen tot inbraak in de digitale systemen van bedrijven en overheden (WRR, 2024).

Zowel statelijke actoren als criminelen hebben het op onze digitale infrastructuur en onze gegevens gemunt, zo valt te lezen in de *Veiligheidsstrategie voor het Koninkrijk der Nederlanden* (NCTV, 2023b). De kans op cyberincidenten neemt toe.[5] Wat precies door mag gaan als een cyberincident verschilt voor elk bedrijf. Maar over het algemeen is iets een cyberincident als

[3] https://www.dutchitchannel.nl/news/511906/rijksoverheid-waarschuwt-bugers-zich-voor-te-bereiden-op-cyberaanval
[4] https://nos.nl/artikel/2548057-navo-baas-rutte-tijd-om-ons-geestelijk-voor-te-bereiden-op-oorlog
[5] Zie ook het AIVD dreigingsbeeld 2023 en het Cybersecuritybeeld (CSBN) 2023 van de NCTV.

dit bedrijfsprocessen, financiën of reputatie ernstige schade kan toebrengen (World Economic Forum [WEF], 2024, p. 5). Dit kan variëren van een hack (digitale inbraak) en gijzelsoftware tot een datalek en een softwarefout. Omdat de kans op cyberincidenten toeneemt, vraagt een goede aanpak ervan maximale aandacht van bedrijven. Toch lijkt het gevoel van urgentie bij veel bedrijven nog te ontbreken (Krauwer, 2024).

Niet alleen de kans op cyberincidenten neemt toe. Bedrijven worden daadwerkelijk voortdurend aangevallen. Soms zelfs zonder dat ze het zelf in de gaten hebben. Vaak gaat het om cybercriminelen die snel en makkelijk geld willen verdienen. Of om scholieren die cyberaanvallen doen voor de lol. Maar we hebben ook te maken met voorbereidingshandelingen voor sabotage, spionage en ongewenste beïnvloeding door andere landen. Denk aan de bemoeienis van Russische schepen met onderzeese infrastructuur in de Noordzee.[6] Een zogenaamde statelijke dreigingsactor kan enorm veel schade aanrichten door een operationeel proces te verstoren of door data te stelen, te veranderen of te wissen. We zijn echter niet klaar voor wat er de komende vier of vijf jaar op ons afkomt, aldus Rutte in zijn eerste grote toespraak als secretaris-generaal van de NAVO.[7] *Onze aanpak schiet te kort.*

Slachtofferschap cybercrime

Volgens de Volkskrant zijn in 2021, 735 duizend fietsen gestolen (Eshuis, 2022). Dat lijkt veel, maar in datzelfde jaar waren volgens het Centraal Bureau voor de Statistiek (CBS), bijna 2,5 miljoen Nederlanders, naar eigen zeggen, slachtoffer van online criminaliteit (Akkermans, Kloosterman, Moons, Reep, Tummers-Van der Aa, 2022). En dat aantal zit al jaren in de lift. Recente cijfers van het CBS (Akkermans, Derksen, Kennis, Kloosterman, & Moons, 2024) laten zien dat in 2023, 16% van de Nederlanders van vijftien jaar en ouder slachtoffer is geweest van een of meerdere vormen van online criminaliteit; een aandeel dat iets lager ligt dan in 2021 (17%), maar hoger ligt dan in 2017 (11%) en 2012 (12%). Uit het *Fenomeenbeeld 2024* van de Eenheid Landelijke Opsporing en Interventies & de Eenheid Landelijke Expertise en Operaties (2024) blijkt dat de politie in 2023, 70.000 meldingen en aangiften van online criminaliteit kreeg. Het totale schadebedrag bedroeg 109 miljoen euro.

[6] https://www.techzine.nl/nieuws/infrastructure/559051/russisch-spionageschip-ook-boven-da-takabel-in-noordzee-actief/
[7] https://nos.nl/artikel/2548057-navo-baas-rutte-tijd-om-ons-geestelijk-voor-te-bereiden-op-oorlog

Nederlanders werden volgens het CBS in 2023 het vaakst slachtoffer van online oplichting en fraude (9%). Denk hierbij aan aankoopfraude via handelsplaatsen zoals Marktplaats, waarbij online gekochte producten niet werden geleverd, terwijl ze wel vooruitbetaald waren. Ook hacking (6%) en online bedreiging en intimidatie (3%) kwamen vaak voor. Bij hacking breekt iemand met kwade bedoelingen zonder toestemming in op een apparaat (zoals een computer of tablet) of een account (zoals een e-mail- of bankaccount) (Akkermans, Derksen, Kennis, Kloosterman, & Moons, 2024).

Jongeren tussen de 15 en de 25 zijn ongeveer anderhalf keer zo vaak slachtoffer van online criminaliteit in vergelijking met andere leeftijdsgroepen (CBS, 2023). Het verschil is het grootst bij online bedreiging en intimidatie en bij hacken. Een op de vijf (21%) van de slachtoffers van online criminaliteit geeft aan dat het online delict heeft geleid tot emotionele, psychische of financiële problemen. Van alle slachtoffers van online criminaliteit heeft bijna de helft (46%) bij een instantie, zoals de fraudehelpdesk - een instantie die slachtoffers adviseert en naar de juiste instantie verwijst - gemeld wat hen is overkomen; 17% heeft aangifte gedaan bij de politie (CBS, 2023).

Hierbij moet worden opgemerkt dat het CBS lang niet alle vormen van online criminaliteit meet. Bovendien laten cijfers op basis van zelfrapportage een onvolledig beeld zien, omdat mensen niet altijd weten dat ze slachtoffer zijn, zoals bij diefstal van persoonsgegevens. Deze niet-geregistreerde criminaliteit staat in de criminologie ook wel bekend onder de term ‘dark number’.
Ook kunnen respondenten zich niet altijd herkennen in het label ‘slachtoffer’, omdat dit voor hen een te negatieve lading heeft. Er kan worden geconcludeerd dat slachtofferschap van online criminaliteit in werkelijkheid hoger is dan de cijfers laten zien (Cyberweerbaar NL, 2024). Nederland is dus niet langer het land van traditionele criminaliteit, zoals fietsendiefstal (zie figuur 1), maar het land van cybercriminaliteit, zoals hacken en online oplichting (zie ook Ruiter, Van Leuken, Van Ruitenburg, Schiks, & Leukfeldt, 2023).

Figuur 1. Gestolen fiets (*bron: Wikimedia Commons; beeld: Functioning-MemberOfSociety*).

Slachtofferschap onder bedrijven

Ook bedrijven lijden elke dag onder cyberaanvallen. Niet zo lang geleden, in 2017, lagen twee containerterminals in de Rotterdamse haven weken stil als gevolg van een gijzelsoftware-aanval bij logistiek concern Maersk. In 2019 kwam de Universiteit Maastricht volledig stil te liggen als gevolg van een digitale gijzeling.[8] In 2020 konden medewerkers van de gemeente Hof van Twente niet meer bij hun gegevens na een aanval met gijzelsoftware.[9] In 2021 vond de zogenaamde kaashack plaats. Door een gijzelsoftware-aanval bij Bakker Logistiek kon er dagenlang minder voedsel aan retailers geleverd worden en raakten kaasschappen leeg.[10] En onlangs was schoolboekenverkoper Iddink slachtoffer van een cyberaanval waarbij de data in de systemen werd gestolen en versleuteld met gijzelsoftware. Voor al deze gevallen gold dat het soms weken duurde voor de problemen opgelost waren.

[8] https://www.maastrichtuniversity.nl/nl/cyberaanval-een-samenvatting
[9] https://vng.nl/sites/default/files/2021-04/20210401-bestuurlijke-lessen-uit-de-hack-bij-hof-van-twente.pdf
[10] https://nos.nl/artikel/2376425-kaas-hack-opgelost-ging-om-gijzelsoftware

Elk jaar krijgt volgens het CBS (2023) ongeveer een op de vijf bedrijven te maken met een cyberincident.[11] Een cyberincident komt het vaakst voor bij middelgrote en grote bedrijven met honderd medewerkers of meer. Daarvan heeft volgens het CBS ongeveer een op de vijftien te maken met een aanval van buitenaf, ofwel een aanval die afkomstig is van een externe bron of partij. Deze incidenten kunnen de bedrijfsvoering ernstig verstoren. Onderzoek onder de Nederlandse bedrijvenpopulatie, exclusief zelfstandigen, laat zien dat in 2023 de primaire bedrijfsprocessen bij een op de vijftien bedrijven al eens stil hebben gelegen als gevolg van een cyberincident (De Jong, Koeman, Konijn, Volberda, & Hollen, 2023). Schattingen wijzen uit dat 60% van de mkb-bedrijven die slachtoffer worden van een cyberaanval binnen zes maanden hun deuren moeten sluiten (Leigh, 2023). Zo vroeg onlangs nog Wodkaproducent Stoli faillissement aan in de Verenigde Staten, mede vanwege een ransomware-aanval.[12] Opmerkelijk is dat er ook bedrijven zijn die niet weten of ze te maken hebben gehad met een cyberincident. Recent onderzoek laat zien dat 6% van alle IT-verantwoordelijken binnen een bedrijf met een omvang tot 400 medewerkers niet weet of het bedrijf een cyberincident heeft doorgemaakt in de afgelopen twaalf maanden (Hof, Van der Kleij, & Mergler, 2024).

Onderzoek dat ABN AMRO samen met onderzoeksbureau MWM2 onder 895 organisaties heeft verricht, laat een nog 'zwarter' beeld zien van slachtofferschap onder bedrijven (Krauwer, 2024).[13] Uit dat onderzoek blijkt dat in 2023 bijna driekwart van de Nederlandse bedrijven te maken had met een cyberaanval.[14] Maar liefst 86% van het grootbedrijf – met een jaaromzet van minimaal 25 miljoen euro – was doelwit van cyberaanvallen. Bij middelgrote en kleine bedrijven gold dit voor 71% en onder zelfstandigen was dit 55%. Dat is een forse stijging ten opzichte van vorige jaren. Waar het percentage getroffen bedrijven in 2021 29% was, steeg dat in 2022 naar 45%.[15]

[11] Het CBS onderscheidt voor incidenten drie varianten: uitval van een ICT-systeem, data-vernietiging (vernietiging of verminking van elektronische gegevens) en dataonthulling (onthulling van vertrouwelijke elektronische gegevens).
[12] https://www.security.nl/posting/867828/Wodkaproducent+Stoli+vraagt+mede+wegens+ransomware+faillissement+aan+in+VS
[13] https://itchannelpro.nl/abn-amro-verfijndere-cyberaanvallen-zijn-geen-wake-up-call/#:~:text=-Maar%20liefst%2086%20procent%20van%20het
[14] Dit betrof cybercriminaliteit in de brede zin, inclusief phishing, malware, datalekken, ransomware, DDoS-aanval, fraude door medewerker en CEO-fraude.
[15] https://www.abnamro.nl/nl/zakelijk/insights/cybersecurity/cyberaanval/aantal-bedrijven-getroffen-door-cyberaanval-gestegen-tot-45procent.html

Het feit dat het aantal cyberaanvallen met 57% is toegenomen sinds 2021, heeft volgens ABN AMRO met twee zaken te maken. Allereerst ontstaat er door de toenemende digitalisering een groter aanvalsoppervlak voor cybercriminelen. Met aanvalsoppervlak wordt gedoeld op manieren waarop een dreigingsactor digitale processen kan aanvallen (NCTV, 2024a, p. 45). Dit betekent dat het gemak voor cybercriminelen toeneemt om een aanval uit te voeren. Een andere verklaring is de professionalisering van cybercriminelen. De trend dat het onderzoek van ABN AMRO schetst, wordt door andere bronnen bevestigd. Zo registreerde de Nederlandse politie in 2021 zo'n 14 duizend gevallen van cybercriminaliteit, een toename van een derde in vergelijking met 2020 en een verdriedubbeling in vergelijking met 2019.[16]

Ongeveer de helft van alle cyberincidenten leidt tot kosten voor bedrijven. Een recent voorbeeld speelde zich af in Hong Kong. Daar werd een financieel medewerker overtuigd om 25,6 miljoen dollar over te schrijven naar online fraudeurs, via een videocall waarin de werknemer in een vergadering dacht te zitten met verschillende collega's. De video bleek op basis van AI in elkaar te zijn gezet en de collega's waren nep.[17] Volgens een recent onderzoek door het Ponemon Institute in opdracht van IBM (2024) zijn de gemiddelde kosten van een datalek in 2024 alleen al $4,88 miljoen. Dit zijn kosten voor onder andere het niet operationeel zijn, apparatuurschade, boetes, reputatieschade, het bemensen van een helpdesk om gedupeerde klanten te woord te kunnen staan en omzetverlies. In Nederland bedroegen de mediane kosten door cyberaanvallen[18] in 2023 zo'n $21 duizend per bedrijf, zo rapporteert verzekeraar Hiscox (2023). IT-beveiliger ESET Nederland schat de kosten van een cyberincident in 2022 bij een mkb-bedrijf in Nederland gemiddeld echter op zo'n €270 duizend, een halve ton meer dan het wereldwijde gemiddelde (Lucas, 2022). Een recente ontwikkeling is bovendien dat cyberincidenten steeds schadelijker worden voor organisaties (Allianz, 2024). Met de voortdurende digitalisering van onze samenleving wordt verwacht dat de jaarlijkse kosten van cyberincidenten de komende jaren blijven toenemen. Deze verwachting wordt onderbouwd door de resultaten van de studie van Ponemon Institute die een stijging laten zien van meer dan 15% in gemiddelde kosten in 2024 ten opzichte van 2020 (IBM, 2024).

[16] Het aantal geregistreerde gevallen van cybercrime is in 2022 licht gedaald ten opzichte van 2021. De politie registreerde in 2022 13.949 incidenten. Dat is een afname van 2 procent in vergelijking met 2021. Toen betrof het 14.166 aangiftes. Zie ook: https://www.politie.nl/nieuws/2023/januari/19/politie-registreert-minder-cybercrime.html

[17] https://www.techzine.nl/blogs/security/549695/fraude-met-deepfakes-hoe-kan-een-organisatie-zich-beschermen/#:~:text=Een%20recenter%20voorbeeld%20daarvan%20speelde,te%20zitten%20met%20verschillende%20collega%27s.

[18] Het is onduidelijk wat Hiscox verstaat onder een cyberaanval en hoe dat is uitgevraagd.

Ondanks het hoge dreigingsniveau blijft de risicoperceptie in het Nederlandse bedrijfsleven achter volgens ABN AMRO en MWM2.[19] Ondernemers lijken de risico's pas te onderkennen als een aanval tot schade leidt, zoals in de vorm van kosten voor herstel van systemen, gederfde inkomsten door stilstand van het bedrijf of reputatieschade door gelekte klantgegevens. Inmiddels hebben aanvallen al bij 59% van het grootbedrijf en 43% van het midden- en kleinbedrijf (hierna: mkb) tot dergelijke schade geleid. Percentages die overeenkomen met de resultaten uit de *Cybersecuritymonitor* van het CBS (2023). Het aantal mkb-bedrijven en zelfstandigen dat cybercriminaliteit als 'hoog' of 'heel erg hoog' risico beschouwt, is ondertussen echter afgenomen. Daar komt bij dat bijna één op de vijf bedrijven naar eigen zeggen onvoldoende voorbereid is op deze dreiging (De Jong, Koeman, Konijn, Volberda, & Hollen, 2023). Een zorgwekkende ontwikkeling als je het mij vraagt, waar in de onderliggende onderzoeken geen verklaring voor wordt gegeven.

Minder cyberweerbaar dan we denken

In een bijdrage voor de rubriek *Opinie* van BN DeStem mocht ik op 14 september 2024 uiteenzetten dat de cyberweerbaarheid van Nederland op dit moment veel minder groot is dan we denken (Van der Kleij, 2024).[20] Als land zijn we onvoldoende voorbereid op cybercrises. Om echt goed voorbereid te zijn, moeten we onze software, hardware en infrastructuur zelf kunnen fiksen als het mis gaat. En of we dit kunnen is nog maar de vraag. Als we de kranten mogen geloven dan hebben we onszelf te afhankelijk gemaakt van buitenlandse partijen.[21] De software die we elke dag gebruiken, draait op de cloudservers van Amerikaanse bedrijven. Onze hardware is vaak afkomstig van bedrijven uit Azië. Op dit moment is dat geen probleem. Als we hulp nodig hebben, springen deze bedrijven graag bij. Maar kunnen we ook op ze bouwen als het echt mis gaat? Want het is volgens Defensie niet ondenkbeeldig dat een lidstaat van de NAVO wordt aangevallen door Rusland.[22]

---

[19] De *Nederlandse innovatie monitor* schets een vergelijkbaar beeld. Bijna de helft van de bedrijven (44%) meent dat cybercriminaliteit een sterk groeiende dreiging vormt in hun sector. Bijna een op de vijf bedrijven is naar eigen zeggen onvoldoende voorbereid op deze dreiging (De Jong, Koeman, Konijn, Volberda, & Hollen, 2023).

[20] Zie ook: Henk Strikkers (2024, 10 september). 'Misschien is er wel een grote ramp nodig om belang in te zien van cyberveiligheid.' Interview met cyberveiligheid-expert Rick van der Kleij. *BN DeStem*.

[21] https://www.nu.nl/tech/6133272/nederland-zou-te-afhankelijk-van-buitenlandse-techbedrijven-worden.html

[22] https://www.gld.nl/nieuws/8122468/oorlogsdreiging-is-reeel-en-dat-moeten-we-ons-realiseren-zegt-nieuwe-generaal

Ook de kennis en de vaardigheden ontbreken die nodig zijn om snel te kunnen herstellen na een incident. Kennis verdwijnt uit Nederland, omdat belangrijke bedrijven weggekocht worden door buitenlandse partijen.[23] Door jarenlange uitbesteding aan buitenlandse bedrijven kunnen we zelf bovendien steeds minder. Mensen die glasvezel kunnen lassen bijvoorbeeld, zijn schaars (figuur 2). Het is nu eenmaal goedkoper om die expertise uit het buitenland te halen. Maar kunnen we ook op die mensen rekenen als onze glasvezelverbindingen beschadigd raken in een oorlogssituatie?

Figuur 2. Lassen van glasvezel (*bron: CTNED.nl; beeld: Peter Timmer Fotografie, www.petertimmerfotografie.nl*).

Niet wachten op een digitale ramp

Soms heb je een ramp nodig om voor hervormingen te zorgen binnen een sector. Na de Watersnoodramp van 1953 ontstond een omslag in het denken in Nederland over waterveiligheid (Vergouwe, 2014). We gingen aan de slag met de Deltawerken en er kwamen strengere veiligheidsnormen voor primaire waterkeringen (zie figuur 3).[24]

[23] https://www.rijksoverheid.nl/documenten/rapporten/2023/04/06/de-economische-kansen-van-de-cybersecuritysector

[24] https://www.rijkswaterstaat.nl/water/waterbeheer/bescherming-tegen-het-water/watersnoodramp-1953

Gegeven het huidige risicobeeld heeft de Nederlandse samenleving dringend een wake-up call nodig die niet alleen leidt tot meer bewustwording, maar ook bedrijven en burgers middelen biedt om weerbaarder te worden, aldus de WRR (2024). De overheid bereidt zich al voor, maar verwacht ook in toenemende mate van inwoners (en bedrijven) dat ze zich beter gaan voorbereiden op de gevolgen van een mogelijke ramp of incident.[25] Op de website *Denk vooruit* worden concrete handelingsperspectieven voor inwoners geboden om zich voor te bereiden op een crisis of ramp.[26]

De eerste voorproefjes van een digitale ramp hebben we als samenleving al gehad. Een grote storing aan het zogenoemde 'Netherlands armed forces integrated network' (Nafin) leidde in augustus 2024 tot grote problemen, onder meer op Eindhoven Airport en bij de hulpdiensten.[27] Een wereldwijde computerstoring van Microsoftsystemen in juli van dat jaar, veroorzaakt door een foutieve configuratie-update van de software van cyberbeveiligingsbedrijf CrowdStrike, legde onder andere Schiphol plat. Voor deze cyberincidenten, als gevolg van niet-moedwillig handelen, gold dat de problemen gelukkig snel opgelost waren. Maar wat als we daadwerkelijk worden aangevallen door een statelijke dreigingsactor?

Niemand zit te wachten op een digitale ramp. Om te zorgen dat we digitaal droge voeten houden, moeten we op tijd in actie komen. Een proactieve houding is nodig, oftewel uitvoeringskracht, waarbij problemen niet alleen worden gesignaleerd, maar ook actief oplossingen worden gezocht en uitgeprobeerd. Intussen zitten ook cybercriminelen niet stil. De dreiging neemt constant toe onder invloed van nieuwe technologische ontwikkelingen zoals generatieve artificiële intelligentie (hierna: GenAI). GenAI is een specifieke vorm van kunstmatige intelligentie die nieuwe inhoud kan genereren, zoals tekst, beeld, broncode en meer (AIVD & RDI, 2024). Een voorbeeld hiervan is een chatbot zoals ChatGPT van OpenAI. Cybercriminelen kunnen GenAI inzetten om geavanceerde malware te ontwikkelen of zeer overtuigende phishing-e-mails te creëren. We kunnen wel stellen dat cybercriminelen met de komst van GenAI superkrachten hebben gekregen. De druk om te innoveren ligt dus hoog.

[25] Informatie over hedendaagse dreigingen is gebundeld in het nieuwe webdossier 'Dreiging in Nederland' op de website van de Rijksoverheid.
[26] https://www.denkvooruit.nl/
[27] Het Nafin is een eigen, zwaarbeveiligd glasvezelnetwerk van het Nederlands Ministerie van Defensie.

Figuur 3. Deltawerken: Oosterscheldekering (*bron: Wikimedia Commons; beeld: Vladimír Šiman*).

Balans is de sleutel tot innovatiesucces

Oplossingen in het cyberdomein worden traditioneel gezocht in de technologische hoek. Een technische benadering van innovatie is leidend. Deze benadering is gebaseerd op het idee dat technologische oplossingen leiden tot meer veiligheid. Maar is dat ook zo? Technologische oplossingen kunnen zeker oplossingen bieden voor het groot digitaal dilemma. Nieuwe en bestaande, maar onderbenutte technologische maatregelen, bieden kansen om de cyberweerbaarheid te verhogen (Van Boheemen, Munnichs, Kool, Diercks, Hamer & Vos, 2020). Denk aan het gebruik van de principes van de kwantummechanica om de overdracht van gegevens te beveiligen. Technologie ontwikkelt zich momenteel echter veel sneller dan de bedrijven aan kunnen.[28] Er lijkt sprake van een steeds groter wordende kloof tussen wat ontwikkelaars aanbieden en de vaardigheden van bedrijven om de technologie goed in te zetten.

[28] https://made-in-europe.nu/2019/04/industrie-houdt-tempo-technologische-innovatie-niet-meer-bij/

Het tempo van de technologische vooruitgang ligt dus hoger dan het vermogen van de meeste bedrijven om nieuwe technologische oplossingen te begrijpen, te implementeren en te maximaliseren in termen van operationele voordelen. Het succes van innovaties wordt daardoor steeds afhankelijker van de manier waarop mensen, bedrijven, organisaties en instellingen omgaan met innovaties (ABI Research, 2019).

Naast en in samenhang met technologische innovatie is daarom dus ook sociale innovatie nodig om de technologische innovatie beter te kunnen benutten en om het innovatief vermogen van organisaties in reactie op de toenemende dreiging te vergroten (Pot, 2009; 2012). Volgens Pot (2009) is sociale innovatie het vernieuwen van de arbeidsorganisatie en het maximaal benutten van competenties, gericht op het verbeteren van de bedrijfsprestaties. In de context van cybersecurity wil ik sociale innovatie definiëren als:

'Het ontwikkelen en implementeren van nieuwe strategieën, processen en samenwerkingsvormen die gericht zijn op het benutten van technische cybersecurity oplossingen door optimaal gebruik te maken van menselijke en organisatorische capaciteiten.'

Technische en sociale innovatie zijn dus onlosmakelijk met elkaar verbonden.[29] Sociale innovatie is cruciaal om meer rendement te halen uit technische innovaties. Alleen door de juiste balans te vinden bereiken we innovatiesucces. *Om te innoveren hebben we mensen nodig die op hun beurt de juiste processen hebben gedefinieerd.* Techniek is maar een onderdeel van innovatiesucces.

[29] https://www.sol-online.nl/nieuws/technische-innovatie-is-niet-succesvol-zonder-sociale-innovatie-food-in-transitie-2030/#:~:text=Sociale%20innovatie%20zorgt%20ervoor%20dat,beschikken%20over%20voldoende%20sociale%20innovatiekracht.

De gouden driehoek

Een goede strategie om de digitale dreigingen aan te pakken zou zich dus moeten richten op innovatie in elk van de drie pijlers: mens, proces en technologie (zie ook: Assibi, 2023). Dit is in mijn ogen een belangrijk inzicht. Ik ga er hieronder wat dieper op in. Deze drie pijlers zijn oorspronkelijk afgeleid van het Diamond-model van Leavitt (1964). Dit model illustreert de relaties tussen vier afhankelijke onderdelen binnen organisaties: taken, mensen, structuur en technologie.[30]

- **Taken:** De routinematige en kritische activiteiten die een organisatie moet uitvoeren.
- **Mensen:** De mensen in een organisatie en de eigenschappen of attitudes die binnen deze mensen moeten worden bevorderd om succesvol te zijn.
- **Structuur:** de organisatiestructuur stelt mensen in staat verantwoordelijkheden te verdelen en efficiënt samen te werken.
- **Technologie:** De apparatuur die het vermogen van een organisatie om haar noodzakelijke functies uit te voeren mogelijk maakt en ondersteunt.

Het model stelt dat veranderingen in één component waarschijnlijk de andere drie zullen beïnvloeden. Om verandering succesvol te laten zijn, moet men dus de impact op alle vier de gebieden evalueren en beheren.[31] Uiteindelijk werden structuur en taken gecombineerd tot processen, waardoor de 'diamant' veranderde in de zogenaamde 'gouden' driehoek met de componenten die tegenwoordig het meest worden gebruikt, ook in het cyberdomein: mens, proces en technologie. Als een component verschuift, moeten de andere twee ook verschuiven om een effectief evenwicht te behouden naarmate de verandering vordert (zie figuur 4).

[30] https://whatfix.com/blog/people-process-technology-framework/
[31] https://www.forbes.com/councils/forbestechcouncil/2022/12/29/is-the-60-year-old-people-process-technology-framework-still-useful/

Figuur 4. Diamond-model (links) en de gouden driehoek (rechts) (*bron: Simon, 2019*).

In de jaren negentig maakte computerbeveiligings- en privacyspecialist Bruce Schneier de gouden driehoek populair binnen het cyberdomein. Hij probeerde hiermee onder de aandacht te brengen dat er naast aandacht voor IT, aandacht moest zijn voor mens en processen in het algemene systeem. De term 'systeem' verwijst in deze context naar een geïntegreerd geheel van hardware, software, netwerken, gegevens, processen en mensen die gezamenlijk werken om essentiële functies en diensten te leveren. Het idee is dat firewalls, virusscanners, proxyservers, enz. (technologie) weinig voorstellen als je ze niet op de juiste manier gebruikt (proces) en het juiste team hebt om ze te gebruiken (mens).

Een veelvoorkomend probleem is dat bedrijven een 'vinkje zetten'-aanpak hanteren voor beveiliging, waarbij ze investeren in specifieke technologie om te voldoen aan verplichtingen die de geldende wet- en regelgeving ze oplegt (compliant te zijn), zonder de juiste mensen of processen in te zetten om optimaal gebruik te maken van die technologie en het systeem echt te beveiligen.[32] Een belangrijk punt dat ik wil maken in deze rede is daarom dat we naast een technologisch perspectief ook een niet-technologisch perspectief bezien als we kijken naar vraagstukken op het gebied van cyberweerbaarheid. En dus de inbreng van alfa- en gammawetenschappen beschouwen.

[32] Dat neemt niet weg dat bij mensen geen uitdagingen liggen. Want hoe kan het toch dat steeds meer mensen zich zorgen maken over veiligheid, maar nog lang niet iedereen maatregelen neemt? Denk hierbij bijvoorbeeld aan ondernemers die bewust ervoor kiezen om geen maatregelen te nemen om hun digitale veiligheid te versterken (zie ook Deloitte, 2024, p.13).

Ik durf met stelligheid te beweren dat het maatschappelijke probleem van cyberweerbaarheid niet op te lossen is zonder de inbreng van alfa- en gammavakken als psychologie, rechten en economie (zie ook Adviesraad voor het Wetenschaps- en Technologiebeleid, 2007). Dit belang wordt benadrukt in onderstaande quote:

> ***'We've had too many computer scientists looking at cybersecurity, and not enough psychologists, economists and human-factors people'***, aldus Douglas Maughan, hoofd van de cybersecurity onderzoeksafdeling van het U.S. department of Homeland Security (Waldrop, 2016).

Daar komt bij dat diverse factoren cybersecurity beïnvloeden en compliceren (NCTV, 2024a). Ook ontwikkelingen die ogenschijnlijk niets met cybersecurity van doen hebben, kunnen blijvend van invloed zijn op de digitale dreiging. Dat geldt bijvoorbeeld voor de eerdergenoemde geopolitieke situatie, arbeidsmarktontwikkelingen, maar ook voor technologische ontwikkelingen. Zo vormt een toekomstige kwantumcomputer niet alleen een kans, maar tevens een digitaal risico van jewelste. Versleutelde data die nu onderschept en opgeslagen wordt, kan mogelijk op een later moment worden 'ontsleuteld' met een kwantumcomputer. Een cyberincident bij een organisatie kan bovendien doorwerken naar vele andere organisaties, zoals de foutieve software-update van CrowdStrike en de softwarefout op het glasvezelnetwerk van Defensie demonstreerden (NCTV, 2024a). We spreken dan over een cyberincident in de toeleveringsketen of een cyber cascade-effect.[33]

Vrij van zorgen over cyberrisico's

Wat we ook doen, alles begint met het creëren van een gevoel van urgentie. Bouwen aan een cyberweerbaar Nederland is niet alleen een taak van de staat. Het is een verantwoordelijkheid die we samen moeten dragen en samen moeten voelen. De overheid bereidt zich goed voor, maar er wordt steeds meer verwacht van de samenleving. Iedereen moet zijn cyberweerbaarheid vergroten: overheden, bedrijven, maatschappelijke organisaties en inwoners.[34] Het WEF (2024) stelt dat bedrijven worstelen om de impact op hun belangrijkste doelen te minimaliseren en hun diensten te blijven leveren bij cyberincidenten. Cyberweerbaarheid is te belangrijk om aan het toeval over te laten.

[33] Zie ook: https://crisismanager.nl/roelofsma-e%C3%A9n-klein-foutje-kan-een-hele-keten-platleggen

[34] https://www.dutchitchannel.nl/news/511906/rijksoverheid-waarschuwt-bugers-zich-voor-te-bereiden-op-cyberaanval

Toch schieten veel bedrijven tekort in hun aanpak. Dit onderstreept de noodzaak om het concept van cyberweerbaarheid volledig te doorgronden en een gedeeld begrip van het belang ervan te ontwikkelen (WEF, 2024, p. 6).

Ook de verschillende opvattingen over de aanpak van cyberrisico's leiden tot verwarring. Velen hanteren een 'kasteel-mentaliteit', waarbij de nadruk ligt op robuustheid tegen voorspelbare risico's. Voor anderen betekent dit juist het accepteren van onkenbare risico's en het leren omgaan met deze onzekerheden door middel van flexibiliteit. Deze meerduidigheid van het begrip 'aanpak' kan leiden tot verwarring en een gebrek aan duidelijke praktische toepassing (Dupont, Shearing, Bernier, & Leukfeldt, 2023). Het kan een negatieve invloed hebben op het vermogen om cyberrisico's te beheren. Deze verwarring wordt versterkt door de hype rond cybersecurity, waarbij leveranciers marketingtaal en hippe modewoorden gebruiken om hun producten te verkopen.

Waar dit verschil in opvatting over de aanpak van cyberrisico's toe kan leiden, wordt weerspiegeld in de rechtszaak die Delta Air Lines onlangs is gestart tegen het beveiligingsbedrijf CrowdStrike, als gevolg van de eerder besproken grootschalige storing in juli van 2024. Die storing leidde tot annuleringen en verstoorde reisplannen van 1,3 miljoen klanten van het luchtvaartbedrijf (zie figuur 5). De financiële schade bedroeg $500 miljoen, zegt het bedrijf.[35] Delta zegt dat CrowdStrike 'ongeteste en foutieve updates bij zijn klanten opdrong, met als gevolg dat meer dan 8,5 miljoen Microsoft Windows-gebaseerde computers wereldwijd crashten', schrijft Reuters.[36]

Delta beschuldigt CrowdStrike van grove nalatigheid en wangedrag, onder meer omdat de problematische update niet gefaseerd naar klanten werd gedistribueerd, maar deze in één keer voor iedereen beschikbaar werd gesteld. CrowdStrike zegt dat de claims van de luchtvaartmaatschappij laten zien dat het bedrijf niet goed begrijpt hoe een moderne aanpak van cyberrisico's werkt. 'Het weerspiegelt een wanhopige poging om de schuld voor het trage herstel van zich af te schuiven'. Volgens CrowdStrike is dat trage herstel namelijk het gevolg van een verouderde IT-infrastructuur. Wat Crowdstrike hier eigenlijk zegt is dat de aanpak van cyberrisico's door Delta niet meer van deze tijd is. Dat Delta teveel een cybersecuritystrategie heeft gevolgd, terwijl dat eigenlijk een cyberweerbaarheidsstrategie had moeten zijn. Wie heeft hier gelijk?

[35] https://www.dutchitleaders.nl/news/512015/delta-air-lines-klaagt-crowdstrike-aan-na-grootschalige-storing-in-juli
[36] https://www.reuters.com/legal/delta-sues-crowdstrike-over-software-update-that-prompted-mass-flight-2024-10-25/

Figuur 5. Vliegtuigen van Delta Air Lines staan geparkeerd (*bron: Wikimedia Commons; beeld: Elisfkc2*).

Hoofdstuk 3

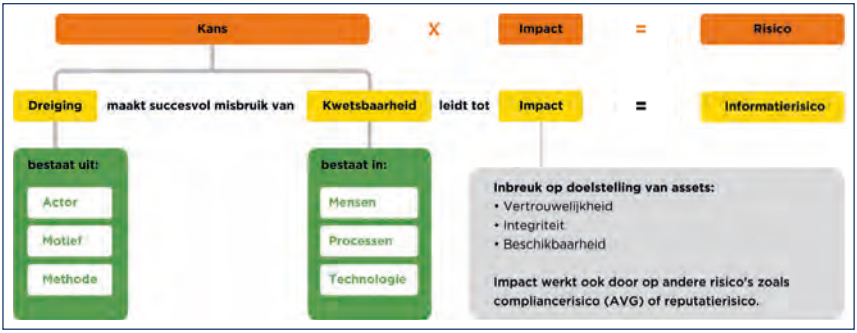
Aanpak van cyberrisico's meer weerbaar maken

De opbouw van cyberrisico's

Naast omvangrijk slachtofferschap met schade tot gevolg, laat het jaarlijkse *Cybersecuritybeeld Nederland* (CSBN) zien dat cyberrisico´s steeds meer toenemen (NCTV, 2024a). In het licht van bovenstaande is het dan ook niet verwonderlijk dat de Cyber Security Raad (CSR) - een nationaal en onafhankelijk adviesorgaan van het kabinet dat is samengesteld uit vertegenwoordigers van publieke en private organisaties en de wetenschap - het nieuwe kabinet adviseert om meer te investeren in digitale veiligheid. De CSR waarschuwt dat de huidige inspanningen en investeringen in cybersecurity niet genoeg zijn om de groeiende digitale dreigingen vanuit statelijke actoren en cybercriminelen het hoofd te bieden (Emerce, 2024). Los van het feit dat meer investeringen nodig zijn, en dat de Nederlandse staat van mening lijkt te zijn dat de bedrijven, burgers en gemeenten zelf verantwoordelijk zijn voor het verbeteren van hun cyberweerbaarheid[37], rijst de vraag waar dan in te investeren? Om die vraag te beantwoorden is het nodig om eerst goed naar het begrip cyberrisico te kijken en hoe daar mee om te gaan.

Onlangs publiceerde SURF, de ict-coöperatie van Nederlandse onderwijs- en onderzoeksinstellingen, een 'formule' voor het berekenen van risico in informatiebeveiliging, wat ook de beveiliging van fysieke informatie omvat (zie figuur 6) (Van Deursen, & Altawekji, 2023). Algemeen gesteld is risico de kans op een incident maal de impact. Binnen de mogelijkheid dat een cyberincident optreedt (kans) is het voor cybersecurity nuttig om een onderscheid te maken tussen dreiging en kwetsbaarheid. Daar waar de politie en het Openbaar Ministerie zich vooral richten op het bestrijden van dreigingen via opsporing en vervolging van criminelen en het verstoren van criminele activiteiten (Openbaar Ministerie & Politie, 2024), nemen bedrijven traditioneel vooral maatregelen om kwetsbaarheden te verhelpen en zich te beschermen tegen cyberdreiging.

[37] In het akkoord tussen de Rijksoverheid en de Nederlandse gemeenten, gepubliceerd in de Staatscourant in december 2023, zijn bijvoorbeeld afspraken gemaakt over de cyberweerbaarheid van gemeenten. Echter, er zijn geen specifieke middelen toegekend om deze afspraken te realiseren. Zie ook Kamerstuk 26643, nr. 1112, https://zoek.officielebekendmakingen.nl/kst-26643-1112.html



Figuur 6. De opbouw van een informatierisico: kans x impact = risico (*herdrukt van Van Deursen & Altawekji, 2023*).

Deze eenzijdige focus op preventie zien we dan ook terug in definities van cybersecurity: het beschermen van computers, servers, mobiele apparaten, elektronische systemen, netwerken en gegevens op die systemen tegen specifieke dreigingen die kwetsbaarheden proberen te misbruiken om gevolgen te bewerkstelligen die economische of politieke impact hebben (zie bijvoorbeeld Gisladottir, Ganin, Keisler, Kepner, & Linkov, 2017). Inspanningen op het gebied van cybersecurity richten zich dan ook voornamelijk op het verminderen van kwetsbaarheden en, in mindere mate, op de gevolgen van een succesvolle aanval, bijvoorbeeld door het maken van back-ups. Het uitvoeren van risicobeoordelingen draagt hier in belangrijke mate aan bij.

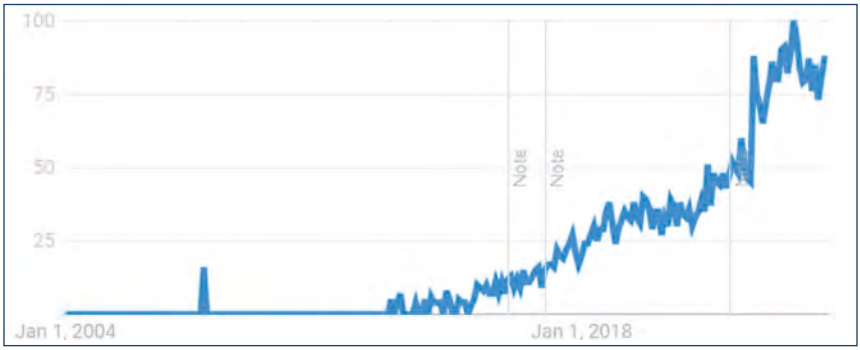
De bovenstaande benadering van het uitvoeren van risicobeoordelingen wordt in de veiligheidskunde gezien als exemplarisch voor zogenoemde enkelvoudige en lineaire incidentmodellen (Ebert, Schaltegger, Ambuehl, Schöni, Zimmermann, & Knieps, 2023). Enkelvoudige modellen schrijven incidenten toe aan één duidelijk omschreven gebeurtenis (bijvoorbeeld een aanval of een technische fout), terwijl lineaire modellen uitgaan van falen op meerdere (maar onderling verbonden) niveaus. De kracht van enkelvoudige en lineaire modellen ligt in hun eenvoud. Ze zijn bijzonder nuttig voor het analyseren van incidenten die veroorzaakt worden door falen van technische componenten of menselijke fouten in eenvoudige socio-technische systemen. Ze zijn dan ook populair in cybersecurity. Het is echter belangrijk te erkennen dat deze klassieke aanpak van cyberrisico's niet onfeilbaar is en mogelijk niet altijd alle bijdragende factoren van een incident omvatten.

Het uitvoeren van een risicobeoordeling is een steeds grotere uitdaging geworden. Dit komt deels door de moeilijkheid om adequaat rekening te houden met mogelijke cascade-effecten die voortvloeien uit storingen (zie ook Dunn Cavelty, Eriksen, & Scharte, 2023; Roelofsma, 2024). Een complicerende factor is dat klassieke risicobeoordelingsmethoden niet kunnen worden toegepast als data niet beschikbaar is, incompleet is, of anderszins niet kan worden bepaald (Dunn Cavelty e.a., 2023). Een risicobeoordeling vereist dat risico's kunnen worden geïdentificeerd *ex ante* (Collier, Hassler, Lambert, DiMase, & Linkov, 2019). Door de snelle ontwikkelingen in het dreigingslandschap ontstaan echter telkens nieuwe dreigingen die op voorhand niet kunnen worden voorzien of voorkomen. Het gebrek aan data over deze nieuwe dreigingen, bijvoorbeeld over de frequentie van voorkomen en mogelijke impact op de bedrijfsvoering, maakt het uitvoeren van risicobeoordelingen lastig. Hierdoor is een cybersecuritystrategie slechts gedeeltelijk effectief. Catastrofale incidenten zoals de COVID-19 pandemie hebben bovendien de politieke significantie vergroot om weerbaar te zijn tegen zogenaamde laagwaarschijnlijke, hoog-impact gebeurtenissen (Dunn Cavelty e.a., 2023).

Naar een nieuwe aanpak van cyberrisico

Een nieuwe risicomanagementbenadering is dus nodig (Collier e.a., 2019; Linkov e.a. 2014). Een aanpak van cyberrisico's die rekening houdt met de toename aan complexiteit in het dreigingslandschap en die ook bescherming biedt tegen toekomstige cyberdreigingen. Leukfeldt noemde in dit verband 'pop-up-criminaliteit'[38]: plotselinge vormen van criminaliteit die in één keer heel groot worden, zoals whatsappfraude. Het onverwachte karakter hiervan maakt het lastig om ons ertegen te beschermen. Het idee dat bedrijven cyberweerbaar (in het Engels: cyber resilient) moeten zijn als reactie op cyberincidenten is de afgelopen jaren dan ook opgekomen en populair geworden (zie ook figuur 7).

[38] https://slachtofferhulp.maglr.com/jaarverslag-slachtofferhulp-nederland-2022/deskundige-en-slachtoffer-online-criminaliteit-aan-het-woord



Figuur 7. Interesse over tijd wereldwijd sinds 2004 voor de zoekterm 'cyber resilience' (*bron: Google Trends; geraadpleegd op 30 september 2024*).

Het algemene idee van weerbaarheid is dat in plaats van alle inspanningen te richten op het buitenhouden van criminelen uit bedrijfsnetwerken, het beter is aan te nemen dat zij uiteindelijk door de verdediging van de systemen zullen breken. Er moet dus ook aandacht zijn voor het verminderen van de impact van deze gebeurtenis. De overheid stapt al over van de notie dat Nederland beschermt moet worden tegen cyberaanvallen, naar de invalshoek *assume breach*: ga ervan uit dat er al een kwaadwillende in je netwerk zit (NCTV, 2023a; 2024a). In het verlengde hiervan zei justitieminister David van Weel in augustus 2024, nadat meerdere overheidsinstanties getroffen waren door de eerder genoemde storing in het digitale krijgsmachtnetwerk Nafin: 'Get used to it.' Later voegde hij tijdens zijn openingsspeech bij de ONE Conference, een internationale cybersecurity conferentie, hieraan toe: 'And deal with it.'[39] Van Weel: 'Kwetsbaarheden gaan we altijd houden. De kwestie is hoe snel kunnen we zorgen dat we kunnen doorwerken als er een storing is. En hoe snel kunnen we de storing vinden en zorgen dat het netwerk weer online komt.' Van Weel benadrukte ook dat overheid en bedrijfsleven weerbaarder moeten worden.[40] Ook premier Dick Schoof relativeerde deze storing in Nafin onlangs nog.[41] Hij noemt het 'op zijn minst gezegd ontzettend vervelend', maar benadrukt daarbij dat kwetsbaarheden in cruciale ict-systemen nu eenmaal niet helemaal te voorkomen zijn: 'Telefoons doen het ook weleens niet. Zo is het ook met systemen.'

[39] One conference 2024. Den Haag
[40] https://www.agconnect.nl/maatschappij/beheer/politici-boos-op-justitie-minister-over-reactie-ict-storing
[41] https://www.agconnect.nl/maatschappij/infrastructuur/premier-schoof-wuift-grote-ict-storing-nederland-weg

Weerbaarheid is meer dan een modewoord

Zoals gezegd is het idee dat organisaties cyber resilient moeten zijn als reactie op cyberincidenten de afgelopen jaren opgekomen en populair geworden. Het woord resilience is afgeleid van het Latijnse woord *resilire* wat *'to leap back'* betekent volgens *Oxford English Dictionary*, ofwel terugveren.[42] Het eerste geregistreerde gebruik is volgens de *Oxford Living Dictionary* uit 1529.[43] In de context van cyberdreigingen is echter de term weerbaarheid gangbaarder dan terugveren. Dat heeft deels te maken met het feit dat weerbaarheid het actieve vermogen benadrukt van een systeem om weerstand te bieden aan dreigingen. Het legt meer de nadruk op de capaciteit van systemen om niet alleen terug te veren, maar ook om zichzelf te verdedigen en aan te passen aan voortdurende en toekomstige dreigingen.

Weerbaarheid is zoals gezegd geen nieuw begrip. Het concept weerbaarheid werd voor het eerst gebruikt in de materiaalkunde. In deze context verwijst het naar het vermogen van een materiaal om te herstellen van stress of spanning zonder permanente vervorming of schade. Het concept beschrijft hoe goed een materiaal kan terugkeren naar zijn oorspronkelijke vorm en functie nadat het is blootgesteld aan krachten die het vervormen, zoals druk, rek, of buiging. In de materiaalkunde gaat het specifiek om de capaciteit van een materiaal om energie op te nemen wanneer het wordt belast en deze energie weer vrij te geven wanneer de belasting wordt verwijderd. Een veerkrachtig materiaal kan bijvoorbeeld buigen onder druk en vervolgens terugveren naar zijn oorspronkelijke vorm zodra de druk wordt weggenomen. Het conceptueel kader van weerbaarheid is later toegepast in andere vakdisciplines, zoals ecologie en psychologie.

Weerbaarheid is een complex concept, aangezien dit geen lineair proces of enkele handeling is, maar eerder vereist dat er competenties aanwezig zijn in verschillende fasen, zowel vóór als na een potentiële schokgebeurtenis, dat makkelijker te observeren is als het ontbreekt dan als het er is (Eken e.a., 2024). Van Harmelen beschrijft weerbaarheid zelfs als een emergent fenomeen (2022). Weerbaarheid is volgens haar geen ding of vaste eigenschap, maar refereert aan een complex dynamisch proces van positieve adaptatie aan een stressor dat zich ontvouwt over tijd. Van Harmelen (2022) stelt dat we weerbaarheid niet kunnen zien of testen, maar wel kunnen afleiden uit de reactie op een

[42] Zie ook https://www.nytimes.com/1983/12/04/magazine/on-language-when-you-say-that-resile.html

[43] https://english.stackexchange.com/questions/397293/what-made-the-usage-of-the-figurative-meaning-of-resilience-popular

schokgebeurtenis, dat een bedrijf weerbaarheid laat zien. Dientengevolge zijn er meerdere definities van weerbaarheid in omloop, die allemaal enigszins van elkaar verschillen, afhankelijk van de vakdiscipline waarbinnen ze worden gebruikt of het niveau van aggregatie (Hillmann & Guenther, 2021). In de kern beschrijft weerbaarheid het vermogen van een systeem, individu, of gemeenschap om te herstellen van en zich aan te passen aan verstoringen of veranderingen, zoals natuurrampen of psychologische stress. De basisprincipes blijven vergelijkbaar: de capaciteit om te absorberen, aan te passen, en terug te keren naar een normale of verbeterde toestand na een verstoring.

Een veelgebruikte definitie van weerbaarheid wordt gegeven door de National Academies of Science (NAS) en luidt als volgt:

> ***'The ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events (National Research Council, 2012).'***

Vrij vertaalt staat hier: 'het vermogen om zich voor te bereiden op, te kunnen reageren op, herstellen van, en zich aan te passen aan ongunstige gebeurtenissen.'

Hollnagel (2011), die belangrijke bijdragen heeft geleverd aan het denken over weerbaarheid, voegt hier aan toe:

> ***'..., so that systems can sustain required operations under both expected and unexpected conditions.'***

Hiermee verwoordt Hollnagel een belangrijk doel van weerbaarheid, namelijk bedrijfscontinuïteit. De focus is daarmee komen te liggen op het vermogen om te functioneren als vereist, ook tijdens alledaagse condities. In later werk heeft Hollnagel (2021) een, in mijn ogen, belangrijke verlenging in focus aangebracht door te stellen dat weerbaarheid daarmee ook een adequate reactie op *kansen* omvat, wanneer die zich voordoen:

> ***'the scope of resilient performance is not just to be able to recover from threats and stresses, but rather to be able to perform as needed under a variety of conditions —and to respond appropriately to both disturbances and opportunities.'***

Het idee dat weerbaarheid niet alleen gaat om het reageren op dreigingen, maar ook om het zoeken naar en benutten van kansen (denk aan de mogelijkheden van GenAI voor geautomatiseerde beveiliging), is een belangrijke toevoeging aan het traditionele denken over weerbaarheid naar mijn mening. Dit betekent dat een weerbaar systeem niet alleen overleeft of zich aanpast bij tegenslagen, maar ook alert is op onverwachte, positieve mogelijkheden om de effectiviteit, veiligheid of duurzaamheid te verbeteren. De nadruk bij weerbaarheid ligt op het *versterken* van de adaptieve capaciteiten van het systeem, zodat zij zich onder wisselende omstandigheden kan aanpassen, in plaats van enkel negatieve uitkomsten te verminderen (Ebert e.a., 2023).

Vier vermogens staan centraal

Vier vermogens, ofwel doelen, staan centraal, zoals ook blijkt uit de definitie van de NAS: voorbereiden, reageren, herstellen en aanpassen (zie ook tabel 1). Na een fase van aanpassen volgt idealiter een transitie terug naar de voorbereidende fase (Eken e.a., 2024).

Voorbereiden legt de basis om diensten beschikbaar en activa functioneel te houden tijdens een verwachte of onverwachte verstorende gebeurtenis. Het omvat de mogelijkheid om te anticiperen op ontwikkelingen, zoals potentiële verstoringen, nieuwe eisen of beperkingen, nieuwe kansen of veranderende operationele omstandigheden (Hollnagel, 2011; 2022). Tijdens de voorbereidingsfase is het cruciaal om gerichte preventieve maatregelen te implementeren en de bescherming te versterken door het ontwikkelen en trainen van responscapaciteiten (Eken e.a., 2024).

Reageren is gericht op behoud van functionaliteit van de meest kritische activa en de beschikbaarheid van diensten terwijl de verstoring wordt afgeweerd of geïsoleerd. Dit betekent dat het systeem in staat moet zijn om te reageren op reguliere en onregelmatige veranderingen, verstoringen en kansen door voorbereidende acties te activeren of de huidige werkwijze aan te passen (Hollnagel, 2011; 2022). Ook het verzamelen en analyseren van relevante gegevens om een goed begrip te krijgen van de omvang en aard van de situatie is van belang (Eken e.a., 2024). Continu en accuraat monitoren op risico's is essentieel om voorbereid te zijn op veranderende omstandigheden en snelle besluitvorming te ondersteunen.

Daarnaast is effectieve en efficiënte communicatie cruciaal tijdens deze fase. Dit omvat het verstrekken van duidelijke en tijdige informatie aan belanghebbenden, zoals overheidsinstanties, organisaties en het brede publiek. Het doel is om snelle en adequate reacties te faciliteren en miscommunicatie of paniek te voorkomen (Eken e.a., 2024). Eken en collega's noemen ook het belang van het waarborgen dat personeel, materieel, capaciteiten en alle noodzakelijke middelen beschikbaar en operationeel zijn voor crisisrespons. Reageren vraagt om een goede samenwerking tussen verschillende partijen om zo effectief en tijdig op de crisis te reageren.

Herstellen richt zich op het resetten van alle activafunctionaliteit en beschikbaarheid van diensten naar hun functionaliteit vóór de verstorende gebeurtenis. Dit omvat het herstarten van economische activiteiten en toegang tot essentiële infrastructuur. Het doel is om stabiliteit en veiligheid voor het getroffen systeem te waarborgen (Eken e.a., 2024). Deze fase omvat ook het terugbrengen van het systeem naar een paraatheidsstaat voor toekomstige crises. Dit houdt in dat verloren middelen worden vervangen en dat het systeem wordt teruggebracht naar een pre-crisis toestand. Voorbeelden hiervan zijn het herstellen van basisvoorzieningen, het hervatten van normale zakelijke activiteiten en het zorgen voor een functionerende infrastructuur.

Het is belangrijk om te definiëren wat herstel na een incident inhoudt en te begrijpen welke acties een organisatie moet ondernemen om ervoor te zorgen dat het herstel zo snel en effectief mogelijk verloopt. Het herstellen van systemen en het terughalen van gegevens maken hier uiteraard deel van uit, net als het in stand houden van kritieke diensten en uiteindelijk het herwinnen van volledige operationele capaciteit. Herstel omvat echter ook het opnieuw opbouwen van reputatie, marktaandeel en klantvertrouwen, wat veel langer kan duren en mogelijk vereist dat de organisatie zelfs beter presteert dan voor het incident (WEF, 2024). Sommige bedrijven zullen in staat zijn om sterker terug te komen, terwijl anderen mogelijk nooit volledig herstellen (Leigh, 2023).
Uit het voorgaande kunnen we opmaken dat succesvol herstel inhoudt dat:

- de operationele activiteiten weer in werking zijn;
- de impact op interne en externe belanghebbenden is verminderd;
- financiële en handelsprestaties zijn hersteld; en
- strategische activa zijn beschermd (WEF, 2024).

In **aanpassen** wordt kennis van de verstorende gebeurtenis gebruikt om het systeem te veranderen met als gewenst resultaat een hoger niveau van weerbaarheid dan voor de verstorende gebeurtenis (Eken e.a., 2024). Dit omvat het verzamelen en analyseren van lessen die zijn opgedaan tijdens de crisis door betrokkenheid van verschillende belanghebbenden. Ook het integreren van de geleerde lessen in de volgende voorbereidende fase om bestaande structuren, instellingen en middelen aan te passen is onderdeel van deze fase. Dit proces richt zich op het versterken van systemen door deze beter af te stemmen op toekomstige uitdagingen.

Recent onderzoek suggereert dat een verstorende gebeurtenis adaptatie of transformatie kan katalyseren, wat kan leiden tot een sterk verbeterde systeemprestatie na een crisis, bekend als 'bouncing forward', 'bouncing back better' (Grøtan, Antonsen & Kolstø Haavik, 2022) en als 'antifragile' (Taleb, 2012). Dit concept is een steeds gangbaarder element geworden in de literatuur (zie bijvoorbeeld Hynes, Trump, Love, & Linkov, 2020). Een belangrijk deel van deze fase is het creëren van innovatieve praktijken. Dit omhelst het ontwikkelen en implementeren van nieuwe en creatieve benaderingen om het vermogen te vergroten om op crises voor te bereiden en erop te reageren. Dit kan innovaties op het gebied van mens, proces of technologie omvatten die de weerbaarheid van het systeem verder versterken.

Tabel 1. De vier doelen van weerbaarheid (*zie ook Ross, Pillitteri, Graubart, Bodeau, & McQuaid, 2021*).

Doel	*Omschrijving*
Voorbereiden	Het handhaven van een staat van geïnformeerde paraatheid voor tegenspoed en kansen.
Reageren	In staat zijn om te reageren op reguliere en onregelmatige veranderingen, verstoringen en kansen.
Herstellen	Missie- of bedrijfsfuncties kunnen herstellen tijdens en na een verstorende gebeurtenis.
Aanpassen	Het gebruiken van kennis van de verstorende gebeurtenis om missie- of bedrijfsfuncties en/of ondersteunende capaciteiten te veranderen met als resultaat een hoger niveau van weerbaarheid en systeemprestatie dan voor de verstorende gebeurtenis.

Weerbaarheid in het veiligheidsdomein: cyberweerbaarheid

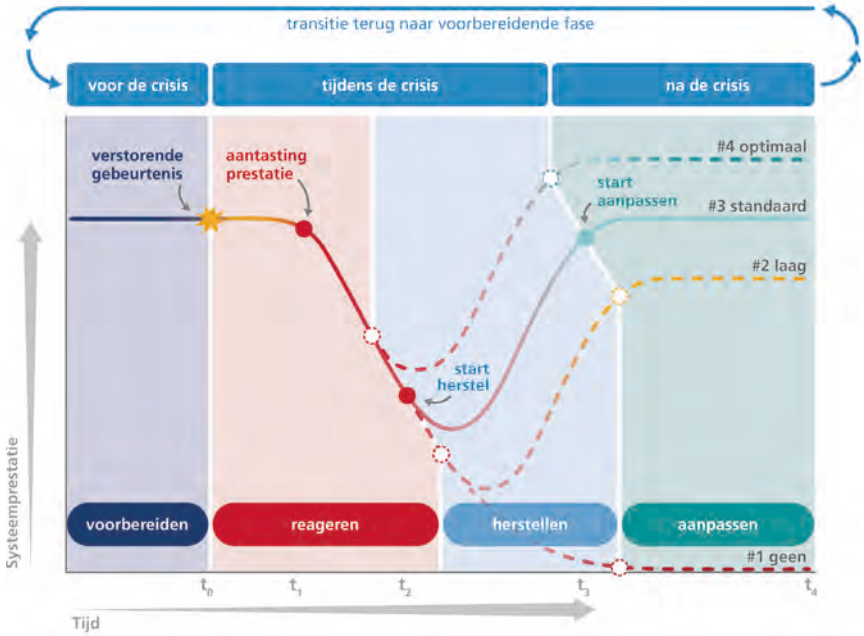
Het gebruik van het concept weerbaarheid in het veiligheidsdomein, waar cybersecurity een subdomein van is, is van recentere datum. In de veiligheidskunde werd vanaf de jaren 2010 het begrip pas populair. Dit werd mede veroorzaakt doordat een groeiend aantal wetenschappers, maar ook praktijkmensen, inzag dat de traditionele definitie van veiligheid in de zin van de afwezigheid van ongevallen niet langer functioneel was en wel een revisie kon gebruiken (Hollnagel, 2022).

In de veiligheidspraktijk is weerbaarheid sterk geïnspireerd door organische systemen, zoals het menselijk immuunsysteem, die zich aan veranderende omstandigheden kunnen aanpassen en zichzelf kunnen herstellen. Net zoals biologische systemen immuniteit ontwikkelen om te reageren op infecties en andere aanvallen, moeten systemen zich aanpassen, zo is de gedachte, aan de steeds veranderende bedreigingen (Wlodarczak, 2017). Net als het menselijk lichaam zijn systemen niet hermetisch afgesloten. Het immuunsysteem is ook niet in staat alle aanvallen buiten de deur te houden (Van Boheemen e.a., 2020; zie ook Ross, Pillitteri, Graubart, Bodeau, & McQuaid, 2021). Systemen moeten in staat zijn om vitale systeemfuncties te blijven beschermen en veerkrachtig te herstellen van de gevolgen van incidenten nu en in de toekomst. Dit idee sluit aan bij het idee om systemen in het veiligheidsdomein te bezien vanuit de sociotechniek, waarbij alle onderdelen van een systeem – zoals mensen, technologie, en organisatorische structuren – in samenhang worden gezien. Samenwerking tussen deze componenten is vereist ten behoeve van gezamenlijke optimalisatie (Appelbaum, 1997). Het streven is naar een veerkrachtig systeem dat niet alleen problemen voorkomt, maar ook steeds beter wordt in het omgaan met en herstellen van verstoringen (Ross e.a., 2021).

Cybersecurity is ongelijk aan cyberweerbaarheid

Cybersecurity legt de nadruk op het voorkomen van degradatie van prestatie en het behoud van functionaliteit. Cyberweerbaarheid daarentegen omvat niet alleen het voorkomen van schade, maar ook het vermogen om te kunnen reageren op, te herstellen van, en zich aan te passen aan ongunstige gebeurtenissen of activiteiten die kunnen leiden tot verstoring van het systeemfunctioneren. Het is zoals gezegd een dynamischer concept dat erkent dat absolute veiligheid niet haalbaar is (Kott & Linkov, 2021). Er bestaat niet zoiets als 100% veiligheid. Organisaties moeten handelen vanuit de aanname dat er aanzienlijke cyberincidenten zullen plaatsvinden. In die zin is cybersecurity niet hetzelfde als cyberweerbaarheid, maar een essentieel onderdeel in het streven ernaar (WEF, 2024, p. 8). Zelfs wanneer risico's worden

geïdentificeerd en er acties worden ondernomen om het risico te verminderen, blijft er altijd een restrisico over. Het managen van cyberweerbaarheid is deels een poging om het algehele vermogen van een systeem te verbeteren om het resterende restrisico te beperken en om onbekende of opkomende (toekomstige) dreigingen en kansen aan te pakken (Linkov & Kott, 2019).



Figuur 8. Cyberweerbaarheidscurve (*bewerkt van Sarker & Lester, 2019*).

Figuur 8 geeft het vermogen om te herstellen van cyberincidenten weer aan de hand van de zogenaamde weerbaarheidscurve. De y-as geeft de systeemprestatie weer en de x-as laat zien dat cyberweerbaarheid over de tijd verschillende uitkomsten kan hebben. De vier weerbaarheidsdoelen - voorbereiden, reageren, herstellen en aanpassen - staan weergegeven boven de x-as. Deze doelen spelen een belangrijke rol vóór, tijdens en na een verstorende gebeurtenis. Onder de x-as staan een aantal gebeurtenissen vermeld. Op t_0 vindt een cyberincident plaats. Op t_1 leidt dit tot een aantasting van de systeemprestatie. De tijd tussen t_0 en t_1 wordt bepaald door de robuustheid van het systeem. Robuustheid refereert aan de mate waarin een systeem in staat is om onverwachte nadelige effecten het hoofd te kunnen bieden zonder degradatie van systeemprestatie tot gevolg. Hoe groter de robuustheid, hoe groter de tijd tussen t_0 en t_1.

Op t_2 begint het herstel van de systeemprestatie. Op t_3 start het aanpassen van het systeem. De cyberweerbaarheid van een systeem is de oppervlakte die ligt besloten in het 'dal' tussen t_1 en t_3. Hoe kleiner de oppervlakte, hoe weerbaarder het systeem.

Idealiter leidt het herstel en de adaptatie tot een hoger algemeen weerbaarheidsniveau. In figuur 8 is dit weergegeven als scenario #4: het optimale cyberweerbaarheidsniveau. Dit scenario kan ook worden omschreven als *bouncing back better* (Grøtan, Antonsen & Kolstø Haavik, 2022). Het hogere weerbaarheidsniveau kan een positief effect hebben op de systeempresentatie (Leigh, 2023). Door te leren van incidenten kan in de toekomst beter worden omgegaan met vergelijkbare verstoringen. Aanpassingsmaatregelen zouden dan ook tenminste gericht moeten zijn op een incrementele verhoging van de cyberweerbaarheid tot een optimaal niveau (Häring, Ebenhöch, & Stolz, 2016). Maar ook andere scenario's zijn denkbaar. Een verstorende gebeurtenis kan leiden tot blijvende aantasting van de systeemprestatie en een nieuw lager normaal. Dit is weergeven als scenario #2. Ook is denkbaar dat het systeem de verstoring niet te boven komt en in elkaar stort (zie ook Hatami & Segel, 2023). Voor een bedrijf betekent dit dat zij failliet gaat. Dit is weergegeven als scenario #1. Op t_4 start de transitie terug naar de voorbereidende fase (zie ook Eken e.a., 2024).

Een systemische kijk op cyberweerbaarheid

Cyberweerbaarheid op het systeemniveau omvat meer dan alleen een technische infrastructuur; het is een samenhangend geheel van hardware, software, netwerken, gegevens, processen en mensen die nodig zijn om zich voor te bereiden op, te kunnen reageren op, herstellen van, en zich aan te passen aan cyberincidenten. Deze bredere benadering omvat een holistische of systemische kijk. Een aanpak waarbij weerbaarheid niet kan worden gereduceerd tot enkel de som van alle technische maatregelen die een bedrijf neemt, maar het resultaat is van constante interacties tussen alle elementen die noodzakelijk zijn om essentiële functies en diensten te leveren (Dunn Cavelty e.a., 2023; Dupont, 2019; Dupont e.a., 2023). Daarnaast klinkt steeds vaker door dat cyberdreigingen ook in samenhang moeten worden bekeken met andere dreigingen, zoals militaire of terroristische dreigingen. Niinistö (2024) noemt dit een *all hazard* aanpak waarvan het belang wordt onderstreept door het huidige kabinet.[44]

[44] Zie Kamerstuk 33 694, 2024/25, nr. 70. Internationale Veiligheidsstrategie, p. 4.

Een systemische kijk zien we terug in systeemmodellen uit de veiligheidskunde (Ebert e.a., 2023). Systeemmodellen erkennen dat incidenten natuurlijke (onvermijdelijke) uitkomsten zijn van de werkomgeving, in plaats van gebeurtenissen die uitsluitend door afzonderlijke oorzaken worden bepaald (Ebert e.a., 2023). Daarom zou de nadruk niet moeten liggen op het voorkomen van cyberincidenten, maar op het anticiperen op hun optreden en het beperken van hun gevolgen. Systeemmodellen zijn geworteld in de systeemtheorie, die stelt dat incidenten meer zijn dan de som van afzonderlijke hoofdoorzaken; ze ontstaan uit de interacties tussen de componenten van een socio-technisch systeem (Qureshi, 2008).

Een systemische of systeemdenken-benadering ziet een organisatie als een set van complexe, onderling afhankelijke elementen. Dit staat tegenover mechanistisch denken, dat een organisatie beschouwt als een verzameling losse onderdelen. Peter Senge (2006), bekend van *The fifth discipline*, stelt dat mechanistisch denken problemen veroorzaakt door complexe processen te reduceren tot geïsoleerde taken. Dit leidt tot silo-denken, waarbij afdelingen als afzonderlijke eenheden functioneren zonder oog voor onderlinge relaties. Systeemdenken daarentegen helpt om cyberrisico's als multidimensionale vraagstukken te benaderen die een holistische oplossing vereisen.

Cyberweerbaarheid gedefinieerd

Vanuit het hierboven geschetste brede en holistische perspectief volgt de in deze rede door mij bepaalde definitie van cyberweerbaarheid:

> ***'Het vermogen van een systeem, dat bestaat uit een samenhangend geheel van hardware, software, netwerken, gegevens, processen en mensen, om onverwachte, positieve mogelijkheden te benutten om digitale processen te verbeteren en zich voor te bereiden op, te kunnen reageren op, te herstellen van, en zich aan te passen aan een verstoring van de digitale omgeving die kan leiden tot een aantasting van het functioneren.'***

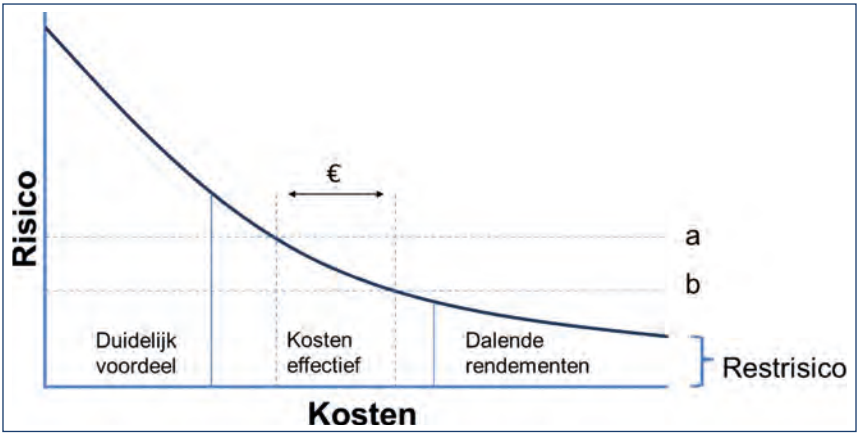
Samenvattend kunnen we stellen dat het toenemende gebruik van de term cyberweerbaarheid een groeiend bewustzijn weerspiegelt dat een hermetisch afgesloten 'kasteel' onmogelijk te bouwen is. Cyberincidenten zijn niet te voorkomen. Het is belangrijk om te leren met tegenslag om te gaan. Dat is zeker niet eenvoudig. Het wordt daarom belangrijker om te accepteren dat incidenten (en kansen) zich voordoen, adequaat te reageren, ervan te herstellen waar nodig en te evalueren en te leren voor een volgende keer. Dat laat onverlet dat de basis – het 'kasteel' – zo stevig mogelijk moet zijn (Van Boheemen e.a., 2020).

Cyberweerbaarheid gaat niet zonder slag of stoot

De veiligheid van digitale processen is essentieel in onze gedigitaliseerde samenleving, maar het belang van die veiligheid concurreert soms met andere belangen (NCTV, 2024b). Stevige en snelle groei van (cyber)weerbaarheid is van groot belang aldus de WRR (2024), maar gaat niet zonder slag of stoot (p.115). Er zullen offers moeten worden gebracht. Belangentegenstellingen kunnen binnen een organisatie spelen, maar het kan ook zo zijn dat de belangen van organisaties concurreren met belangen op landelijk niveau (NCTV, 2024b). Daarnaast nemen de kosten van veiligheid alsmaar toe.

Cybersecurity is, zoals ik eerder heb laten zien, gericht op het identificeren en versterken van kritieke elementen van het systeem die kwetsbaar zijn voor dreigingen. Opkomende technologieën resulteren in nieuwe dreigingen met veelal onbekende impact. De gevolgen van deze nieuwe dreigingen in termen van economisch verlies, uitvaltijd en overige schade zijn veelal nog onbegrepen en lastig te kwantificeren. Ik hoop u in deze rede overtuigd te hebben van het feit dat cybersecurity in deze gevallen tekort schiet.

Door de inherente onzekerheid van nieuwe dreigingen neemt het aantal kritieke componenten en potentiële kwetsbaarheden exponentieel toe. Het is niet langer kosteneffectief om al deze componenten te beschermen tegen alle mogelijke vormen van dreiging. Er komt een punt, zoals op het diagram weergegeven in figuur 9, dat de kosten niet langer opwegen tegen de baten, het beter is om restrisico te accepteren en te investeren in maatregelen die de *cyberweerbaarheid* vergroten, zoals een goed herstelplan (Linkov, Ligo, Stoddard, Perez, Strelzoffx, Bellini, & Kott, 2023). Cyberweerbaarheid ligt daarmee dus deels in het verlengde van cybersecurity, gericht op de aanpak van restrisico (Linkov & Kott, 2019).



Figuur 9. Diagram van kosten om risico's aan te pakken. Door risiconiveau 'a' te accepteren over risiconiveau 'b' kan budget worden gealloceerd aan maatregelen die de cyberweerbaarheid vergroten (*bewerkt van Bostick, Connelly, Lambert, & Linkov, 2018*).

Investeringen in cyberweerbaarheid brengen kosten met zich mee die zich veelal niet direct uitbetalen in extra systeemfunctionaliteit. Dit heeft een nadelig effect op de efficiëntie van het systeem op de korte termijn. Door de hoge mate van (1) onzekerheid op het zich voordoen van incidenten die (2) samenhangt met veelal onbekende dreigingen en (3) door onzekerheid over de terugverdientijd van de investering blijven noodzakelijke investeringen in cyberweerbaarheid regelmatig uit. De dreigingen liggen veelal op de lange termijn ver buiten de aanstellings- of ambtstermijn van management of bestuur. Wat ook meespeelt in de besluitvorming rondom investeringen in cyberweerbaarheid is de hang naar efficiëntie bij bedrijven. Principes als *just-in-time* en *outsourcing* zorgen voor verbeterde efficiëntie, maar gaan vaak ten koste van de cyberweerbaarheid (Stratix, 2024). Het doen van investeringen kan bovendien een nadelig effect hebben op de concurrentiepositie. Als concurrenten niet investeren in cyberweerbaarheid dan hebben die partijen, op de korte termijn althans, een concurrentievoordeel.

Meyer en Kunreuther (2017) noemen de kortzichtigheidheuristiek als verklaring voor het uitblijven van investeringen. Beslissingen om te investeren in cyber-beveiligingsmaatregelen vereisen vooruitziendheid. Of het nu gaat om de beslissing van een ondernemer om te investeren in een geavanceerde firewall, of een burger die moet beslissen zijn of haar computer te beschermen tegen cybercrime, al deze beslissingen vereisen voorafgaande investeringen om uitgestelde (en meestal onzekere) voordelen te behalen. Helaas is een van onze grootste zwakheden als mens dat onze intuïtieve planningshorizonten meestal korter zijn dan nodig is om de langetermijnwaarde van dergelijke investeringen te zien.

Hoewel we misschien de noodzaak van meer cyberweerbaarheid waarderen, legt onze kortzichtigheid een verlammende handicap op onze capaciteit om maatregelen te adopteren. We zien ofwel de waarde van de investeringen niet, of we stellen ze uit, ten onrechte gelovend dat de toekomstige versies van onszelf vooruitziender zullen zijn dan de huidige versie. Als mens kijken we te weinig naar de toekomst bij het nadenken over onze keuzes, vergeten we te snel het verleden en proberen we deze beperkingen te overwinnen door het gedrag van andere mensen te imiteren die net zo vatbaar zijn voor deze fouten als wij (Meyer & Kunreuther, 2017).

Linkov en collega's (2023) hebben modelmatig gedemonstreerd dat investeringen in cyberweerbaarheid noodzakelijk zijn voor optimalisatie van de efficiëntie van het systeem op de lange termijn. Een hogere weerbaarheid vermindert de impact van verstoringen en versnelt het herstel ervan, wat tot gevolg heeft dat de economische kosten van cyberincidenten op de langere termijn aanzienlijk lager zijn. Investeren in cyberweerbaarheid draagt bovendien bij aan een verbetering van de reputatie van een organisatie, bijvoorbeeld door te voldoen aan klantvereisten en het op de markt brengen van veilige producten (Saeed, Altamimi, Alkayyal, Alshehri, & Alabbad, 2023). Het is dan ook van belang dat ondernemers gaan inzien dat investeringen in cyberweerbaarheid positieve uitkomsten hebben. Volgens sommige schattingen genereren cyberweerbaardere bedrijven zelfs aandeelhoudersrendementen die ongeveer 50% hoger zijn dan die van hun minder weerbare concurrenten (Hatami & Segel, 2023). Het niet opbouwen van cyberweerbaarheid kan daarentegen leiden tot verstoring van bedrijfsprocessen en, zoals eerder besproken, zelfs tot faillissement (Hatami & Segel, 2023).

De cyberweerbaarheidsopgave

Ik kom dan nu tot wederom een belangrijk deel van mijn betoog. Hoe gaan we het groot digitaal dilemma waar bedrijven voor staan aanpakken? Hoe kunnen we zorgen dat bedrijven cyberweerbaarder worden? Want het ontstaat niet vanzelf (Boin, Linck, Van Duin, Hendriks, Berger, & Van der Varst, 2020). Als een bedrijf meer cyberweerbaarheid nuttig en nodig acht, vraagt dit om gerichte inspanningen. Je komt er niet met een strategie van *laisser-faire*. En hoewel er al een solide basis ligt, is het niet genoeg, aldus het NCTV (2024b). In het huidige tijdsgewricht, met een verslechterende veiligheidssituatie, ontkomen we er niet aan om een flinke stap extra te zetten. We moeten onze cyberweerbaarheid verhogen door inzichtelijk te maken wat aanvullend nodig is, ook wel de cyberweerbaarheidsopgave genoemd.[45]

Deze opgave kan worden begrepen als een regelproces, of ander hulpmiddel voor continu leren en verbeteren, zoals de kwaliteitscirkel van Deming (*Plan-Do-Check-Act*), van voorbereiden, organiseren en controleren van de middelen van een systeem om ervoor te zorgen dat het naar behoren functioneert (Hollnagel, 2022). De doelen zijn ofwel het benaderen van een nieuwe en meer wenselijke toestand of het vermijden of ontwijken van een bestaande maar ongewenste toestand van cyberweerbaarheid. Naast het benaderen of vermijden van iets, kan de reden voor een verandering ook zijn om de huidige positie te handhaven. Dit lijkt misschien een paradox, maar dat is het niet. Als een bedrijf zich op de beoogde of gewenste positie bevindt, wil ze daar uiteraard blijven. Omdat de omstandigheden—zowel intern als extern—in de praktijk nooit perfect stabiel zijn, zullen er veranderingen nodig zijn om te compenseren voor alles wat de status quo kan beïnvloeden (Hollnagel, 2022).

Hollnagel (2022) gebruikt als voorbeeld het plannen van een reis om het managen van cyberweerbaarheid te beschrijven. Deze (reis)metafoor is handig, omdat het helpt om te kunnen controleren hoe iets beweegt en van positie verandert, of de reis nu fysiek of abstract is en of het onderwerp tastbaar of ontastbaar is. De metafoor is ook nuttig, omdat het wijst op de noodzaak van drie verschillende soorten kennis.

[45] Zie ook: https://www.rijksoverheid.nl/onderwerpen/dreiging-in-nederland/nieuws/2024/12/06/kabinet-werkt-aan-verhogen-weerbaarheid-tegen-militaire-en-hybride-dreigingen

Het is noodzakelijk om te weten:
1. wat de huidige positie is,
2. wat het doel is, en
3. welke middelen nodig zijn, dat wil zeggen welke veranderingen nodig zijn en hoe deze te maken om in de richting van het doel te bewegen (Hollnagel, 2022).

Ik licht dit hieronder toe.

Het bepalen van de huidige positie

Een belangrijke eerste stap in de cyberweerbaarheidsopgave waar bedrijven voor staan is het meten van hun huidige cyberweerbaarheid (zie ook Kott & Linkov, 2021). Zonder goede metingen is het lastig te bepalen of maatregelen de cyberweerbaarheid verbeteren of juist verminderen. De CSR pleit in een beleidsreactie van 25 november 2024 voor een jaarlijkse meting.[46] Huidige metingen zoals de *Cybersecuritymonitor* van het CBS meten vooral cybercrime-gerelateerde incidenten en de maatregelen die getroffen worden om deze incidenten te voorkomen. Dit zijn uitdrukkelijk geen metingen van cyberweerbaarheid. Maar eerder van cybersecurity. Hoe moet het dan wel?

Eerder refereerde ik al aan de opvatting dat weerbaarheid een emergent fenomeen is. Van Harmelen (2022) stelt dat weerbaarheid niet refereert aan een vaste eigenschap die je kan meten zoals temperatuur met een thermometer, of gewicht met een weegschaal. Weerbaarheid refereert aan het proces van dynamische adaptatie aan een schokgebeurtenis. Dat betekent dat we weerbaarheid alleen kunnen vaststellen uit de reactie op de schokgebeurtenis. Een goede meetmethode dient derhalve in staat te zijn om de dynamische interacties over het verloop van tijd in kaart te brengen.

Nederveen en collega's (2024) inventariseerden onlangs methoden om maatschappelijke weerbaarheid te meten. Ze onderscheiden daarbij verschillende methoden, waaronder indices, methoden gebaseerd op beoordelingen door deskundigen en kwantitatieve benaderingen. Slechts drie methoden voldeden aan redelijke eisen, zoals repliceerbaarheid en validiteit. Om een inschatting te kunnen maken van de weerbaarheid in de context van nationale veiligheid is uiteindelijk gekozen voor de weerbaarheidsmatrix van Linkov, Eisenberg, Bates, Chang, Convertino, Allen, Flynn en Seager (2013). Deze methode laat per cel bepaalde capaciteiten van het systeem scoren door deskundigen.

[46] https://www.cybersecurityraad.nl/documenten/adviezen/2024/06/04/csr-advies-verkleinen-van-de-cyberweerbaarheidskloof

De scoring resulteert in een matrix waarin iedere cel een gemiddelde score bevat die de weerbaarheid van een systeem meet (Nederveen, Hoorens, Frinking, & Van Soest, 2024, p.45). Een interessante vraag zou zijn of deze methode ook geschikt is voor een jaarlijkse meting van de cyberweerbaarheid.

Bepalen van het doel

Het CSBN 2021 kopt 'cyberaanvallen tasten zenuwstelsel maatschappij aan' en stelt dat cyberweerbaarheid in onze maatschappij nog onvoldoende is, waarbij een groot verschil tussen bedrijven wordt geconstateerd in de mate hiervan (NCTV, 2021). Het CSBN spreekt in dit verband over een 'cyberweerbaarheidskloof'. Ook recente versies van het CSBN bevestigen dit beeld. Het CSBN uit 2023 stelt bijvoorbeeld:

> ***'Er gaapt een groeiende kloof tussen organisaties die de cyberveiligheid op orde hebben en organisaties die dat niet hebben (NCTV, 2023a; zie ook de NLCS 2022-2028 p.13).'***

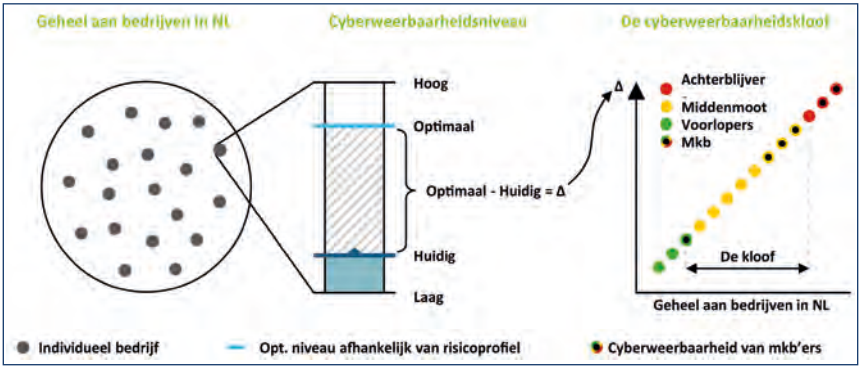
Het CSBN uit 2023 constateert daarbij dat ondanks beste bedoelingen deze 'achterblijvers' niet altijd actie ondernemen in het verhogen van hun huidige cyberweerbaarheidsniveau naar een optimaal niveau, passend bij het risicoprofiel van het bedrijf. De CSR stelt in de hierboven genoemde beleidsreactie dat vooral in het mkb relatief veel achterblijvers zijn.

Deloitte (2024, p. 12) beschrijft de cyberweerbaarheidskloof aan de hand van het huidige cyberweerbaarheidsniveau versus het optimale cyberweerbaarheidsniveau van een bedrijf (zie figuur 10). De huidige cyberweerbaarheid van een bedrijf is het vertrekpunt. De optimale cyberweerbaarheid is het beoogde doel dat nodig is om vastgestelde risico's afdoende te mitigeren en digitaal weerbaar te zijn. Het totaalpakket aan risico's (het risicoprofiel) wordt onder andere bepaald door de aard van een bedrijf, de sector en de keten waarin het actief is, de digitale infrastructuur, de gevoeligheid van data en het dreigingslandschap.

Het optimale cyberweerbaarheidsniveau is dus afhankelijk van het risicoprofiel, en verschilt daarom ook per bedrijf. Bedrijven waarbij het huidige niveau van cyberweerbaarheid ook het optimale niveau van cyberweerbaarheid betreft (of daar heel dichtbij zit) hebben hun cyberrisico's onder controle, terwijl er ook bedrijven zijn waarbij het huidige cyberweerbaarheidsniveau ver achterblijft bij het optimale niveau.

Voor deze laatste groep betekent dit dat bedrijven of:

- de huidige en/of optimale cyberweerbaarheidsniveaus niet kennen, of
- deze niveaus wel kennen, maar er bewust niet voor kiezen of onvoldoende in slagen de cyberweerbaarheid te versterken.



Figuur 10. De cyberweerbaarheidskloof (*herdrukt van Deloitte, 2024*).

Deloitte (2024) stelt daarmee dat het optimale cyberweerbaarheidsniveau afhankelijk is van het type bedrijf. Een bakker hoeft in absolute termen niet even cyberweerbaar te zijn als een internationaal technologiebedrijf in de medische sector. Als bedrijven onderling worden vergeleken, is dus het verschil tussen het optimale en huidige niveau van belang. Dit verschil definieert of een bedrijf voorloopt of achterblijft in vergelijking met andere bedrijven. Een bedrijf dat vooroploopt hoeft dus niet per se de meeste cyberbeveiligingsmaatregelen te hebben geïmplementeerd.

Welke middelen nodig zijn

Het mag duidelijk zijn dat de cyberweerbaarheid van een systeem wordt beïnvloed door vele verschillende factoren, vaak op een complexe en tegenstrijdige manier. Het verkleinen van het verschil tussen het optimale en het huidige niveau van weerbaarheid vereist dat deze factoren zorgvuldig worden beheerd of benut. Tegelijkertijd verschillen systemen onderling, waardoor het niet mogelijk is om een uniforme set maatregelen te bieden om de cyberweerbaarheid te verbeteren (NCTV, 2024b, p.47; Eken e.a., 2024, p. 5). De bakker uit het voorbeeld hierboven heeft bijvoorbeeld vooral behoefte aan een beveiligd kassasysteem, terwijl een bedrijf in de gezondheidszorg

vooral behoefte heeft aan begin-tot-eindversleuteling van patiëntgegevens en gesegmenteerde netwerken. Ondanks dat er geen standaardaanpak bestaat voor het doen laten toenemen van de cyberweerbaarheid in de richting van het optimale niveau, wil ik hieronder toch een poging doen om zeven inzichten samen te vatten, als onderdeel van de essentie van mijn betoog, die ik bij het schrijven van deze rede heb opgedaan.

Zeven inzichten voor optimale cyberweerbaarheid

Naar een nieuw paradigma

Mijn eerste inzicht is dat een paradigmaverschuiving nodig is in ons denken over cyberveiligheid. Ik hoop u na het lezen van deze rede overtuigd te hebben dat het huidige denkkader dat we cybersecurity noemen niet meer afdoende is in onze benadering van cyberrisico's. Cybersecurity richt zich op het versterken van kwetsbare onderdelen van het bedrijf om voorspelbare dreigingen te kunnen weerstaan. Maar dat is, zoals ik heb laten zien in deze rede, allang niet meer passend. Geopolitieke spanningen, verschuivende internationale machtsverhoudingen en technologische innovaties zorgen voor een toename van nieuwe dreigingen en de snel voortgaande digitalisering zorgt voor een toename van complexiteit en onvoorspelbaarheid in het dreigingslandschap. Bedrijven worden daardoor steeds kwetsbaarder. Een doorbraak naar een nieuw paradigma is nodig.

Het denkkader dat bedrijven weerbaar moeten zijn als reactie op cyberrisico's is de afgelopen jaren opgekomen en populair geworden. We noemen deze nieuwe kijk op de aanpak van cyberrisico's ook wel cyberweerbaarheid. Het managen van cyberweerbaarheid omvat niet alleen een aanpak gericht op het voorkomen van schade. Het omvat ook het vermogen om onverwachte, positieve mogelijkheden te benutten om de veiligheid te verbeteren en te kunnen reageren op, te herstellen van, en zich aan te passen aan ongunstige gebeurtenissen of activiteiten. De nadruk bij weerbaarheid ligt op het versterken van de adaptieve capaciteiten van het systeem, zodat zij zich onder wisselende omstandigheden kan aanpassen, in plaats van enkel negatieve uitkomsten te verminderen (Ebert e.a., 2023). Praktijkgericht onderzoek vervult een belangrijke rol in de doorbraak naar dit nieuwe paradigma, omdat deze doorgaans wordt afgedwongen doordat bepaalde nieuwe wetenschappelijke inzichten steeds opnieuw proefondervindelijk worden gestaafd (Kuhn, 1962). Hierover meer in het laatste deel van mijn rede (zie H. 4.).

Eenduidigheid in terminologie

Een tweede inzicht is dat een streven naar een gemeenschappelijk begrippenkader over de aanpak van cyberrisico's nodig is. In deze rede heb ik laten zien dat er verschillende opvattingen zijn over deze aanpak en, gerelateerd daaraan, het begrip cyberweerbaarheid. Deze meerduidigheid van begrippen en het niet goed afstemmen van terminologie kan leiden tot miscommunicatie, verwarring en een gebrek aan duidelijke praktische toepassing (Dupont e.a., 2023). Dit kan een negatieve invloed hebben op het streven van bedrijven om de cyberweerbaarheid te doen laten toenemen in de richting van het optimale niveau.

Deze meerduidigheid maakt het verhaal uit het Oude Testament over de Babylonische spraakverwarring[47] actueel. Volgens dit verhaal wilden de mensen een toren bouwen die tot in de hemel reikte om zo hun naam groot te maken en niet over de hele aarde verspreid te raken. Deze toren is uitgebeeld in figuur 11. God zag hun hoogmoed en besloot hun taal te verwarren, zodat ze elkaar niet meer konden verstaan. Hierdoor werd de bouw van de toren gestaakt en verspreidden de mensen zich over de aarde.[48]

Figuur 11. Pieter Bruegel I, De toren van Babel, ca. 1565, olieverf op paneel (*bron: Museum Boijmans Van Beuningen; beeld: Fotografie Studio Tromp*).

[47] http://www.biblija.net/biblija.cgi?Bible=Bible&m=Genesis+11%3A1-9&pos=0&set=10&l=en
[48] https://historiek.net/babylonische-spraakverwarring-herkomst-van-de-uitdrukking/95738/#-google_vignette

Net zoals de mensen in Babel verschillende talen begonnen te spreken, kan meerduidigheid ertoe leiden dat onderliggende patronen en wederzijdse afhankelijkheden worden gemist. Dit kan leiden tot inefficiëntie en conflicten tussen belanghebbenden, zoals afdelingen binnen het bedrijf of tussen ketenpartners, en een gefragmenteerde aanpak van beveiligingsmaatregelen. Het optimaliseren van de cyberweerbaarheid vraagt om expliciete keuzes, ook in de bestuurlijke keuze voor begrippen. Het is van belang dat daarin wordt onderkend dat cybersecurity niet hetzelfde als cyberweerbaarheid is, maar slechts een klein onderdeel in het streven ernaar. Nog beter zou het zijn, zoals hierboven beargumenteerd, als we afstappen van het idee dat we cybersecurity noemen. De door mij bepaalde definitie van cyberweerbaarheid, zoals verwoord in deze rede, kan dienen als uitgangspunt richting harmonisatie van de verschillende opvattingen over de aanpak van cyberrisico's en praktische toepassing (zie p. 37).

Balans in doelen

Een derde inzicht is dat er evenwicht moet zijn in onze aandacht voor de vier doelen van cyberweerbaarheid: voorbereiden, reageren, herstellen en aanpassen. Van deze vier doelen krijgen voorbereiden en aanpassen veelal de minste aandacht (Van der Kleij & Leukfeldt, 2019). Cyberincidenten vragen directe actie, terwijl de vermogens tot voorbereiden en aanpassen zonder sterke sturing blijven liggen. Dat is, simpel gezegd, niet handig, want juist door te balanceren of navigeren tussen ervaringen uit het verleden (aanpassen) en verwachtingen voor de toekomst (voorbereiden), zorgen bedrijven ervoor dat ze niet alleen reageren op dreigingen, maar ook een adequate reactie tonen op *kansen* als die zich voordoen. Dit betekent dat een cyberweerbaar systeem niet alleen zich aanpast bij tegenslagen, maar ook anticipeert en alert is op onverwachte, positieve mogelijkheden, zoals de opkomst van (Gen)AI, om de effectiviteit, veiligheid of duurzaamheid van het systeem te verbeteren.

Door te *leren* van wat in het verleden fout is gegaan kunnen organisaties hun verdediging bovendien versterken en zich beschermen tegen toekomstige cyberdreigingen. Organisaties kunnen leren van hun eigen ervaringen, maar ze kunnen ook proberen te leren van wat fout gaat en wat goed werkt bij andere organisaties (Verweijen, 2022). Het voordeel van dergelijk plaatsvervangend leren is dat organisaties niet gebukt gaan onder de risico's of kosten van een directe ervaring, maar wel lessen kunnen trekken van andere organisaties om hun eigen cyberweerbaarheid te verbeteren.

Er is echter nog weinig onderzoek gedaan naar hoe organisaties hun strategie rondom cyberweerbaarheid kunnen baseren op cyberincidenten (Patterson, Nurse, & Franqueira, 2023). Laat staan dat we weten hoe organisaties kunnen leren van dat wat goed gaat (zie ook Hollnagel, 2018). Hollnagel (2018) stelt bijvoorbeeld dat het moeilijk is te detecteren wat goed gaat, omdat dit regelmatig voorkomt en omdat dit niet systematisch of duidelijk kan worden uitgelegd. Door een benadering te volgen die zich richt op het begrijpen en versterken van wat goed gaat in een systeem, in plaats van alleen te proberen te voorkomen wat fout kan gaan, kunnen organisaties niet alleen leren van fouten, maar ook van successen, wat leidt tot een weerbaarder systeem. Hollnagel (2018) noemt deze benadering Safety-II. Safety-II moedigt aan tot een meer positieve kijk op veiligheid. Waar Safety-I zich richt op het voorkomen van ongevallen en incidenten door te analyseren wat er fout gaat, legt Safety-II de nadruk op het begrijpen en versterken van wat goed gaat in een systeem.

Relationeel kapitaal

Een vierde inzicht dat ik hier wil noemen is dat relationeel kapitaal van essentieel belang is in de cyberweerbaarheidsopgave. Een hoog niveau van relationeel kapitaal stelt bedrijven in staat om cybercrises het hoofd te bieden en om de cyberweerbaarheid te versterken (Matos, Tonial, Monteiro, Selig, & Edvinsson, 2022). Relationeel kapitaal kan worden begrepen als een immateriële hulpbron van de organisatie die in staat is kennis te genereren uit haar relaties met haar strategische partners. In andere woorden, bedrijven kunnen de cyberweerbaarheid optimaliseren door meer (relevante) samenwerkingen op te tuigen (zie ook Jansen, 2023; p. 66).

Relationeel kapitaal is gebaseerd op het idee dat bedrijven geen geïsoleerd systeem zijn, maar deel uitmaken van een onderling verbonden systeem, afhankelijk van hun relatie met de externe omgeving. Een nauwe relatie met strategische partners kan aldus een effectieve aanpak van cyberweerbaarheid vergroten (zie ook Jansen, 2023). Het overheidsinitiatief om samenwerking tussen publieke en private organisaties te stimuleren via het landelijk Cyberweerbaarheidsnetwerk (CWN) benadrukt dit belang.[49]

Door samen te werken kunnen bedrijven hun kennis en ervaringen delen, wat leidt tot een beter begrip van cyberrisico's en effectieve manieren om deze te mitigeren. Een gecoördineerde aanpak maakt het daarnaast mogelijk om sneller te reageren op cyberincidenten, waardoor de impact ervan kan worden beperkt. Door middelen en expertise te bundelen, kunnen bovendien

[49] https://www.ncsc.nl/aansluiten-en-samenwerken/cyberweerbaarheidsnetwerk-cwn

kosten worden bespaard op de aanschaf van cyberbeveiligingsmaatregelen. Een gezamenlijke aanpak, ten slotte, versterkt de algehele veerkracht van het netwerk, waardoor het beter bestand is tegen toekomstige aanvallen. Meer over het belang van relationeel kapitaal volgt in het laatste deel van mijn rede, waar ik mijn eigen onderzoekslijnen bespreek.

Systemisch perspectief

Het vijfde inzicht is dat we cyberweerbaarheid alleen in haar volle rijkdom kunnen begrijpen vanuit een systemisch perspectief. Zoals duidelijk mag zijn uit het voorgaande is het optimaliseren van de cyberweerbaarheid op systeemniveau een complexe opgave. Er zijn veel factoren die invloed uitoefenen op de weerbaarheid en op elkaar. Een systemische ofwel systeemdenken-benadering biedt een geschikte, geïntegreerde benadering door de interacties tussen mens, proces en technologie als geheel te analyseren en samenwerking tussen organisatieonderdelen die een rol spelen in de cyberweerbaarheid te bevorderen.

Een punt dat ik er hier uit wil lichten is dat in het huidige denken over cyberweerbaarheid vooral de mens als component nog wel eens wordt vergeten. De meeste investeringen zitten volgens Gartner in technologie, 85%, 14% gaat naar processen, slechts 1% gaat naar de mens.[50] De balans is helemaal zoek. En dat is opmerkelijk voor een maatschappelijk multidimensionaal vraagstuk dat een holistische oplossing vereist. Om de balans terug te brengen pleit ik hier voor meer aandacht voor de rol van de mens in het systemische perspectief op cyberweerbaarheid.

Dat is geen eenvoudige opgave, want de rol van de mens kan verschillende, vaak tegenstrijdige, vormen aannemen. Drenth en Hendriks (2024) verwoordden dit onlangs treffend door te stellen dat de mens zowel een lastpak als oplossing kan zijn. Zo zien we dat, alle goede bedoelingen ten spijt, ondernemers regelmatig de keuze maken niet te handelen. Dat wil zeggen dat ze besluiten om niet te investeren in hun cyberweerbaarheid en daarmee een belemmering zijn in het maatschappelijke streven de cyberweerbaarheidskloof te overbruggen. Hoe we ondernemers kunnen aanzetten tot handelen blijft een belangrijk aandachtspunt voor de komende jaren, dat ook wordt onderkend door de overheid.[51]

---

[50] https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem#:~:text=Worldwide%20spending%20on%20information%20security,2020%20(see%20Table%201)

[51] Zie ook: https://www.cybersecurityraad.nl/documenten/adviezen/2024/06/04/csr-advies-verkleinen-van-de-cyberweerbaarheidskloof

De mens wordt eveneens genoemd als belangrijke maatregel om de cyberweerbaarheid te versterken. Zo spelen mensen een cruciale rol bij het anticiperen op ontwikkelingen, het continu en accuraat monitoren om voorbereid te zijn op veranderende omstandigheden, het reageren op verstoringen van digitale processen, het herstel van het systeem en het verzamelen en analyseren van lessen die zijn opgedaan tijdens de crisis (zie ook Stratix, 2024). Medewerkers moeten beschikken over vaardigheden, hulpmiddelen en processen om de functies van voorbereiden, reageren, herstellen en aanpassen uit te voeren (zie ook Dupont e.a., 2023, p.7). Door training, educatie en bewustmakingscampagnes kunnen zij worden geïnformeerd over mogelijke dreigingen en hoe ze kunnen bijdragen aan de cyberweerbaarheidsopgave, bijvoorbeeld door het melden van (bijna) cyberincidenten (Nederveen e.a., 2023). Meer over de rol van de mens volgt in het laatste deel van mijn rede.

Positieve business case

Een zesde inzicht is dat we meer moeten toewerken naar positieve business cases op het gebied van cyberweerbaarheid. Het is nodig dat bedrijven cyberweerbaarheid gaan zien als ‘force multiplier’ in plaats van als hinderlijke kostenpost en zodoende investeren in hun cyberweerbaarheid. Het belang van het opstellen van een positieve business case, waarvan de essentie is dat de baten ten gevolge van een beslissing om te investeren in cyberweerbaarheid de kosten overstijgen, kan niet genoeg worden benadrukt. Linkov en collega's (2023) toonden aan dat hoewel investeringen in cyberweerbaarheid op de korte termijn inefficiënties kunnen veroorzaken, deze investeringen cruciaal zijn voor de optimalisatie van de systeemefficiëntie op de lange termijn. Een hogere cyberweerbaarheid vermindert de impact van verstoringen en versnelt het herstel, wat resulteert in aanzienlijk lagere kosten van cyberincidenten op de lange termijn.

Het is dus nodig om bedrijven te vertellen dat investeringen in cyberweerbaarheid positieve uitkomsten hebben. Dat investeringen niet alleen de economische kosten verminderen van cyberincidenten zoals datalekken en verlies van intellectueel eigendom, maar ook bijdragen aan een verbetering van de reputatie van de organisatie, het waarborgen van de bedrijfscontinuïteit en kansen bieden om een concurrentievoordeel te behalen in de markt. De essentie is dat het in alle gevallen helder moet zijn hoe cyberweerbaarheid bijdraagt aan de strategie en doelstellingen van een bedrijf. Een bedrijf dat consequent veilige producten op de markt brengt, bouwt een sterke en positieve reputatie op. Bovendien genereren cyberweerbare bedrijven volgens sommige schattingen, aandeelhoudersrendementen die ongeveer 50% hoger zijn dan die van hun minder weerbare concurrenten (Hatami & Segel, 2023). Het niet investeren in cyberweerbaarheid vergroot daarentegen het risico op verstoring van bedrijfsprocessen en zelfs tot faillissement.

Empirische onderbouwing

Als zevende en laatste inzicht wil ik nogmaals het belang van praktijkgericht onderzoek noemen. We mogen niet uit het oog verliezen dat de belangrijke vragen zijn:

> ***Wat werkt daadwerkelijk in de praktijk, onder welke omstandigheden – en hoe kunnen we dit empirisch vaststellen?***

Praktijkgericht onderzoek, gebaseerd op data en onderzoek in plaats van op anekdotes, zorgt voor oplossingen die direct toepasbaar zijn en aansluiten bij de behoeften van de praktijk. Voor oplossingen die *wel* werken (zie ook Leukfeldt, 2024). Het is naar mijn mening dan ook doorlopend nodig. Zodoende creëren we een doorbraak naar het nieuwe paradigma van cyberweerbaarheid en een situatie waar het werkveld voldoende geïnformeerd is om de juiste besluiten te nemen over het toepassen van de laatste stand van kennis in hun beveiligingspraktijk. Daarover meer in het volgende en laatste deel van deze rede.

Hoofdstuk 4

Mijn leeropdracht

Praktijkgericht onderzoek

De leeropdracht waar ik invulling aan mag geven binnen Avans Hogeschool, is gericht op het cyberweerbaarder maken van Nederland tegen een alsmaar toenemende cyberdreiging. Dit wordt in mijn ogen bereikt door in publiek-private samenwerkingen *praktijkgericht onderzoek* te doen naar direct bruikbare manieren om de maatschappelijke cyberweerbaarheid te vergroten. Ik geloof daarbij in een holistische aanpak van cyberrisico's waarbij de rol van mens, proces en technologie in samenhang moet worden beschouwd vanuit verschillende vakdisciplines. Dit geeft richting aan een toekomst waarin iedereen ten volle kan profiteren van deelname aan de digitale samenleving, vrij van zorgen over cyberrisico's.[52]

Praktijkgericht onderzoek richt zich op het ontwikkelen van praktische, haalbare oplossingen voor actuele problemen in nauwe samenwerking met de praktijk. Het adagium in het cyberdomein is momenteel: we moeten nu iets doen, anders verliezen we de race met de cybercriminelen (Leukfeldt, 2024). Leukfeldt (2024) betoogt dat we het daar niet zomaar mee eens moeten zijn. Ja, we moeten in actie komen, maar dan wel op een goede manier. Leukfeldt roept in dit verband op tot een streven naar *evidence-based cybersecurity,* waarbij wetenschappelijk bewijs de effectiviteit van beveiligingsmaatregelen bepaalt (zie ook De Bruijn & Van Summeren, 2024, p. 210). Dat betekent dat we met elkaar moeten zorgen:

1. voor een goede theoretische onderbouwing van het beleid, de interventie of het project;
2. dat de resultaten meetbaar zijn; en
3. dat we de effectiviteit ook daadwerkelijk meten (Leukfeldt, 2024, p.5).

[52] Zie ook Strategie digitale economie, 2022, pijler 5: versterken cybersecurity, via https://open.overheid.nl/documenten/ronl-c6a3495a523bef54ca41011f629b77b7b611045f/pdf

Tegelijkertijd zien we dat bedrijven de basisbeveiliging vaak niet op orde hebben.[53] Ondernemers missen kennis over de cyberrisico's van hun bedrijf.[54] Nog vaker missen ze kennis over maatregelen om die risico's te verlagen. De ervaring leert mij dat zij soms klakkeloos cyberbeveiligingsmaatregelen overnemen van andere bedrijven. Dit zou best eens schadelijk kunnen zijn voor de cyberweerbaarheid, want wat als die maatregelen incompatibel zijn met de eigen bedrijfssystemen?

Een meer onderzoekende houding door ondernemers is hier gewenst. Door te investeren in praktijkgericht onderzoek kunnen bedrijven hun cyberweerbaarheid optimaliseren. Juist bedrijven die kennis zo hard nodig hebben, trekken echter niet zo makkelijk de beurs. Ik vind dat bedrijven praktijkgericht onderzoek meer serieus moeten nemen als een investering in hun cyberweerbaarheid.[55]

Is cyberweerbaarheid een markt voor zilveren kogels?

Een markt waar alle partijen voldoende geïnformeerd zijn om de juiste besluiten te nemen staat in schril contrast met onvolwassen markten waarin informatie asymmetrisch is verdeeld, zoals zogenaamde markten voor citroenen of limoenen. Een markt voor citroenen is een markt waar de verkoper significant meer kennis heeft dan de koper. Denk aan de markt voor gebruikte auto's. Een markt voor limoenen kenmerkt zich dan juist weer door een situatie waar de koper significant meer kennis heeft dan de verkoper. Denk hierbij aan de markt voor verzekeringen. Het cyberdomein kan worden gezien als een markt waar zowel de verkoper als de koper onvoldoende kennis hebben om rationele besluiten te nemen over de goederen die worden verhandeld.[56] Dit wordt ook wel een onvolwassen markt of een markt voor 'zilveren kogels' genoemd. Een zilveren kogel is een vakterm voor een product of proces dat wordt gepresenteerd als effectief, zonder dat er enige rationele onderbouwing voor die claim bestaat.

[53] https://nos.nl/artikel/2541723-meer-nederlandse-bedrijven-slachtoffer-van-gijzelsoftware-dan-gedacht
[54] https://www.cybersecurityraad.nl/documenten/adviezen/2024/06/04/csr-advies-verkleinen-van-de-cyberweerbaarheidskloof
[55] Zie ook mijn blog van 12 november 2024 over dit onderwerp op Dutch IT Leaders: https://www.dutchitleaders.nl/blog/514186/cyberveiliger-door-praktijkgericht-onderzoek
[56] Ian Grigg, 2008. The market for silver bullets. https://iang.org/papers/market_for_silver_bullets.html; zie ook: https://ventureinsecurity.net/p/cybersecurity-is-not-a-market-for

Een voorbeeld van een onvolwassen markt is die voor firewalls. Een firewall beschermt het computernetwerk tegen ongeautoriseerde toegang door hackers. Een bedrijf dat een firewall aanschaft, heeft vaak beperkte kennis van hoe effectief de software daadwerkelijk is. De koper vertrouwt veelal op marketingclaims of een gevoel van urgentie in plaats van gedetailleerde technische kennis of een grondige beoordeling van de werkelijke prestaties van het product. Tegelijkertijd hebben de cybersecuritybedrijven ook niet volledige kennis van het specifieke risicoprofiel en beveiligingsbehoeften van de koper, vooral omdat deze afhankelijk zijn van de unieke bedrijfsomgeving. Zij verkopen veelal een standaardoplossing zonder op maat gemaakte aanpassingen of adviezen. De klant heeft niet de technische expertise om volledig rationele keuzes te maken. Dit leidt tot inefficiënties in de markt en tot suboptimale niveaus van cyberweerbaarheid.

De Bruijn en Van Summeren (2024) stellen dat een onvolwassen markt kan leiden tot onzekerheid en terughoudendheid bij het aanschaffen van nieuwe of onbekende oplossingen (p. 206). Daar komt bij dat dit ook kan leiden tot een toestand van '*solution uncertainty*': doordat er zoveel aanbod is van standaardoplossingen weten bedrijven en ondernemers niet zo goed meer wat te kiezen, met als gevolg dat investeringen in cybersecurity worden uitgesteld. Grüter (in De Bruijn & Van Summeren, 2024, p. 206) stelt dat bedrijven hierdoor 'vastroesten' in de huidige, maar niet meer passende, oplossingen. Het hoeft geen betoog dat dit de cyberweerbaarheid niet ten goede komt. Praktijkgericht onderzoek kan verandering brengen in dit disfunctioneren van de markt. Door het ontwikkelen van bewijslast voor de effectiviteit en betrouwbaarheid van cyberbeveiligingsmaatregelen kan solution uncertainty worden tegengegaan.

Het resultaat van praktijkgericht onderzoek en de markt die dit creëert is dus essentieel voor het vergroten van de cyberweerbaarheid. Cyberdreigingen zijn dynamisch en veranderen voortdurend. De snelheid waarmee nieuwe technologieën worden ontwikkeld kan ervoor zorgen dat bestaande beveiligingsmodellen snel verouderen. Er is een constante behoefte aan onderzoek naar nieuwe risico's die voortkomen uit deze ontwikkelingen. Praktijkgericht onderzoek maakt het mogelijk om cyberbeveiligingsmaatregelen te blijven verbeteren en aan te passen aan de nieuwste cyberrisico's. Zonder voldoende aandacht hiervoor kunnen bedrijven niet goed inspelen op nieuwe cyberdreigingen en blijven ze kwetsbaar voor aanvallen die kunnen worden voorkomen met de juiste kennis.

Weinig aandacht voor onderzoek

Waarom krijgt het praktijkgericht onderzoek, ondanks het evidente belang, dan zo weinig aandacht, zowel van bedrijven alsmede de overheid? Ten eerste zien we dat bedrijven de cyberdreigingen vaak onderschatten (Deloitte, 2024). Cyberweerbaarheid wordt vaak pas een prioriteit na een incident. Dit reactieve gedrag voorkomt dat bedrijven proactief investeren in onderzoek naar preventie en verbetering van hun cyberweerbaarheid. Ten tweede zien bedrijven cyberweerbaarheid vaak als een kostenpost in plaats van als een noodzakelijke investering in het optimaliseren van de bedrijfsprocessen (zie ook pag. 38: Cyberweerbaarheid gaat niet zonder slag of sloot). Er is weinig ruimte in het budget voor veiligheid, laat staan voor innovatie, vooral bij kleinere bedrijven die geen eigen IT-afdeling hebben. Ze geven de voorkeur aan direct meetbare winst en stellen investeringen in onderzoek en technologie uit, met het risico dat ze kwetsbaar blijven voor toekomstige cyberincidenten.

Hoe kunnen we zorgen dat bedrijven praktijkgericht onderzoek serieus nemen? Een belangrijke taak lijkt weggelegd voor het beroepsonderwijs. De toekomstige ondernemers die het beroepsonderwijs opleidt, hoeven niet altijd zelf onderzoek te kunnen doen, maar ze moeten wel onderzoek kunnen lezen en begrijpen waar het over hun werk gaat. En ze moeten het kritisch kunnen beschouwen en uiteindelijk ook kunnen gebruiken in hun eigen werk. Het praktijkgerichte onderzoek van het middelbaar en hoger beroepsonderwijs in de vorm van respectievelijk practoraten en lectoraten draagt hieraan bij.[57] Het onderzoek dat hierbinnen plaatsvindt, is gericht op het verhogen van de kwaliteit van studenten, het aansluiten van het onderwijs op actuele ontwikkelingen in de praktijk en het invoeren van innovatie in de beroepspraktijk.[58]

De overheid kan richtlijnen of wetgeving implementeren, denk hierbij aan EU-richtlijnen, zoals de NIS2-richtlijn[59], die bedrijven verplicht om te investeren in cyberweerbaarheid. Tegelijkertijd kan de overheid belasting-voordelen bieden aan bedrijven die deelnemen aan praktijkgericht onderzoek. De maatschappelijke uitdaging op het gebied van cyberweerbaarheid vraagt tevens om stabiele en structurele aandacht en financiering voor onderzoek door de overheid zelf. Laat dit nu net onder druk staan. IP-vakblad voor

[57] https://www.avans.nl/over-avans/nieuws-en-pers/nieuwsberichten/detail/2024/02/lectoren-janine-janssen-en-jos-brouwers-we-zien-hbos-als-verbindende-schakel-tussen-universiteit-en-praktijk
[58] https://lectoren.nl/lector-en-lectoraten/profiel-van-de-lector
[59] Meer hierover, zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

informatieprofessionals kopte onlangs *Kabinet heeft nauwelijks aandacht voor digitale veiligheid in Miljoenennota*.[60] Ondanks dat de maatschappelijke uitdaging op het gebied van cyberweerbaarheid om overheidsfinanciering vraagt, lijkt cybersecurity geen financiële prioriteit te hebben voor de regering. Dit is zorgwekkend. Want laat het aanjagen van innovatie nu net een belangrijke rol van de overheid zijn (zie ook De Bruijn & Van Summeren, 2024, p. 230).

Drie onderzoekslijnen

Wat ga ik nu zelf doen binnen dit interessante veld? Ik geef invulling aan de eerder genoemde leeropdracht en de cyberweerbaarheidsopgave van het kabinet door drie onderzoekslijnen die nauw aansluiten bij de pijlers van de *Nederlandse Cybersecurity Strategie*, het daaraan verwante *actieplan Nederlandse Cybersecuritystrategie 2022-2028*, de *Strategie Digitale Economie* uit 2022 (pijler 5: versterken cybersecurity), *De Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023-2029* (actielijn 7), de *CSR meerjarenstrategie 2022-2025* en de *Kennis- en Innovatieagenda (KIA) Veiligheid 2024-2027* (in het bijzonder 'missie 2').

Ik leg hierbij ook nadrukkelijk de verbinding met de proposities voor weerbaarheid van TNO, waar ik naast mijn aanstelling bij Avans Hogeschool werk aan cyberweerbaarheidsvraagstukken binnen de unit Defensie en Veiligheid. De onderzoekslijnen van het lectoraat sluiten tevens aan bij de programmalijnen van het Centre of Expertise Veiligheid & Veerkracht, het onderwijs van verschillende academies binnen Avans Hogeschool en overige kennis-, innovatie- en onderzoekagenda's, zoals de *Agenda Digitale Open Strategische Autonomie* (DOSA), de *KIA digitalisering* en de *Onderzoeksagenda voor praktijkgericht onderzoek* van het SPRONG-expertisenetwerk Cyberweerbaar NL.

De focus van het SPRONG expertisenetwerk ligt, net als van ons lectoraat, niet zozeer op de techniek, maar juist op de mens:

> ***Welke gedrag- en houdingsaspecten beïnvloeden cyberweerbaarheid en hoe kunnen bedrijven deze aspecten ten behoeve van cyberweerbaarheid verbeteren?***[61]

[60] https://informatieprofessional.nl/kabinet-heeft-nauwelijks-aandacht-voor-digitale-veiligheid-in-miljoenennota/
[61] Zie ook: https://cyberweerbaarnl.nl/

De ambitie van de SPRONG-groep is om een toonaangevend expertisenetwerk te worden op het gebied van cyberweerbaarheid binnen publieke en private organisaties en hoogwaardige, relevante en praktisch toepasbare kennis te ontwikkelen op dit onderwerp. Dit met als doel om de cyberweerbaarheid in Nederland te bevorderen (Jansen, 2023).

Een van de doorlopende doelen van het lectoraat is het opzetten en onderhouden van een netwerk van kennis- en werkveldpartners, ofwel de gebruikers van kennis op het gebied van cyberweerbaarheid. Ik ben dan ook verheugd om te kunnen melden dat mijn lectoraat sinds oktober 2024 is aangesloten als partner bij het SPRONG expertisenetwerk Cyberweerbaar NL. Ik zie uit naar de samenwerking met de collega-onderzoekers van de Haagse Hogeschool, Saxion Hogeschool en NHL Stenden.

De drie onderzoekslijnen van mijn lectoraat, in willekeurige volgorde, zijn:
- Cyberweerbaarheid van bedrijven, ketens en ecosystemen;
- Digitale veiligheid van hard- en software;
- Cybersecurity-arbeidsmarkt, onderwijs en cyberweerbaar gedrag.

Figuur 12 verbeeldt de lijnen, kennisproducten en verankering in het werkveld van het lectoraat in een zogenaamde kennisboom. Dijkgraaf (2012) stelt eerder al dat een boom zich bij uitstek leent als beeldspraak voor praktijkgericht onderzoek. De drie takken van de boom symboliseren de zich splitsende kennis (de lijnen), de bladeren de concrete onderwerpen en kennisproducten, zoals cybersecurity by design. De wortels symboliseren de verankering in het werkveld. Hieronder werk ik de onderzoekslijnen verder uit.

Figuur 12. De kennisboom van het lectoraat (*gemaakt met Microsoft Copilot op 21 februari 2025*).

Cyberweerbaarheid van bedrijven, ketens en ecosystemen

Op 4 juni 2024 overhandigde de CSR het advies *Verkleinen van de Cyberweerbaarheidskloof* aan voormalig minister Adriaansens van Economische Zaken en Klimaat.[62] Deze kloof gaat over de grote verschillen tussen bedrijven die hun cyberweerbaarheid op orde hebben en achterblijvers bij wie dit nog niet het geval is. Het advies is mede gebaseerd op de uitkomsten van een onderzoek van Deloitte (2024) naar de oorzaken van de cyberweerbaarheidskloof. Ook verwijst de raad naar een onderzoek van TNO in opdracht van het Digital Trust Center (DTC) naar de beweegredenen voor ondernemers om al dan niet in te zetten op verbetering van hun cyberweerbaarheid (Hof e.a., 2024; zie ook Van der Kleij & Hof, 2024).

[62] https://www.cybersecurityraad.nl/actueel/nieuws/2024/06/04/cyber-security-raad-de-cyber-weerbaarheid-van-het-mkb-moet-versterkt

Niet alleen kennisgebrek speelt een rol bij de groeiende kloof tussen organisaties die hun cyberweerbaarheid goed op orde hebben en organisaties die hier minder makkelijk in mee kunnen komen. Vaak is er ook onvoldoende motivatie, stelt dit rapport van TNO, waar ik niet geheel toevallig de hoofdonderzoeker van was. Je moet dus ook nadenken over hoe je bedrijven kunt enthousiasmeren, hen op hun eigen verantwoordelijkheid kunt wijzen.

Veel bedrijven in vooral het mkb blijven achter met hun cyberweerbaarheid, constateerde de CSR onlangs.[63] Dat is een risico voor de bedrijven zelf, maar kan ook tot maatschappelijke ontwrichting leiden. 'Het mkb vormt de ruggengraat van onze economie en is onmisbaar voor alle grote maatschappelijke transities', zegt CSR-covoorzitter Theo Henrar. 'Tegelijk zien we dat het mkb nadrukkelijk doelwit is van cybercriminelen. Onvoldoende cyberweerbaarheid is een risico voor het voortbestaan van het bedrijf zelf, maar door de onderlinge verbondenheid van bedrijven in de keten ook voor de hele bedrijfsketen zelf en daarmee dus ook voor het functioneren van onze samenleving.'

Veilig digitaal ondernemen

Wanneer bedrijven slachtoffer worden van een cyberincident, krijgen ze te maken met financiële gevolgen, dataverlies en mogelijke schade aan hun reputatie. Het goede nieuws is echter dat veel incidenten kunnen worden voorkomen of een verminderde impact kunnen hebben wanneer beschermende maatregelen worden genomen. Deze maatregelen kunnen eenvoudige acties omvatten, zoals het regelmatig updaten van software, het maken van back-ups of het implementeren van multifactorauthenticatie. Ik noem dit *veilig digitaal ondernemen* (Hof e.a., 2024).

Ondanks dat deze acties eenvoudig lijken en er veel partijen zijn die advies geven over de implementatie ervan, voeren bedrijven ze niet altijd uit. Dit komt door verschillende barrières die hen ervan weerhouden actie te ondernemen om hun cyberweerbaarheid te verbeteren.[64] Sommige ondernemers geloven bijvoorbeeld niet dat cyberdreigingen een risico voor hen vormen, terwijl anderen de mogelijke impact van cyberincidenten onderschatten of niet weten welke stappen ze kunnen nemen om zich ertegen te beschermen.

[63] https://www.cybersecurityraad.nl/actueel/nieuws/2024/06/04/cyber-security-raad-de-cyber-weerbaarheid-van-het-mkb-moet-versterkt

[64] Zie ook mijn blog van 23 juli 2024 over dit onderwerp op Dutch IT Leaders: https://www.dutchitleaders.nl/research/464418/cyberweerbaarheidskloof-verkleinen-overwin-eerst-belemmerende-overtuigingen

Naast een gebrek aan cyberkennis onder ondernemers, constateert Deloitte (2024) dat zij het moeilijk vinden te bepalen hoeveel en waarin zij moeten investeren. Het aanbod van hulpmiddelen voor het mkb is niet overzichtelijk en samenhangend en sluit niet aan bij de behoefte van veel mkb'ers.

Onlangs mocht ik, zoals hierboven al benoemd, voor TNO samen met collega's een onderzoek doen naar het verkleinen van de cyberweerbaarheidskloof. De hoofdvraag van dit onderzoek was hoe de actiebereidheid vergroot kan worden onder niet-vitale organisaties om de digitale weerbaarheid te versterken. Het doel van het onderzoek was om inzicht te geven in de motivaties en barrières die verschillende bedrijven ervaren bij veilig digitaal ondernemen.

Het onderzoek laat zien dat de doelgroep is op te delen in vijf segmenten van verschillende omvang. Deze segmenten verschillen van elkaar wat betreft de mate van veilig digitaal ondernemen en onderliggende gedragsbepalers. Op het gebied van het treffen van maatregelen voor veilig digitaal ondernemen zijn er drie segmenten die achterblijven. Deze vormen maar liefst 66% van alle bedrijven. Het is dan ook van belang dat de overheid hen gericht aanmoedigt om specifieke cyberbeveiligingsmaatregelen te treffen. Bedrijven in deze segmenten hebben te maken met verschillende factoren die hen belemmeren om daadwerkelijk maatregelen te nemen. De overheid kan via een reeks stappen tot interventies komen die aansluiten bij de behoeften van elke specifieke doelgroep. Welke specifieke interventies dit zijn is een onderwerp voor toekomstig onderzoek.

Cyberweerbaarheid van ketens en ecosystemen

Een ander belangrijk onderwerp waar deze onderzoekslijn naar kijkt, is de mogelijkheid om bedrijven en de ketens waarin ze opereren te helpen om hun cyberweerbaarheidsniveau naar een voor hen optimaal niveau te brengen. Binnen het ecosysteem zijn digitale processen, systemen en netwerken in sterke mate verweven met elkaar. Geen enkele organisatie is meer in staat om alle taken volledig zelf uit te voeren (Van Boheemen e.a., 2020). Het gevolg daarvan is een groot en groeiend aanvalsoppervlak voor kwaadwillenden en een grotere kans op uitval. De kwetsbaarheid die deze afhankelijkheid van andere partijen met zich meebrengt, wordt vaak onderschat. Een keten is maar zo sterk als de zwakste schakel. Een aanval op de leveranciersketen veroorzaakt niet alleen problemen bij het gecompromitteerde bedrijf, maar ook bij andere organisaties in de keten (NCTV, 2024a; Munnichs, Kouw, & Kool, 2017).

Een belangrijke vraag is hoe bedrijven effectief kunnen omgaan met de cyberrisico's die ontstaan door deze onderlinge afhankelijkheid (Rorive e.a., 2024). Het gebruik van verklaringen, certificeringen en eigen vragenlijsten vormen veelal de basis om de cyberbeveiliging van ketenpartners te toetsen. Maar deze aanpak brengt met zich mee dat het beantwoorden van al deze vragenlijsten steeds tijdsintensiever wordt. Bedrijven kunnen dit ervaren als een disproportionele last. Rorive en collega's (2024) stellen terecht de vraag of deze methoden wel optimaal zijn, en zo ja, hoe ze slimmer en efficiënter kunnen worden ingezet.

De onderlinge verwevenheid van bedrijven zorgt niet alleen voor een grotere kwetsbaarheid. Een nauwe samenwerking tussen stakeholders, zoals overheden, bedrijven en academische instellingen, kan tevens een effectieve aanpak van cyberweerbaarheid vergroten, zoals ik ook heb betoogd in het vorige deel van deze rede. Een eerdere studie uitgevoerd binnen het Centre of Expertise Veiligheid & Veerkracht van Avans Hogeschool, waar mijn lectoraat onder valt, in samenwerking met het Cyber Weerbaarheidscentrum Brainport en het Regiobureau Integrale Veiligheid Oost-Brabant, stelt zelfs dat het noodzakelijk is om samenwerking centraal te stellen teneinde de digitale veiligheid binnen ecosystemen te verbeteren (Kokkeler, Van den Oord, Ten Thij, & Vollenberg, 2023). Door samen te werken kunnen bedrijven leren van elkaar over de aanpak van cyberdreigingen en kunnen ze actuele dreigingsinformatie verkrijgen. De overheid ziet samenwerking als essentieel om als bedrijf weerbaarder te worden tegen cyberdreigingen[65]. Ze ziet ook dat het in de praktijk echter lastig blijkt voor bedrijven om een samenwerking op te starten en relevante informatie te delen. Eerder heb ik al laten zien dat belemmerende overtuigingen het samenwerken hinderen.[66] Hierdoor komt de cyberweerbaarheid van Nederland in het geding.

De voorliggende uitdaging om bedrijven meer te laten samenwerken om een effectieve aanpak van cyberweerbaarheid te bevorderen kan worden gezien als gedragsvraagstuk. De overheid wil bedrijven stimuleren om vaker informatie te delen via samenwerkingsverbanden over cyberrisico's. Om dit gedrag te beïnvloeden (en te verklaren), maar ook ander gedrag waarmee organisaties de kans om slachtoffer te worden van een cyberincident verkleinen en de gevolgen van incidenten tot een minimum beperken, kan gebruik worden gemaakt van gedragsmodellen.

[65] https://www.digitaltrustcenter.nl/cybersecurity-initiatieven/digital-trust-center#:~:text=Samenwerking%20is%20essentieel%20om%20als,%2C%20regio%2C%20sector%20of%20branche.
[66] https://www.dutchitleaders.nl/news/422158/belemmerende-overtuigingen-staan-betere-cyberweerbaarheid-in-de-weg

Een veelgebruikt model is het *Behavioral change wheel* (Michie, Van Stralen & West, 2011). Dit model is gebaseerd op het idee dat gedrag wordt aangedreven door kennis, gelegenheid en motivatie. Dit model voorspelt dat informatiedelen afhangt van de kennis die de bedrijven hebben over hoe een samenwerking is te organiseren, de gelegenheid die de bedrijven daartoe hebben en de mate waarin de bedrijven gemotiveerd zijn om dat ook daadwerkelijk te doen. Het model doet ook aanbevelingen over hoe gedrag te beïnvloeden is. De eerste toepassingen van dit gedragsmodel in het cyberdomein zijn veelbelovend (zie bijvoorbeeld Van der Kleij, Van 't Hoff-de Goede, Van de Weijer, & Leukfeldt, 2020; Van der Kleij, Wijn, & Hof, 2020). Zo laten Van der Kleij, Hof en Wijn (2020) zien dat het model veilig digitaal werken van medewerkers in de financiële sector verklaart. Van der Kleij, Van 't Hoff-de Goede, Van de Weijer en Leukfeldt (2020) laten zien dat het model tevens gebruikt kan worden om het online gedrag van burgers te verklaren.

Onderzoeksvragen

Relevante onderzoeksvragen binnen deze onderzoekslijn zijn:

- Hoe kunnen we via specifieke maatregelen het gedrag van bedrijven beïnvloeden om hun cyberweerbaarheid te optimaliseren?
- Hoe kunnen we ondernemers aanzetten tot veilig digitaal ondernemen, die van nature geen reden zien om actie te ondernemen om hun weerbaarheid te vergroten, ongeacht de kwaliteit en beschikbaarheid van hulpbronnen?
- Hoe kunnen we het optimale cyberweerbaarheidsniveau vaststellen van bedrijven, passend bij het risicoprofiel van het bedrijf, alsmede het huidige niveau en hoe kunnen we hen helpen via concreet handelingsperspectief om dat niveau te bereiken?
- Welke rol spelen intermediairs, zoals brancheorganisaties, banken, boekhouders, accountants, die dichter bij de ondernemer staan dan de overheid, als mechanisme om gedragsinterventies gericht op het optimaliseren van de cyberweerbaarheid meer succesvol te laten zijn?

Digitale veiligheid van hard- en software

Deze onderzoekslijn focust op het vergroten van de veiligheid van producten en diensten met een digitaal element, voor burgers, bedrijfsleven en overheid, inclusief nieuwe technologieën zoals GenAI. Binnen deze lijn onderzoeken we hoe maatregelen zoals leiderschap en beleid strategisch in te zetten zijn om de transitie naar het ontwikkelen van veilige digitale producten en diensten positief te beïnvloeden. Ook formuleren we aanbevelingen voor verdere actie

en onderzoek op het gebied van cybersecurity van nieuwe technologieën zoals GenAI. Dit draagt idealiter bij aan een toename van hard- en software die cyberveilig zijn, zonder dat daarbij de gebruikservaring wordt belemmerd met meer cyberweerbaarheid als resultaat. Hieronder bespreek ik deze twee onderwerpen, cybersecurity by design (hierna: CSbD) en cybersecurity van GenAI, in meer detail.

Cybersecurity by design

De EU heeft nieuwe cyberbeveiligingsregels voorgesteld voor veiligere producten via de *Cyber Resilience Act* (CRA).[67] De CRA legt cyberbeveiligingsverplichtingen op aan alle producten met digitale elementen. Bovendien introduceert de CRA een wettelijke verplichting tot CSbD.[68] Op 10 oktober 2024 heeft de Raad van de EU goedkeuring gegeven aan de CRA.[69] Deze nieuwe wetgeving, gericht op fabrikanten, distributeurs en importeurs van hardware en software, moet ervoor zorgen dat digitale producten in Europa veiliger worden. Zowel tijdens de ontwikkeling als gedurende hun levenscyclus.

Het idee achter CSbD is dat veel beveiligingsproblemen kunnen worden voorkomen door producten met digitale elementen zo te bouwen dat ze bescherming bieden tegen kwaadwillige cyberactoren voordat ze worden ingezet in een operationele omgeving in de echte wereld. Misschien herinnert u zich nog de hack van beveiligingscamera's en videobabyfoons jaren geleden, waardoor live beelden van deze camera's massaal werden gedeeld op het internet.[70] Veelal doordat kwetsbaarheden in de software konden worden uitgebuit om ongeoorloofde toegang te verkrijgen. Ook levenskritieke systemen zoals pacemakers en insulinepompen zijn volgens experts kwetsbaar voor hacks door gebrekkige ingebouwde beveiliging.[71] Hard- en softwareontwikkelaars houden daarom idealiter vanaf het begin rekening met cybersecurity. Ook met de toenemende integratie van GenAI in diverse aspecten van ons leven, rijzen nieuwe uitdagingen op het gebied van cyberweerbaarheid. GenAI-systemen worden steeds complexer en krachtiger, maar tegelijkertijd worden ze ook vatbaarder voor aanvallen en misbruik.

---

[67] EPRS Briefing on the EU Cyber Resilience Act (14-12-2022)
[68] Nynke Brouwer & Minke Reijneveld 2023. De ontwikkeling van cyberveiligheid in Europa. Voorstel voor de Cyber Resilience Act. NEDERLANDS JURISTENBLAD – 17-03-2023 – AFL. 10
[69] https://www.digitaleoverheid.nl/nieuws/europese-raad-keurt-cyber-resilience-act-goed/
[70] https://www.bbc.com/news/technology-16919664; zie ook: https://tweakers.net/nieuws/179032/hack-gaf-toegang-tot-150000-cameras-in-onder-andere-gevangenissen-en-fabrieken.html
[71] https://www.upi.com/Health_News/2022/06/01/medical-devices-pacemakers-cybersecurity/7041653656330/

In mijn blog van 3 juni 2024 op het online platform van Dutch IT Leaders over CSbD betoog ik dat een beveiligingsmentaliteit bij ontwikkelaars een goede stap voorwaarts is. Het is echter geen wondermiddel voor meer cybersecurity, tenzij het ontwikkelteam integraal verantwoordelijk wordt gesteld voor de digitale veiligheid in al haar facetten.[72] Want een (te) eenzijdige aandacht voor technische aspecten van security kan leiden tot onbruikbare security. Onbruikbare security zorgt uiteindelijk altijd voor 'olifantenpaadjes' in het gebruik, met onveilige situaties tot gevolg. Zo kan het zijn dat een beveiligingscamera veel veiligheidsinstellingen heeft, maar deze niet worden gebruikt omdat ze het gebruiksgemak in de weg staan, waardoor de gebruiker nog steeds het risico loopt om slachtoffer te worden van een hack. Zie hiervoor ook mijn blog van 4 maart 2024 op Dutch IT Leaders, over de rol van de mens in het veiligheidssysteem.[73]

CSbD is dus meer dan alleen veiligheid door ontwerp. CSbD zou ook aandacht voor gebruiksvriendelijkheid moeten omvatten. Maar hoe doen we dat? Hoe zetten we een transitie in beweging naar een meer integrale kijk op veiligheid binnen ontwikkelteams met een overwegend technische oriëntatie? Want er is nog maar weinig aandacht voor het veilig en gebruiksvriendelijk ontwikkelen van producten met digitale elementen. In veel conventionele projecten worden veiligheid en gebruiksvriendelijkheid niet beschouwd als primaire doelen en (dus) vaak geofferd in het proces om deadlines te halen tegen minimale kosten.

Onderzoeken laten zien dat er een relatie is tussen de bedrijfscultuur en het nastreven van CSbD (zie bijvoorbeeld Arizon-Peretz, Hadar, & Luria, 2022; Van der Kleij, Van Hemert, Te Paske, & Rooijakkers, 2024). Bedrijfscultuur wordt gereflecteerd door het gedrag van medewerkers. Dit gedrag wordt beïnvloed door het implementeren van specifieke componenten door de organisatie, zoals kledingvoorschriften, processen of technische maatregelen. Om de hier besproken gewenste integrale kijk op digitale veiligheid te cultiveren in ontwikkelteams, kunnen organisaties ervoor zorgen dat een relevante en adequate set van componenten wordt geïmplementeerd (Da Veiga & Eloff, 2007). Dit draagt bij aan de ontwikkeling van producten die digitaal veiliger zijn zonder dat daarbij de gebruikservaring wordt belemmerd met meer cyberweerbaarheid van gebruikers van deze producten als resultaat.

[72] https://www.dutchitleaders.nl/blog/458433/om-technische-producten-cyberveilig-te-maken-is-een-cultuurverandering-nodig
[73] https://www.dutchitleaders.nl/blog/424598/fouten-maken-mag

Cybersecurity van GenAI

Met de toenemende integratie van AI in diverse aspecten van ons leven, rijzen ook nieuwe uitdagingen op het gebied van cyberweerbaarheid. AI-systemen worden steeds complexer en krachtiger, maar tegelijkertijd worden ze ook vatbaarder voor aanvallen en misbruik. GenAI wordt vaak breed ingezet in allerlei organisaties en op allerlei netwerken. Die omgevingen zijn niet altijd (technisch) goed afgeschermd voor intern gebruik of gesegmenteerd van andere operationele netwerken. Dit vergroot het aanvalsoppervlak voor cybercriminelen waardoor ook de risico´s op binnendringen, manipulatie en datalekken toenemen.[74]

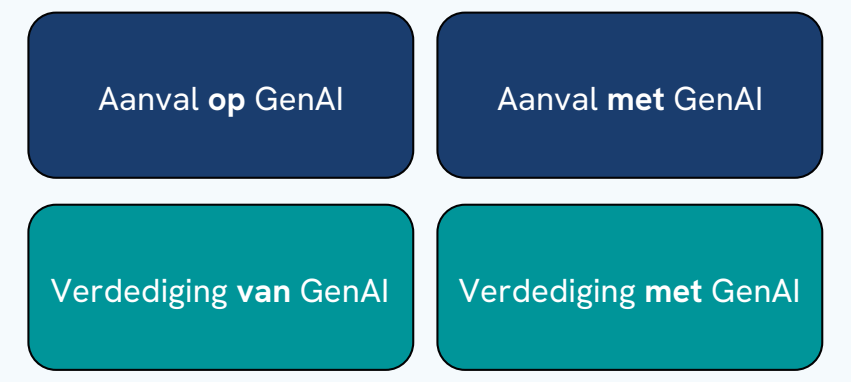
Het grootschalig gebruik van AI-software brengt ook algemene cyberrisico's met zich mee. Juist door (te) snelle invoering is de AI-programmatuur zelf niet in alle gevallen uitvoerig getest en op (onbewuste) fouten gecontroleerd. Ook de authenticiteit en integriteit van datasets en trainingsprogramma's is niet altijd gewaarborgd.[75] In lijn met de CRA en de *Digital Services Act* (DSA)[76] die de EU oplegt, zijn hiervoor extra waarborgen nodig, zeker in bepaalde domeinen zoals de zorg, waar mensenlevens op het spel staan en veel vertrouwelijke data rondgaat.

Het gebruik en de mogelijkheden van GenAI zijn zich nog volop aan het ontwikkelen en de impact op de samenleving kent nog vele onduidelijkheden. Er zijn in ieder geval vier relevante invalshoeken (NCTV, 2024b, p.44):

1. De algoritmen en de data waarmee de algoritmen worden gevoed, kunnen doelbewust worden gemanipuleerd. Dat kan bijvoorbeeld door cyberaanvallen.
2. Gebruikers kunnen (onbedoeld en onbewust) toegang krijgen tot zoekvragen en/of gevoelige informatie door de vragen die ze stellen, de informatie die ze invoeren of de informatie waarmee ze de applicaties voeden.
3. GenAI kan worden gebruikt voor cyberaanvallen. Zo kunnen met behulp van AI meer op een ontvanger toegesneden phishing-mails worden gemaakt. Verder kunnen kwaadwillenden GenAI gebruiken om snel en automatisch interessante doelwitten te detecteren en informatie daarover te verzamelen. Ook kan laagdrempeliger malware worden ontwikkeld.
4. GenAI kan worden ingezet ter verdediging tegen cyberaanvallen, door bijvoorbeeld onregelmatigheden te detecteren in data.

[74] Zie ook: https://www.cybersecurityraad.nl/documenten/brieven/2023/12/22/informerende-brief-aan-de-staatssecretaris-van-bzk-over-generatieve-ai-en-cybersecurity
[75] Ibid.
[76] https://www.digitaleoverheid.nl/nieuws/dsa-voor-alle-digitale-diensten-van-kracht/

Om de bovengenoemde invalshoeken verder te duiden, hebben de Algemene Inlichtingen- en Veiligheidsdienst en de Rijksinspectie Digitale Infrastructuur (AIVD & RDI, 2024) het GenAI cybersecuritykwadrant geïntroduceerd (zie figuur 13). Het kwadrant bestaat uit twee assen. De bovenste vlakken hebben betrekking op de offensieve aspecten van GenAI. Dit zijn dus de dreigingen die gepaard kunnen gaan met GenAI. De onderste as heeft betrekking op het verdedigen van GenAI-systemen en het gebruik van GenAI voor het verdedigen van systemen tegen cyberaanvallen, in het kader van cyberweerbaarheid en veilig gebruik. Op de linkerzijde van het kwadrant is het GenAI-systeem het doel van de aanval of verdediging; rechts wordt GenAI gebruikt als het middel voor de aanval of verdediging.



Figuur 13. GenAI cybersecuritykwadrant (*bewerkt van de AIVD en de RDI, 2024*).

Een eerste verkennend onderzoek binnen mijn lectoraat is reeds gestart naar cybersecurity van GenAI. Docent-onderzoeker Peter van Eck leidt het onderzoek binnen het zorgdomein samen met de Avans Hogeschool lectoraten van Ander de Keijzer en Janine Jansen, het DTC van het ministerie van EZ, zorgverzekeraar ONVZ en met hulp van Z-CERT, het expertisecentrum voor cybersecurity in de zorg. Het onderzoek richt zich primair op het kwadrant linksboven in figuur 13: aanval op GenAI. Hierbij gaat het om aanvallen die gericht zijn op het verstoren of misleiden van GenAI-systemen, inclusief pogingen om de trainingsdata te beïnvloeden of de GenAI op ongepaste wijze te manipuleren (AIVD & RDI, 2024). Vanuit het lectoraat werken ook Esger ten Thij, Renske Korenromp, Astrid van Erk, Roel de Beer en Bert Bambach mee aan dit onderzoek. De resultaten zullen dienen als basis voor verdere onderzoeksinspanningen om de veiligheid van GenAI te versterken en de ontwikkeling van veilige en betrouwbare AI-systemen te bevorderen.

Onderzoeksvragen

Relevante onderzoeksvragen binnen deze onderzoekslijn zijn:

- Hoe is een transitie naar een integrale beveiligingsmentaliteit bij bedrijven te stimuleren in het ontwikkelproces van veilige producten en diensten met een digitale component?
- Welke rol speelt veiligheidscultuur binnen een organisatie in het streven naar cybersecurity by design en hoe is die cultuur te beïnvloeden?
- Hoe kunnen cyberbeveiligingsmaatregelen zo worden ontworpen dat ze het eindgebruikers makkelijk maken om veilig te werken?
- Welke cyberrisico's zijn verbonden aan het gebruik van GenAI en hoe zijn die te verminderen?

Cybersecurity-arbeidsmarkt, onderwijs en cyberweerbaar gedrag

De onderzoekslijn die ik hier als laatste noem draagt zorg voor aandacht op het gebied van cyberweerbaarheid in het curriculum van het onderwijs, voldoende gekwalificeerd personeel en duurzaam veilig digitaal gedrag thuis en op de werkvloer. We onderzoeken manieren om de cyberweerbaarheid van burgers, werknemers, inclusief kwetsbare groepen, te doen laten toenemen, wat op den duur bijdraagt aan een cyberweerbare samenleving. De focus ligt binnen deze lijn dus niet zozeer op het organisatie- en systeemniveau, maar op het niveau van het individu. Ik noem hieronder enkele voorbeelden van onderzoeken die lopen binnen deze lijn en van de onderwerpen waar we ons op willen richten.

Cyberweerbaarheid binnen het primair en voortgezet onderwijs

In de huidige digitale samenleving neemt de blootstelling van jongeren aan cybercriminaliteit snel toe. Hoewel nieuwe conceptkerndoelen voor digitale geletterdheid in maart 2024 zijn geïntroduceerd, blijft de aandacht voor het thema cyberweerbaarheid binnen het primair en voortgezet onderwijs (PO en VO) beperkt. Beschikbare lesprogramma's zoals Hackshield, Mijn Cyberrijbewijs en De Kiesraad worden nog onvoldoende benut, wat wijst op obstakels in de implementatie door scholen. Met praktijkgericht onderzoek levert het lectoraat inzichten in de factoren die de bereidheid van docenten beïnvloeden om cyberweerbaarheid structureel te borgen in het curriculum. Het doel is om barrières en motieven te identificeren die van invloed zijn op de handelingsbereidheid van docenten. Roel de Beer, Astrid van Erk en Renske Korenromp, allen (docent-)onderzoekers bij het lectoraat, onderzoeken daartoe waarom bestaande lesprogramma's beperkt worden ingezet en welke omstandigheden bijdragen aan effectieve integratie in het onderwijs.

Daarnaast loopt een pilot waarin jeugdagenten gastlessen over digitale criminaliteit verzorgen. Wij onderzoeken de impact van gastlessen op de kennis en het begrip van jeugdagenten over digitale criminaliteit. Ook kijken we of gastlessen leiden tot een verbetering van de connectie tussen jeugdagenten en jongeren vanuit het perspectief van de jeugdagenten. Beide projecten zijn onderdeel van een programma voor visievorming en beleidsafstemming binnen het PO en VO, getrokken door de Politie Oost-Brabant, waarin onder andere Kennisnet, Future NL, PO-VO Raad en Universiteit Utrecht participeren.

Voldoende gekwalificeerd personeel

Het benutten van de kansen voor het verhogen van de cyberweerbaarheid staat of valt met het kunnen beschikken over voldoende expertise. De NCTV (2024a) kopt zelfs: 'weerbaarheid in het geding door schaarse cybersecuritycapaciteit'. Naar verwachting blijft de vraag naar cybersecurity-expertise toenemen waarbij het aanbod van gekwalificeerd personeel achterblijft (NCTV, 2022). De verwachting is dat deze tekorten zullen toenemen vanwege ontwikkelingen rondom Europese wet- en regelgeving (Platform Talent voor Technologie & Dialogic, 2024; NCTV, 2024a). Ook door de verdere ontwikkeling en inzet van AI zullen nieuwe taken ontstaan en nieuwe competenties benodigd zijn, resulterend in een toenemende vraag naar cybersecurityprofessionals (zie ook NCTV, 2024a).

Van Deursen (2022) spreekt over een mismatch tussen vraag en aanbod als het gaat om cybersecuritytalent. De huidige aanwas voorziet niet in de bestaande en verwachte toekomstige vraag naar talent. Daar komt bij dat vaak te veel wordt gevraagd van de professional. Die moet kunnen acteren op alle drie de pijlers van cybersecurity: mens, proces en techniek. Dat is als zoeken naar het spreekwoordelijke schaap met vijf poten: dat bestaat niet. Een oplossingsrichting is het denken in cyberteams waarin verschillende functies geclusterd zijn, aldus Ruijsendaal in gesprek met Van Deursen (2022). Door cyberweerbaarheid integraal te benaderen creëer je breed draagvlak binnen organisaties voor de implementatie ervan. Door de werklast te verdelen wordt het werk bovendien behapbaar en daarmee ook duurzaam aantrekkelijker. Een andere oplossing zou kunnen zijn het delen van bepaalde functies tussen samenwerkende (kleinere) bedrijven. Kokkeler en collega's (2023, p. 19) noemen in dit verband 'shared functies', zoals een gedeelde CISO-rol, met de kanttekening dat het ook hier in de praktijk waarschijnlijk niet zal gaan om één persoon, maar om teams.

Ook Platform Talent voor Technologie en Dialogic (2024) doen in hun verkennend onderzoek over de Nederlandse cybersecurity-arbeidsmarkt aanbevelingen, maar laten tevens zien dat het totale ecosysteem van arbeidsmarkt en onderwijs omvangrijk en divers is. Er is dan ook geen uniforme oplossing die alle deelproblemen gaat oplossen.[77] Om zorg te dragen voor voldoende gekwalificeerd personeel, nu en in de toekomst, neemt het lectoraat deel aan diverse initiatieven, zoals de werkgroep Opleiden, Trainen en Oefenen (OTO) als onderdeel van het landelijk Cyberweerbaarheidsnetwerk (CWN)[78], de thematafel talentontwikkeling binnen het Brabant House of Cyber (HOC-B) en de Taskforce Cybersecurity, onderdeel van de Human Capital Agenda (HCA) ICT.

Veilig digitaal gedrag

In het cyberdomein lijkt het vaak alsof 'menselijke fouten' de oorzaak zijn van cyberincidenten. Maar is het echt zo eenvoudig? Dat het misgaat ligt niet per se aan de mens zelf. Zie hiervoor ook mijn blog van 4 maart 2024 op Dutch IT Leaders, over de rol van de mens in het veiligheidssysteem.[79]

Het nieuws staat vol met organisaties die slachtoffer zijn van een datalek. Zo heeft Pensioenfonds ABP in 2023 per ongeluk de e-mailadressen gelekt van 500 gepensioneerden. Het fonds spreekt van een 'menselijke fout'.[80] De e-mailadressen zijn ingevuld in het verkeerde veld, zegt het ABP. In plaats van in het zogeheten BCC-veld werden ze in het CC-veld ingevoerd. Bij BCC (*blind carbon copy*) kunnen de ontvangers niet zien wie de mail nog meer heeft gekregen, bij CC (*carbon copy*) is die lijst wel zichtbaar. Ook de GGD IJsselland had te maken met een datalek. Ook hier zijn, aldus de GGD door een menselijke fout de gegevens van 148 mensen, die in 2022 werden uitgenodigd voor een vaccin tegen de apenpokken, op straat komen te liggen.[81] Een medewerker stuurde per ongeluk de lijst met mensen die een uitnodiging krijgen voor een apenpokken-vaccinatie naar iemand buiten de organisatie. De mail was bedoeld voor een collega, maar werd per ongeluk verstuurd naar een verkeerd adres.

---

[77] Zie ook: Beslisnota bij Kamerbrief Human Capital Cybersecurity. https://www.tweedekamer.nl/downloads/document?id=2024D19329

[78] https://www.ncsc.nl/aansluiten-en-samenwerken/cyberweerbaarheidsnetwerk-cwn

[79] https://www.dutchitleaders.nl/blog/424598/fouten-maken-mag

[80] https://www.rtl.nl/tech/artikel/5388296/menselijke-fout-abp-mailadressen-lekken-abp-datalek-autoriteit

[81] https://www.oost.nl/nieuws/2134883/datalek-ggd-ijsselland-medewerker-stuurde-vaccinatie-lijst-apenpokken-per-ongeluk-naar-verkeerd-mailadres

Rapporten van Verizon hebben in de afgelopen jaren telkens vastgesteld dat de mens betrokken is bij meer dan 80% van datalekken wereldwijd (zie bijvoorbeeld Verizon, 2024). Het is een bekend feit dat bij veel cyberaanvallen het gedrag van werknemers wordt geëxploiteerd (Leukfeldt, 2014; Leukfeldt, Kleemans, & Stol, 2017). Ongeacht hoe veilig een systeem is, is de eindgebruiker vaak een kritieke achterdeur naar het netwerk (Bulgurcu, Cavusoglu, & Benbasat, 2009; Dodge, Carver, & Ferguson, 2007; Talib, Clarke, & Furnell, 2010). Aanvallers zoeken naar kwetsbaarheden om toegang te krijgen tot systemen; deze kunnen voortkomen uit gebruikers die risicovol gedrag vertonen, zoals het niet volgen van beleid of het onthullen van te veel persoonlijke informatie op sociale netwerksites. De mens is de zwakke schakel in cybersecurity, hoor je dan ook vaak. Als eindgebruikers nu eens goed zouden snappen waar de risico's liggen dan zou de organisatie een stuk minder kwetsbaar zijn voor allerhande cyberellende, zo is de gedachte bij veel securityteams.

Maar is het wel zo dat menselijke fouten verantwoordelijk zijn voor cyberincidenten zoals datalekken? Als je goed kijkt, is er vaak meer aan de hand. Want ja, mensen maken fouten, vergeten dingen en zijn daarmee een kritieke achterdeur naar het netwerk, maar wat veroorzaakt deze fouten? Eerder in deze rede noemde ik al de zogenoemde enkelvoudige en lineaire incidentmodellen (Ebert e.a., 2023). Enkelvoudige modellen schrijven incidenten toe aan één duidelijk omschreven gebeurtenis (bijvoorbeeld een aanval of een technische fout), terwijl lineaire modellen uitgaan van falen op meerdere (maar onderling verbonden) niveaus. Deze kijk op cybersecurity verklaart een succesvolle cyberaanval door deze toe te schrijven aan bijvoorbeeld het onveilige gedrag van een eindgebruiker, zoals een IT-beheerder die een cloudaccount verkeerd configureert. Of dus een medewerker die e-mailadressen invult in het verkeerde veld. Ondanks dat deze kijk op cybersecurity helaas nog veel in gebruik is, is al ruime tijd geleden aangetoond dat er betere modellen zijn om incidenten te verklaren (Zimmermann & Renaud, 2019). Incidenten hebben veelal geen enkele oorzaak, zoals een medewerker die e-mailadressen invult in het verkeerde veld, maar ontstaan door fouten op verschillende niveaus in het systeem.

Holistische modellen zijn nodig om de complexiteit in het ontstaan van incidenten te verklaren. Deze modellen nemen ook cultuur, beleid, procedures, management en de systemen die we gebruiken mee om te verklaren hoe incidenten ontstaan (Ebert e.a., 2023). Deze factoren vallen vaak niet onder de controle van mensen die het werk uitvoeren. Belangrijk is dat deze modellen menselijke fouten dan ook veelal uitsluiten als primaire bron van incidenten. Want de 'menselijke fout' blijkt meestal gewoon een fout die elders in het systeem ligt. En omdat we niet verder kijken dan menselijke fouten worden de werkelijke redenen van incidenten vaak niet aangepakt.

Security awareness als oplossing?

Vaak wordt beveiligingsbewustzijn, oftewel security awareness, gezien als oplossing voor menselijk falen. Security awareness is de mate waarin mensen risico's herkennen en zich ervan bewust zijn dat deze de veiligheid van te beschermen belangen in gevaar kunnen brengen.[82] Door goede praktijken of cyberveilig of -hygiënisch gedrag, zoals het gebruiken van sterke wachtwoorden en adequaat reageren op (bijna) incidenten, kunnen werknemers helpen de organisatie cyberweerbaarder te maken. Het vertellen aan mensen dat ze voorzichtiger moeten zijn, is echter niet de oplossing. Hoewel het redelijk is om van mensen te verwachten dat ze opletten en voorzichtig zijn, is het hierop vertrouwen niet voldoende om cyberrisico's te beheersen.

In een TED talk in 2023 tijdens het KPN SecureID event[83] mocht ik mijn visie geven op dit onderwerp: hoe gaan we van bewustzijn naar veilig gedrag? Veilig gedrag zou het doel moeten zijn. Niet het beveiligingsbewustzijn van medewerkers. Het is niet kennis die hackers buiten de deur houdt, maar veilig gedrag. We weten allang dat gedrag niet tot stand komt op basis van kennis alleen. Bijna iedereen weet wel dat groente en fruit goed voor ons zijn, maar toch eet lang niet iedereen ook daadwerkelijk de minimale voorgeschreven hoeveelheid. Ook op gebied van cybersecurity is deze kloof tussen kennis en gedrag aangetoond. Wetzer, gedragswetenschapper bij Secura, ontdekte dat mensen veelal zeggen dat ze zich veilig gedragen, bijvoorbeeld sterke wachtwoorden gebruiken, maar als je dan kijkt naar het daadwerkelijke gedrag, blijkt maar een klein gedeelte het ook echt te doen (zie ook Van der Kleij, Van 't Hoff-de Goede, Van de Weijer, & Leukfeldt, 2020).[84]

---

[82] Zie: Cybersecurity woordenboek: https://cyberveilignederland.nl/woordenboek
[83] TED Talk op NLSecure[ID] 24/01/2023: Het is tijd voor security awareness nieuwe stijl. https://youtu.be/ScgVOD2F5dg
[84] Zie bijvoorbeeld: https://www.secura.com/nl/services/mens/safe/analyzing-behavior-cyber-resilience

Er is meer nodig dan kennis alleen om veilig gedrag tot stand te laten komen. Eerder liet ik al zien dat ook motivatie en gelegenheid ertoe doen als het erop aankomt, bijvoorbeeld in de vorm van een veilige werksfeer. Zo'n sfeer ontstaat niet door mensen te straffen als ze op een verkeerde link klikken. Die negatieve benadering zorgt er vooral voor dat mensen incidenten niet meer melden, met alle gevolgen van dien. In plaats daarvan zouden organisaties het melden van incidenten moeten aanmoedigen. IT'ers hebben niet per definitie verstand van menselijk gedrag, laat staan dat ze gedragsverandering kunnen realiseren. Je vraagt mij als psycholoog toch ook niet om een computerprogramma te schrijven? Je moet mensen met een IT-achtergrond dan ook niet vragen om zich bezig te houden met gedragsvraagstukken (zie ook Van der Kleij, 2023).

De eenzijdige kijk op mensen waarmee beveiligingsbewustzijn wordt toegepast betekent automatisch dat andere belangrijke aspecten worden vergeten. Er bestaan immers technische- en organisatorische oplossingen die het delen van persoonsgegevens met personen buiten de organisatie voorkomen. Het ophogen van securitymaatregelen kan echter ook contraproductief werken stelt Van Rijsewijk, directeur Cyber Defense bij Thales. Hij betoogt dat we cybersecurity niet het probleem moeten maken van de eindgebruikers.[85]

'Een restrictief security-beleid zorgt uiteindelijk altijd voor olifantenpaadjes', is zijn mening. 'Een omgeving 100% dichtzetten is naast onmogelijk, ook gewoon onwenselijk. Het zorgt alleen maar voor meer frictie en ongewenst eigen initiatief van medewerkers.'

Oplossingen die het eindgebruikers makkelijk maken om veilig te werken zijn beter. Denk aan een applicatie die de gebruiker waarschuwt als deze op het punt staat om vertrouwelijke informatie te versturen. Deze feedback is cruciaal in dat het eindgebruikers helpt om de (negatieve) uitkomsten van hun actie te overzien en daarmee fouten te voorkomen. Dit feedbackmechanisme ontbrak vermoedelijk in de e-mailapplicatie van pensioenfonds ABP.

Iedereen maakt fouten. Hoe goed opgeleid en gemotiveerd we ook zijn. Dat mensen fouten maken, moeten we accepteren. De uitdaging is dus om fouttolerante systemen te ontwikkelen die rekening houden met de kenmerken

[85] https://www.techzine.nl/blogs/security/465326/maak-cybersecurity-niet-het-probleem-van-eindgebruikers/

en beperkingen van de menselijke onderdelen. Ik roep dan ook al jaren dat we niet meer security awareness nodig hebben bij de eindgebruikers, maar meer human awareness bij de securityteams.[86] [87]

Cyberweerbaarheid van kwetsbare groepen

Onderzoek naar de cyberweerbaarheid van groepen met een licht verstandelijke beperking (lvb) is van groot belang vanwege hun verhoogde kwetsbaarheid in de digitale wereld. Deze groep loopt niet alleen het risico slachtoffer te worden van cybercriminaliteit, maar wordt ook regelmatig geronseld door criminelen voor illegale activiteiten.[88]

Mensen met een lvb hebben vaak moeite met het begrijpen van complexe digitale omgevingen en herkennen daardoor minder snel cyberdreigingen, zoals phishing, online fraude of manipulatieve berichten. Ze kunnen hierdoor gemakkelijker worden misleid, wat leidt tot financiële schade, identiteitsdiefstal of andere vormen van uitbuiting. Daarnaast zien we dat criminelen soms bewust gebruik maken van de zwakke cyberweerbaarheid van deze groep door hen te ronselen voor illegale praktijken. Een voorbeeld hiervan is het inzetten van mensen met een lvb als 'geldezels', waarbij hun bankrekeningen worden gebruikt voor het witwassen van geld.[89] De gevolgen hiervan zijn vaak ernstig: de betrokkenen worden strafrechtelijk vervolgd, terwijl ze zich vaak niet volledig bewust zijn van de implicaties van hun handelingen.

Cybersecuritymaatregelen zijn veelal niet afgestemd op de specifieke behoeften van kwetsbare groepen. Onderzoek naar deze doelgroep helpt bij het creëren van een meer inclusieve digitale samenleving, waarin ook mensen met een lvb ten volle kunnen profiteren van deelname aan de digitale samenleving, vrij van zorgen over cyberrisico's. Door praktijkgericht en transdisciplinair onderzoek wil Astrid van Erk, docent-onderzoeker bij het lectoraat, interventies ontwikkelen om mensen met een lvb beter te beschermen tegen cyberdreigingen. Dit kan bijvoorbeeld door het aanbieden van laagdrempelige educatieprogramma's, ook voor de begeleiders van mensen met een lvb en duidelijke richtlijnen voor digitale veiligheid en systemen die vroegtijdig signalen van misbruik herkennen.

[86] https://www.infosequre.com/nl/ons-cybergedrag-is-veel-onveiliger-dan-we-zelf-denken
[87] https://www.securitymanagement.nl/cybersecurity-is-meer-dan-technologie-alleen/
[88] Zie bijvoorbeeld: https://www.kenniscentrumlvb.nl/themas/risicos-lvb/dossier-criminaliteit-lvb/
[89] Zie bijvoorbeeld: https://www.websitevoordepolitie.nl/zorg-voor-kwetsbare-geldezels/

Onderzoeksvragen

Relevante onderzoeksvragen binnen deze onderzoekslijn zijn:

- Hoe lossen we de mismatch op tussen vraag en aanbod als het gaat om cybersecuritytalent?
- Hoe stimuleren we digitaal veilig gedrag en overwinnen we belemmerende overtuigingen thuis en op de werkvloer?
- Hoe kunnen we via gedragsinterventies lvb-groepen cyberweerbaarder maken?
- Welke rol spelen begeleiders van mensen met een lvb bij het cyberweerbaarder maken van deze groep?

Dankwoord

Graag wil ik aan het einde van mijn rede een aantal mensen bedanken. Ik dank allereerst het College van Bestuur van Avans Hogeschool en het Centre of Expertise Veiligheid & Veerkracht (CoE V&V) voor het in mij gestelde vertrouwen. In het bijzonder dank ik Nienke Fabries, directeur van het CoE V&V, en Jacomine Ravensbergen, toenmalig voorzitter van het College van Bestuur, voor hun inspanningen om het lectoraat Cyberweerbare Organisaties te realiseren. Daarnaast wil ik de bestuurders van de Academies, Diensteenheden en Centres of Expertise die ik de afgelopen periode heb gesproken, bedanken voor hun bijdragen, direct of indirect, aan het formuleren van mijn leeropdracht.

Ik ben dankbaar voor de kansen die ik heb gekregen en de steun die ik heb ontvangen van TNO. De kennis en ervaring die ik hier heb opgedaan, hebben een solide basis gelegd voor het lectoraat. Het voert te ver om iedereen daar te benoemen, maar in ieder geval wil ik bedanken: Hans van den Broek, Inge van der Beijl, Tessa Bruijne, Peter Essens, Patrick de Graaf, Dianne van Hemert, Dimitri Hehanussa, Tineke Hof, Karel van Houten, Jose Kerstholt, Allard Kernkamp, Tjarda Krabbendam-Hersman, Sico van der Meer, Bert Jan te Paske, Tom van Schie, Jan Maarten Schraagen, Lotte Schuilenborg, Berry Vetjens, Reinder Wolthuis, Sjoerd Jan Wiarda, Remco Wijn en Heather Young.

Ik kan het niet alleen. Ik ben ontzettend veel dank verschuldigd aan mijn kenniskringleden: Bert Bambach, Roel de Beer, Peter van Eck, Astrid van Erk, Femke Knaapen-Liebreks, Renske Korenromp, Jan Otten, Esger ten Thij en Jim van Zon. Samen zijn we aan de slag gegaan met het formuleren van de leeropdracht en de onderzoekslijnen binnen het lectoraat met een prachtig resultaat. Ik had me geen beter team kunnen wensen.

Ook alle andere directe collega's binnen Avans Hogeschool wil ik bedanken voor de fijne samenwerking. Ik noem in het bijzonder de lectoren: Amarante Böttger, Bart Claes, Janine Janssen, Ingrid Janssen, Ander de Keijzer, Ben Kokkeler, Ron Meelen (ai), Julien van Ostaaijen, Teun van Ruitenburg, Henk Spies en de associate lectoren Peter Novitzky en Thom Snaphaan. Daarnaast wil ik mijn waardering uitspreken voor de ondersteuners van het CoE V&V, die altijd voor mij klaarstaan, vooral Morena Brouwers, Lisette Klaassen, Reyhana Stevels, Suzanne de Winter en Annette Zonnenberg.

Samenwerking is essentieel om de cyberweerbaarheid in Nederland naar een optimaal niveau te brengen. Hierbij wil ik dan ook graag alle opdrachtgevers, samenwerkings- en netwerkpartners bedanken voor het werk wat we de afgelopen periode al hebben gedaan en de komende tijd en daarna zullen verrichten. Ik noem in het bijzonder Jel Bedaux, Piet Bel, Eddy Boot, Harm de Bruin, Karijn van Doorne, Hendrik-Jan van Engelen, Edwin Franse, Bas Goddrie, Evi Gimbrère, Rens Lambert, Guido Leestemaker, Sten Meijer, Claudia van Orden, Paul Samwel, Onno Sidler en Mieke Zijlstra. Het gaat hierbij niet alleen om het werkveld, zoals gemeenten, belangenorganisaties en private organisaties, maar ook om partners van kennisinstellingen. In deze laatste categorie wil ik Jurjen Jansen, Rutger Leukfeldt en Remco Spithoven, samen met hun kenniskring, specifiek benoemen. Met hen zijn we een duurzame samenwerking aangegaan in het SPRONG Expertisenetwerk Cyberweerbaar NL.

Rutger heeft mij, in de tijd dat ik bij De Haagse Hogeschool werkte, de ruimte gegeven om op zoek te gaan naar het antwoord op de vraag 'hoe de psychologie kan bijdragen aan het vergroten van de cyberweerbaarheid van burgers en bedrijven'. Een groot deel van dat antwoord heeft u terug kunnen vinden in deze rede. Ik heb vanaf 2018 ruim vier jaar, naast mijn werk bij TNO, met veel plezier gewerkt in het lectoraat van Rutger. Het voert te ver om ook iedereen daar te benoemen, maar in ieder geval wil ik bedanken voor de samenwerking: Michele Ancher, Luuk Bekkers, Jelle Groenendaal, Susanne van 't Hoff-de Goede, Iris Meerts, Daniel Meinsma, Fred van Noord, Marco Romagna, Marcel Spruit en Maaike Vergeer.

Tot slot mijn familie en vrienden: heel fijn dat jullie erbij zijn om dit moment met mij te delen. Bedankt voor jullie gezelligheid, steun en begrip gedurende het schrijven van deze rede. En de Ardennen-vrienden: ik zie alweer uit naar de volgende editie.

Ik heb gezegd.

Referenties

ABI Research. (2019). *The Industrial Revolution: Top Trends and Takeaways from Hannover Messe 2019*. New York, USA: ABI Research.

Adviesraad voor het Wetenschaps- en Technologiebeleid. (2007). *Alfa en Gamma stralen. Valorisatiebeleid voor de Alfa- en Gammawetenschappen*. Den Haag: AWT. Geraadpleegd op https://www.awti.nl/binaries/awti/documenten/adviezen/2007/3/15/alfa-en-gamma-stralen/a70.pdf

Akkermans, M., Derksen, E., Kennis, M., Kloosterman, R., & Moons, E. (2024). *Veiligheidsmonitor 2023*. Den Haag: CBS. Geraadpleegd op https://www.cbs.nl/nl-nl/longread/rapportages/2024/veiligheidsmonitor-2023/5-online-criminaliteit

Akkermans, M., Kloosterman, R., Moons, E., Reep, C., & Tummers-van der Aa, M. (2022). *Veiligheidsmonitor 2021*. Den Haag: CBS. Geraadpleegd op https://www.cbs.nl/nl-nl/longread/rapportages/2022/veiligheidsmonitor-2021

Algemene Inlichtingen- en Veiligheidsdienst & Rijksinspectie Digitale Infrastructuur. (2024). *Generatieve AI: een transformatieve impact op cybersecurity*. Den Haag: AIVD. Geraadpleegd op https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2024/10/17/generatieve-ai.-een-transformatieve-impact-op-cybersecurity/Generatieve+AI.+Een+transformatieve+impact+op+cybersecurity.pdf

Allianz. (2024). *Allianz Risk Barometer: Identifying the major business risks for 2024*. München, Duitsland: Allianz Commercial. Geraadpleegd op https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

Appelbaum, S. H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. *Management decision*, *35*(6), 452-463.

Arizon-Peretz, R., Hadar, I., & Luria, G. (2022). The importance of security is in the eye of the beholder: Cultural, organizational, and personal factors affecting the implementation of security by design. *IEEE Transactions on Software Engineering, 48*(11), 4433-4446.

Assibi, A.T. (2023). Literature Review on Building Cyber Resilience Capabilities to Counter Future Cyber Threats: The Role of Enterprise Risk Management (ERM) and Business Continuity (BC). *Open Access Library Journal*, *10*(4), 1-15.

Boin, A., Linck, R., Van Duin, M., Hendriks, J., Berger, E., & Van der Varst, L. (2020). *Versterken van de veerkracht: Naar een gezamenlijke aanpak van ongekende crises*. Arnhem/Zoetermeer: Nederlands Instituut Publieke Veiligheid.

Bostick, T. P., Connelly, E. B., Lambert, J. H., & Linkov, I. (2018). Resilience Science, Policy and Investment for Civil Infrastructure. *Reliability Engineering & System Safety, 175*, 19-23.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *EMCIS2009, Proceedings of the European and Mediterranean Conference on Information Systems* (pp. 419–430).

Centraal Bureau voor de Statistiek. (2023). *Cybersecuritymonitor 2023*. Den Haag: CBS. Geraadpleegd op https://www.cbs.nl/nl-nl/longread/rapportages/2024/cybersecuritymonitor-2023

Collier, Z., Hassler, M., Lambert, J., DiMase, D., & Linkov, I. (2019). Supply chains. In A. Kott & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks, Risk, Systems and Decisions*. New York, USA: Springer International Publishing.

Cyberweerbaar NL. (2024). *Naar een cyberweerbaar Nederland. Onderzoeksagenda voor praktijkgericht onderzoek*. Expertisenetwerk Cyberweerbaar NL.

Da Veiga, A., & Eloff, J. H. (2007). An information security governance framework. *Information systems management, 24*(4), 361-372.

De Bruin, B., & Van Summeren, F. (2024). Security innovation Stories. Vught: Beyond Products BV.

De Jong, G., Koeman, N., Konijn, S., Volberda, H., & Hollen, R. (2023). *Nederlandse Innovatie Monitor 2023: Oververhitting in het Nederlandse Innovatielandschap*. Rapport 2023-95. Amsterdam: SEO Economisch Onderzoek.

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

Dijkgraaf, R. (2012, 15 december). Kennisboom. *NRC*.

Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers & Security, 26*(1), 73-80.

Drenth, A., & Hendriks, K. (2024, 8 juli). *De mens in cybersecurity: lastpak of oplossing?* Weblogbericht NCSC. Geraadpleegd van https://www.ncsc.nl/actueel/weblog/weblog/2024/de-mens-in-cybersecurity-lastpak-of-oplossing

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. *Journal of Risk Research, 26*(7), 801-814. doi:10.1080/13669877.2023.2208146

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity, 5*(1), 1-17.

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, E.R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & security*, *132*, 103372.

Ebert, N., Schaltegger, T., Ambuehl, B., Schöni, L., Zimmermann, V., & Knieps, M. (2023). Learning from safety science: A way forward for studying cybersecurity incidents in organizations. *Computers & Security*, 103435.

Eenheid Landelijke Opsporing en Interventies & Eenheid Landelijke Expertise en Operaties. (2024). *Online fraude in beeld: Fenomeenbeeld Online fraude 2024*. Zoetermeer: Politie.

Eken, M., Lucas. R., Hoorens, S., & Nederveen, F. (2024). *Strengthening societal resilience. A perspective on strategic priorities for the Netherlands amidst geopolitical tensions.* RAND Europe.

Emerce. (2024, 5 februari). *Cyber Security Raad aan nieuw kabinet: Nederland moet meer investeren in digitale veiligheid*. Geraadpleegd op https://www.emerce.nl/wire/cyber-security-raad-nieuw-kabinet-nederland-moet-meer-investeren-digitale-veiligheid

Eshuis, N. (2022, 3 oktober). Diefstal van fietsen met 735 duizend per jaar veel hoger dan gedacht: vooral goedkope fietsen gestolen. *De Volkskrant*.

Europese Unie. (2022). *Digital Economy and Society Index (DESI)*. Geraadpleegd op https://ec.europa.eu/newsroom/dae/redirection/document/88764

Gisladottir, V., Ganin, A., Keisler, J., Kepner, J., & Linkov. I. (2017). Resilience of cyber systems with over-and underregulation. *Risk Analysis, 37*(9), 1644-1651.

Grøtan, T. O., Antonsen, S., & Haavik, T. K. (2022). Cyber resilience: a pre-understanding for an abductive research agenda. In F. Matos, P. M. Selig & E. Henriqson (Eds.), *Resilience in a Digital Age: Global Challenges in Organisations and Society* (pp. 205-229). Cham: Springer International Publishing.

Häring, I., Ebenhöch, S., & Stolz, A. (2016). Quantifying resilience for resilience engineering of socio technical systems. *European Journal for Security Research*, *1*, 21-58.

Hatami, H., & Segel, L. (2023, April 6). *Six CEO priorities for 2023*. McKinsey & Co. https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/six-ceo-priorities-for-2023.

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? *International journal of management reviews, 23*(1), 7-44.

Hiscox. (2023). *Hiscox Cyber Readiness Report*. Pembroke, Bermuda: Hiscox Ltd. Geraadpleegd op https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf

Hof, T., Van der Kleij, R., & Mergler, S. (2024). *Veilig digitaal ondernemen: Inzicht in motivaties en barrières door doelgroepsegmentatie*. Den Haag: TNO.

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

Hollnagel, E. (2018). *Safety-I and safety-II: the past and future of safety management.* CRC press.

Hollnagel, E. (2021). Erik Hollnagel homepage. Geraadpleegd op https://erikhollnagel.com/ideas/resilience-engineering.html

Hollnagel, E. (2022). Systemic potentials for resilient performance. In F. Matos, P. M. Selig & E. Henriqson (Eds.), *Resilience in a digital age: Global challenges in organisations and society* (pp. 7-17). Cham: Springer International Publishing.

Hynes, W., Trump, B., Love, P., & Linkov, I. (2020). Bouncing forward: A resilience approach to dealing with COVID-19 and future systemic shocks. *Environment Systems and Decisions*, *40*, 174-184.

IBM. (2024). *Cost of a Data Breach Report 2024*. USA: IBM Corporation.

Jansen, J. (2023). *Digitale weerbaarheid van mens en organisatie: De kracht van verbinding* (Inaugurale rede). Leeuwarden: NHL Stenden.

Kokkeler, B., Van den Oord, S., Ten Thij, E., & Vollenberg, Q. (2023). *Sterke schakels versterken de keten: Een ontwerponderzoek naar samenwerking in de keten tussen high tech MKBs op gebied van cybersecurity*. Den Bosch: Avans Hogeschool.

Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *IEEE Computer, 54*(2), 80-85.

Krauwer, J. (2024). *Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker* (Sectorrapport 2024). ABN AMRO. Geraadpleegd op https://www.abnamro.nl/nl/media/202404_Steeds-verfijndere-cyberaanvallen_tcm16-228031.pdf

Kuhn, T. S. (1962). The Structure of Scientific Revolutions (1st ed.). Chicago, USA: University of Chicago Press, Ltd.

Leavitt, H. J. (1964). *Managerial Psychology: An introduction to individuals, pairs and groups in organizations.* Chicago, USA: The University of Chicago Press, Ltd.

Leigh, D. (2023, March 14). 60% of SMEs that suffer a cyber attack go out of business within six months. *TechRound*. Geraadpleegd op https://techround.co.uk/news/60-of-smes-that-suffer-a-cyber-attack-go-out-of-business-within-six-months/.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551-555.

Leukfeldt, E. R. (2024). *Meer dan alleen een goed idee: Naar een empirisch onderbouwde aanpak van cybercrime* (Inaugurale rede). Universiteit Leiden.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). A typology of cybercriminal net-works: from low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21-37.

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. *Cyber resilience of systems and networks*, 1-25.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., ... Thiel-Clemen, T. (2014). Changing the resilience paradigm. *Nature Climate Change, 4*, 407–409.

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., Flynn, S. E., & Seager, T. P. (2013). Measurable Resilience for Actionable Policy. *Environmental Science and Technology, 47*(18), 10108-10110.

Linkov, I., Ligo, A., Stoddard, K., Perez, B., Strelzoffx, A., Bellini, E., & Kott, A. (2023). Cyber Efficiency and Cyber Resilience. Complementary objectives competing for the same resources. *Communications of the ACM, 66*, 4, 33–37. https://doi.org/10.1145/3549073

Lucas, J. (2022, 18 november). Cybercrime kost bedrijfsleven veel meer dan in andere landen. *BNR*. Geraadpleegd op https://www.bnr.nl/nieuws/technologie/10494716/cybercrime-kost-bedrijfsleven-veel-meer-dan-in-andere-landen

Matos, F., Tonial, G., Monteiro, M., Selig, P. M., & Edvinsson, L. (2022). Relational Capital and Organisational Resilience. In F. Matos, P. M. Selig & E. Henriqson (Eds.), *Resilience in a Digital Age: Global Challenges in Organisations and Society* (pp. 39-58). Cham: Springer International Publishing.

Meyer, R., & Kunreuther, H. (2017). *The Ostrich paradox: Why we underprepare for disasters.* Pennsylvania, USA: Wharton digital press.

Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science*, *6*, 1-12.

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreiging en versterking van weerbaarheid*. Den Haag: Rathenau Instituut. https://www.rathenau.nl/nl/digitale-samenleving/een-nooit-gelopen-race

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2021). *Cybersecuritybeeld Nederland 2021* (CSBN 2021). Den Haag: Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.nctv.nl/binaries/nctv/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021/CSBN2021_def_interactieve+pdf_web.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2021). *Cybersecuritybeeld Nederland 2021* (CSBN 2021). Den Haag: Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.nctv.nl/binaries/nctv/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021/CSBN2021_def_interactieve+pdf_web.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2022). *Nederlandse Cybersecuritystrategie 2022-2028. Ambities en acties voor een digitaal veilige samenleving*. Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.nctv.nl/binaries/nctv/documenten/publicaties/2022/10/10/nederlandse-cybersecuritystrategie-2022-2028/Nederlandse+Cybersecuritystrategie+2022-2028.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2023a). *Cybersecuritybeeld Nederland 2023* (CSBN 2023). Den Haag: Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.nctv.nl/binaries/nctv/documenten/publicaties/2023/07/03/cybersecuritybeeld-nederland-2023/CSBN2023.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2023b). *De Veiligheidsstrategie voor het Koninkrijk der Nederlanden*. Den Haag: Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden/Veiligheidsstrategie+voor+het+Koninkrijk+der+Nederlanden.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2024a). *Cybersecuritybeeld Nederland 2024* (CSBN 2024). Den Haag: Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.nctv.nl/binaries/nctv/documenten/publicaties/2024/10/28/cybersecuritybeeld-nederland-2024/CSBN+2024+A4+-+Webversie+DEF+-+kopie.pdf

Nationaal Coördinator Terrorismebestrijding en Veiligheid. (2024b). *Weerbaarheidsopgave: Versterken van weerbaarheid in het licht van militaire en hybride dreigingen*. Den Haag: Ministerie van Justitie en Veiligheid. Geraadpleegd op https://www.rijksoverheid.nl/onderwerpen/dreiging-in-nederland

National Research Council. (2012). *Disaster Resilience: A National Imperative*. Washington D.C., USA: The National Academies Press.

Nederveen, F., Hoorens, S., Frinking, E., & Soest, H. V. (2023). *Weerbaarheid becijferd: Een methode om weerbaarheid tegen dreigingen voor de nationale veiligheid inzichtelijk te maken*. RAND Europe.

Niinistö, S. (2024). *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*. European Commission. Geraadpleegd op https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en

Openbaar Ministerie en Politie Nederland. (2024). *Cybercrimebeeld Nederland 2024*. Geraadpleegd op https://fts.politie.nl/cybercrimebeeld/

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

Platform Talent voor Technologie & Dialogic. (2024). *Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity*. Geraadpleegd op https://open.overheid.nl/documenten/c0ac3595-28e3-43df-aa85-7d9e8a426c25/file

Pot. F. (2009). *Sociale innovatie als inspiratie* (Inaugurale rede). Radboud Universiteit Nijmegen.

Pot. F. (2012). Sociale innovatie: historie en toekomstperspectief. *Tijdschrift voor Arbeidsvraagstukken, 28*(1), 6-21. https://doi.org/10.5117/2012.028.001.006

Qureshi, Z. H. (2008). *A review of accident modelling approaches for complex critical sociotechnical systems* (Report DSTO-TR-2094). Australia: Defence Science and Technology Organisation.

Roelofsma, P. (2024). *Cascade Cyber Risk Management: Between Rule and Reality* (Lectorale rede). Den Haag: Haagse Hogeschool. Geraadpleegd op https://www.thuas.com/media/inaugural-lecture-peter-roelofsma

Rorive, K., Goedhart, W., Gloudemans, R., Spitteler, M., Breedijk, F., Leeuwerik, M., Rhuggernaath, S., & Krul., J. (2024). *Raak niet verdwaald in de cyberveiligheidsketen.* Managed Service Provider Information Sharing & Analysis Centre.

Ross, R., Pillitteri, V., Graubart. R., Bodeau, D., & McQuaid, R. (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* (NIST Special Publication 800-160 Vol. 2, Revision 1). https://doi.org/10.6028/NIST.SP.800-160v2r1.

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

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 1-20.

SANS. (2023). *Managing human risk: Security awareness report*. Bethesda, USA: SANS Institute, Security Awareness Division.

Sarker, P., & Lester, H. D. (2019). Post-disaster recovery associations of power systems dependent critical infrastructures. *Infrastructures, 4*(2), 30.

Senge, P. M. (2006). *The fifth discipline: The art and practice of the learning organization*. Broadway Business.

Simon, B. (2019). Everything You Need to Know about the People, Process, Technology Framework. Geraadpleegd op https://www.smartsheet.com/content/people-process-technology.

Stratix. (2024). *Digitale weerbaarheid in ecosystemen*. Hilversum.

Taleb, N. (2012). *Antifragile: Things That Gain from Disorder*. Penguin Books.

Talib, S., Clarke, N.L., & Furnell, S.M. (2010). An analysis of information security awareness within home and work environments. In: *Proceedings of the International Conference on Availability, Reliability, and Security* (pp. 196-203).

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

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

Van der Kleij, R. (2023). Herstel de mens als sterkste schakel. *Cyber Security Perspectives, 9*, 57-61.

Van der Kleij, R. (2024, zaterdag 14 september). Ons land is echt minder cyberweerbaar dan we denken. Opinie. *BN DeStem*. 12-13.

Van der Kleij, R., & Hof, T. (2024). Why Do Organizations Fail to Practice Cyber Resilience? In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust*. HCII 2024. Lecture Notes in Computer Science, vol 14728. Springer, Cham. https://doi.org/10.1007/978-3-031-61379-1_9

Van der Kleij, R. Kleinhuis, G., & Young, H. (2017). Computer Security Incident Response Team Effectiveness: A Needs Assessment. *Frontiers in Psychology*. doi: 10.3389/fpsyg.2017.02179.

Van der Kleij, R., & Leukfeldt, E. R. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. In T. Ahram & W. Karwowski (Eds.), *Advances in Human Factors in Cybersecurity*. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960. Springer, Cham. https://doi.org/10.1007/978-3-030-20488-4_2

Van der Kleij, R., Van Hemert, D., Te Paske, B. J., & Rooijakkers, T. (2024). Human-centric security engineering: Towards a research agenda. *AHFE International. Human Factors in Design, Engineering, and Computing, Vol. 159*, 2024, 1–10.

Van der Kleij, R., Van 't Hoff - de Goede, S., Van de Weijer, S., & Leukfeldt, E. R. (2020). Ons cybergedrag is veel onveiliger dan we zelf denken: Implicaties voor effectief beïnvloedingsbeleid door de overheid. *Justitiële Verkenningen, 46*(2), 113-128.

Van der Kleij, R., Wijn, R., & Hof, T. (2020). An application and empirical test of the Capability Opportunity Motivation-Behaviour model to data leakage prevention in financial organizations. *Computers & Security, Vol. 97.* 101938.

Van Deursen, J. (2022). Interview Mark Ruijsendaal (HSD) over tekort aan security specialisten: 'Stop met zoeken naar schaap met de vijf poten'. *IB Magazine, 22* (2), 4-6.

Van Deursen, J., & Altawekji, A. (2023). *Cyberdreigingsbeeld 2023: Onderwijs en onderzoek*. Utrecht: Security Expertise Centrum, SURF.

Van Harmelen, A-L. (2022). *Veerkracht bestaat niet* (Inaugurale rede). Universiteit Leiden.

Van Rijsewijk, R. (2016). *Cyberrisico als kans: Strategisch cyberrisicomanagement in het informatietijdperk*. Den Haag: Koninklijke Boom uitgevers.

Vergouwe, R. (2014). *De veiligheid van Nederland in kaart* (Eindrapportage VNK). Den Haag: Ministerie van Infrastructuur en Milieu. Geraadpleegd op https://zoek.officielebekendmakingen.nl/blg-450816.pdf

Verizon. (2024). *Data breach investigation report.* New York: USA. Geraadpleegd op https://www.verizon.com/business/resources/Tefd/reports/2024-dbir-data-breach-investigations-report.pdf

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

Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature, 533*(7602), 164–167. Geraadpleegd op https://www.nature.com/articles/533164a

Wetenschappelijke Raad voor het Regeringsbeleid. (2024). *Nederland in een fragmenterende wereldorde*, WRR-Rapport 109, Den Haag: WRR.

Wlodarczak, P. (2017). Cyber Immunity - A Bio-Inspired Cyber Defense System. In I. Rojas & F. Ortuño (Eds.), *IWBBIO, Part II*. (pp. 199–208). https://doi.org/10.1007/978-3-319-56154-7_19

World Economic Forum. (2024). *Unpacking Cyber Resilience* (White paper). Geraadpleegd op https://www3.weforum.org/docs/WEF_Unpacking_Cyber_Resilience_2024.pdf

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187.

Over Rick van der Kleij

(*Beeld: Rick Wink*)

Rick van der Kleij (1973) studeerde Cognitieve Psychologie aan de Vrije Universiteit in Amsterdam en Industrieel Ontwerpen aan de TU Delft. Hij promoveerde in 2007 bij de vakgroep Arbeids- en Organisatiepsychologie aan de Universiteit van Amsterdam op een proefschrift over virtuele teams. Sinds 1 januari 2024 is hij lector van het lectoraat Cyberweerbare Organisaties bij het Centre of Expertise Veiligheid & Veerkracht, Avans Hogeschool. Door praktijkgericht onderzoek vanuit een breed perspectief uit te voeren, waarbij mens, proces en technologie in samenhang worden meegenomen, levert hij een bijdrage aan optimaal niveau van cyberweerbaarheid voor het Nederlandse bedrijfsleven. Zodat zij ten volle kan profiteren van deelname aan de digitale samenleving, vrij van zorgen over cyberrisico's. Naast zijn werk als lector bij Avans Hogeschool is hij sinds 1998 wetenschappelijk onderzoeker bij TNO.

Colofon

Dit is een uitgave van het Centre of Expertise Veiligheid & Veerkracht,
Avans Hogeschool.

Uitgegeven ter gelegenheid van de lectorale rede van dr. Rick van der Kleij.

ISBN 9789465260266

NUR 800 - Bedrijfskunde algemeen

Redactie en coördinatie
Femke Knaapen-Liebreks en Reyhana Stevels

Druk en vormgeving
De Bondt Grafimedia Communicatie
Milieuvriendelijk geproduceerd op ongestreken, 100% hergebruikt papier.

www.veiligheidenveerkracht.nl

SecretariaatVenV@avans.nl