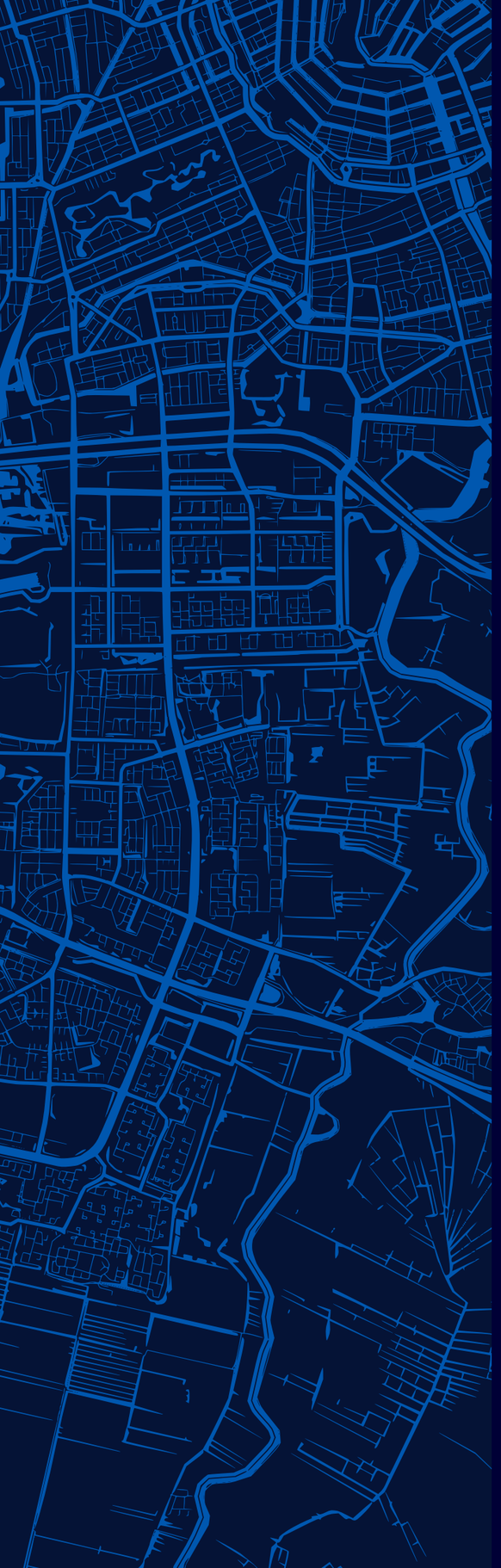
Trends in Veiligheid 2026

Digitale veiligheid & dienstbaarheid

Capgemini



Digitale veiligheid & dienstbaarheid

- Een strategische visie op vijf maatschappelijke kernvragen 02

Burger Centraal

- **Interview:** “Digitalisering mag nooit ten koste gaan van de menselijke maat” 06
- Van cel naar samenleving: hoe overheidsorganisaties samen veiligheid en perspectief creëren door werk in detentie 10
- Van beleid naar betekenis 15
- Bestuurlijke grip op digitale risico’s: sturen, kaderen en toetsen 20

Data

- **Interview:** Grenzen aan datagedreven politiewerk 24
- Evidence-based werken als kompas in een AI-gedreven veiligheidsdomein 30
- Voor wie werkt jouw model nou eigenlijk? 36
- Data Mesh bij Defensie: dataproducten voor een effectieve krijgsmacht 42
- Enterprise Agentic Intelligence voor het veiligheidsdomein 48

Toekomst van werk

- **Interview:** De toekomst van werk in het veiligheidsdomein vraagt om andere keuzes 54
- Humanoids als toekomst van de strafrechtketen: de nieuwe collega op straat 58
- Een wankel kaartenhuis: Waarom AI-innovatie geen ROI oplevert 65
- Cyber Resilience Act: Nieuwe spelregels voor digitale veiligheid bij publieke veiligheidsorganisaties 72

Weerbaarheid

- **Interview:** “Weerbaarheid begint niet bij technologie, maar bij mensen” 82
- Kan je weerbaar zijn zonder censuur? 84
- Regie voeren in een weerbarstig ecosysteem 90
- Hoe soeverein wil je zijn? 94

Wendbaarheid

- Buiten de gebaande paden is het veiliger 98
- Effectieve AI voor continue weerbaarheid en compliance 104

Digitale veiligheid & dienstbaarheid

Een strategische visie op vijf maatschappelijke kernvragen

Trends in Veiligheid 2026 schetst een veiligheidsdomein dat onder hoge druk staat door digitalisering, maatschappelijke polarisatie, digitaliserende criminaliteit en toenemende afhankelijkheden in ketens. De rode draad door alle artikelen is dat veiligheid steeds meer draait om menselijke legitimiteit, digitale weerbaarheid, slimme inzet van technologie en ketensamenwerking. Organisaties moeten wendbaar en betrouwbaar zijn en altijd kunnen uitleggen wat ze doen. Een flinke opgave, zeker als je bedenkt dat de risico's sneller toenemen dan ons vermogen om ze te beheersen.

Burger centraal

De relatie tussen overheid en burger verandert ingrijpend. Burgers verwachten dat publieke organisaties altijd bereikbaar, toegankelijk en betrouwbaar zijn, en dat zij deze organisaties kunnen benaderen via het kanaal dat bij hen past. In het interview met Jolanda Aalbers wordt duidelijk dat digitalisering hierin leidend is, maar dat de rol van traditionele kanalen nog niet is uitgespeeld. Miljoenen burgers vinden de politie inmiddels digitaal, terwijl traditionele kanalen zoals telefonie óók blijven groeien. Nieuwe digitale mogelijkheden vervangen de bestaande contacten dus niet. Ze brengen ons juist in contact met nieuwe groepen. Jongeren bellen bijvoorbeeld nauwelijks nog. Voor hen is digitale dienstverlening essentieel.

Aalbers benadrukt dat digitalisering nooit een doel op zich mag worden. Technologie moet ruimte creëren voor menselijk contact, niet andersom. De menselijke maat blijft het uitgangspunt. Innovaties zoals videobellen, digitale loketten en meertalige politieloketten helpen om dienstverlening toegankelijker te maken, maar fysieke nabijheid blijft essentieel in situaties waarin context, emotie of specialistische kennis een rol spelen. De strategie "digitaal intelligent, fysiek excellent" onderstreept dat technologie vooral moet bijdragen aan vertrouwen, verbinding en vakmanschap.

Ook binnen detentie staat de burger centraal. Het artikel *Van cel naar samenleving laat* zien hoe werk en leren bijdragen aan rust, veiligheid en perspectief. Door gedetineerden een zinvolle dagbesteding te bieden, vakmanschap te laten ontwikkelen en opdrachten te laten uitvoeren die aansluiten op kansrijke beroepen, ontstaat een leefklimaat dat zowel binnen als buiten de muren effect heeft. Het motto: "binnen beginnen om buiten te blijven".

Op hetzelfde moment worstelt de strafrechtketen met doorlooptijden en uitvoerbaarheid. In het artikel *Van beleid naar betekenis* wordt de keten beschreven als een ecosysteem van organisaties die in wisselende allianties samenwerken. De Algemene Rekenkamer constateert dat doorlooptijden in strafzaken te lang zijn, mede doordat organisaties vaak handelen vanuit hun eigen belang in plaats van het ketenbelang. Nauwere samenwerking is dus geboden. Deze samenwerking is gebaseerd op inzicht in spanningen tussen waarden, een gedeelde visie op wat de keten moet opleveren en een gedeelde aanpak waarin zowel burgers als professionals centraal staan.

Organisaties moeten wendbaar en betrouwbaar zijn en altijd kunnen uitleggen wat ze doen.

Data

De digitalisering van criminaliteit en samenleving maakt dat data een steeds grotere rol spelen in het veiligheidsdomein. In het interview met Ruud Staijen wordt duidelijk dat datagedreven politiewerk alleen effectief is wanneer het verantwoord, uitlegbaar en proportioneel wordt ingezet. De essentie van datagedreven werken is niet het verzamelen van zoveel mogelijk data, maar het combineren van signalen met domeinkennis.

Staijen waarschuwt dat technologische mogelijkheden sneller groeien dan maatschappelijke normen. Wat technisch kan, is niet altijd wenselijk. Daarom pleit hij voor een digitale escalatieladder: een stelsel van waarschuwingsmomenten, toetsing en verantwoording dat helpt om proportionele keuzes te maken. Legitimiteit is daarbij cruciaal. Burgers moeten erop kunnen vertrouwen dat data zorgvuldig, rechtmatig en uitlegbaar worden gebruikt.

Evidence-Based Werken biedt een methodisch kompas voor complexe veiligheidsvraagstukken, waarbij AI helpt om patronen te herkennen en scenario's te verkennen. Tegelijkertijd moeten we onderkennen dat AI nooit neutraal is. Modellen dragen impliciete waarden en aannames met zich mee. Organisaties moeten daarom actief bepalen welke waarden zij willen dat hun AI-systemen uitdragen. De vraag *Voor wie werkt jouw model eigenlijk*? raakt daarmee de kern van datagedreven veiligheid.

Ook Defensie staat voor een datagedreven uitdaging, blijkt uit het artikel *Data Mesh voor Defensie.* Het Data Mesh-concept draait om een federatief stelsel: data wordt centraal beschikbaar gesteld en decentraal gebruikt. Dat bevordert gegvensuitwisseling en effective samenwerking tussen defensieonderdelen. Daardoor wordt data beter vindbaar en betrouwbaarder, en bruikbaarder als effectieve bron voor AI-toepassingen. Zo ontstaat een slagvaardiger, effectiever defensieapparaat.

AI stelt, mits goed toegepast, defensiepersoneel in staat zich te richten op kerntaken. Het artikel over Enterprise Agentic Intelligence beschrijft hoe AI-agenten routinematig werk kunnen overnemen, mits ze onder strikte architectuur en onder menselijk toezicht worden ingezet.

Toekomst van werk

Het interview met Wim-Pieter Huijsman maakt duidelijk dat digitalisering het werk in het veiligheidsdomein fundamenteel verandert. Organisaties moeten af van het denken in functies en meer kijken naar de expertise die nodig is om een taak uit te voeren. Soms kan een systeem of AI-oplossing die expertise leveren, maar menselijke interpretatie is onmisbaar. De mens blijft altijd in de loop, zeker wanneer beslissingen directe gevolgen hebben voor burgers.

Voor professionals betekent dit dat leren en ontwikkelen een continu proces wordt. Technologie verandert voortdurend, en daarmee ook de dreigingen die ermee gepaard gaan. Dat alles stelt steeds nieuwe eisen aan vaardigheden die nodig zijn om ermee om te gaan.

Humanoids zijn een logische volgende stap in de voortdurende ontwikkeling van het veiligheidsdomein. Ze worden zichtbaar in publieke ruimtes en kunnen bijdragen aan toezicht en ondersteuning, maar roepen ook normatieve vragen op over gezag en legitimiteit, die alleen door de mens beoordeeld en beantwoord kunnen worden.

Ondertussen moeten we niet denken dat het innovatieproces vanzelf gaat. Het artikel *Een wankel kaartenhuis* laat zien dat 70% van de investeringen in AI geen rendement oplevert. Vaak is dat terug te voeren op zwakke plekken in de organisatie als het gaat om cultuur, datakwaliteit en governance. En daarbij moet ook veiligheid een integrale overweging zijn bij elke ontwikkeling. De Cyber Resilience Act dwingt organisaties om security by design en security by default te omarmen.

Weerbaarheid

Het interview met Arie Franke laat zien dat weerbaarheid begint bij mensen. De strafrechtketen is steeds afhankelijker geworden van digitale informatie en infrastructuur. Camerabeelden, audio-opnamen en andere digitale bronnen spelen een steeds grotere rol in bewijsvoering. Dat vraagt om systemen die betrouwbaar, controleerbaar en transparant zijn, maar ook om professionals die begrijpen hoe risico's moeten worden afgewogen en hoe digitale middelen verantwoord kunnen worden ingezet.

Weerbaarheid betekent niet alleen technische beveiliging, maar ook organisatorische robuustheid, duidelijke verantwoordelijkheden en een cultuur waarin digitale veiligheid onderdeel is van het dagelijkse werk. Kwetsbaarheid ontstaat vaak juist in periodes waarin alles goed lijkt te gaan. Daarom is oefenen, scenario-denken en het expliciet maken van bestuurlijke keuzes essentieel.

Desinformatie is een groter probleem dan ooit, aangejaagd door technologie. Ironisch genoeg ligt de oplossing ook besloten in de weloverwogen toepassing van technologie. Digitale platforms en AI-toepassingen kunnen ook worden ingezet om patronen, coördinatie en herhaling zichtbaar te maken. Maar waakzaamheid blijft geboden; er is een dunne scheidslijn tussen bestrijding van desinformatie en censuur. De menselijke maat blijft ook hier leidend. Dat blijkt uit het artikel *Kan je weerbaar zijn zonder censuur*?

JenV en Asiel & Migratie opereren in complexe ketens, onder permanente operationele, juridische en maatschappelijke druk. De afgelopen jaren is vooral ingezet op versterking van de regie, met beheersing van de hele keten als doel. Maar continue afstemming, coördinatie en rapportage alleen leiden niet tot de noodzakelijke versnelling. Volgens het artikel *Regie voeren in een weerbarstig ecosysteem* moeten we sturen op capabilities. Alleen zo kun je focus aanbrengen in overbelaste ecosystemen.

Digitale soevereiniteit wordt steeds belangrijker, zeker nu afhankelijkheden van internationale technologiepartijen toenemen. Maar als we die soevereiniteit zuiver technologisch aanvliegen, komen we er niet. Het artikel *Hoe soeverein wil je zijn*? stelt dat ook dit aspect vanuit het perspectief van de mens moet worden benaderd. Met andere woorden: niet de technologie moet leidend zijn, maar de adoptie ervan. Zonder digitale adoptie geen digitale soevereiniteit. Anders is het gevaar van onbeheersbare *shadow IT* levensgroot.

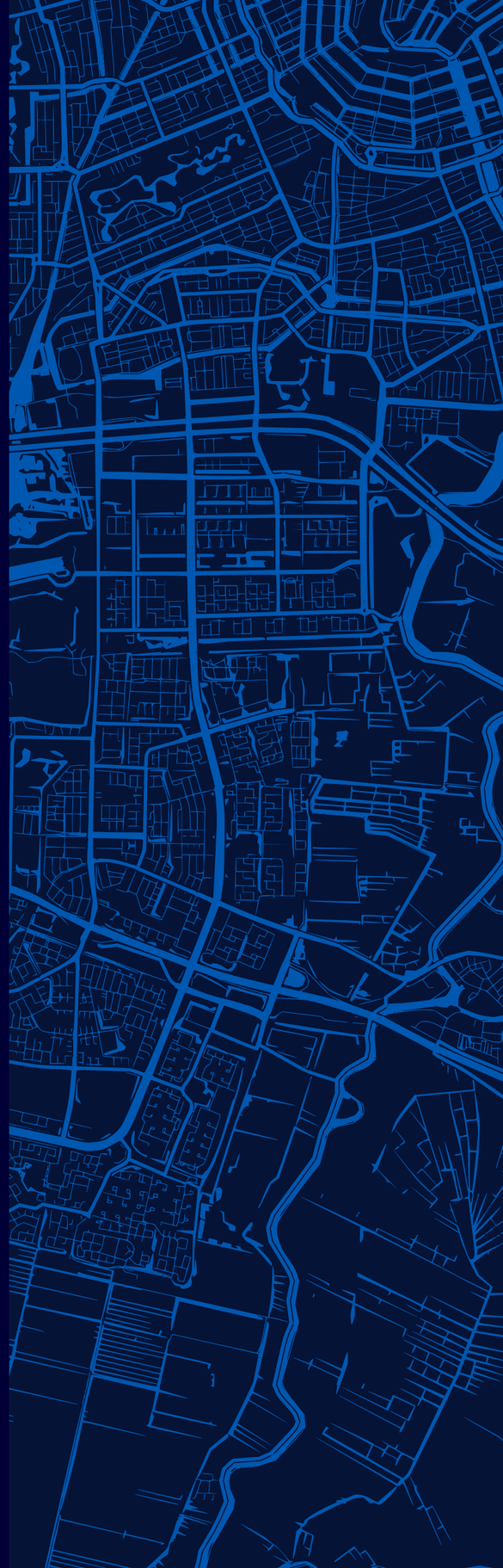
Wendbaarheid

Veel taakorganisaties binnen het ministerie van Justitie en Veiligheid worstelen met dezelfde cybersecurity-eisen. Een gezamenlijk Security Operations Center (SOC) biedt een kans om veiliger, slimmer en betaalbaarder te werken,mits zorgvuldig ingericht met aandacht voor governance. En: de onafhankelijkheid van zo'n SOC moet altijd geborgd zijn. Dat stelt het artikel Buiten de gebaande paden is het veiliger. De trend is momenteel een andere: we lijken toe te gaan naar een situatie met tientallen lokale SOC's. In dit artikel lees je waarom dat onverstandig is en hoe het beter kan.

Het artikel *Effectieve AI voor continue weerbaarheid en compliance* stelt vast dat dreigingen sneller toenemen dan ooit. Hoe kunnen organisaties hun digitale weerbaarheid zó versterken dat security, continuïteit en compliance aantoonbaar geborgd blijven? We zien dat traditionele risicobeheersing in een ketenafhankelijke wereld niet langer voldoet.

In dit spanningsveld komen AI-agents in beeld. Zij kunnen continu werken en beleid, risico's, logs en controles in samenhang interpreteren. AI-agents zijn geen vervanging van professionals, maar een versterking van bestaande rollen en verantwoordelijkheden. Bestuurders krijgen daarmee een actueel en samenhangend beeld van waar risico's zich opstapelen en of bestaande maatregelen nog volstaan. Daardoor kan tijdig worden bijgestuurd, voordat daadwerkelijke uitval optreedt.

Aydan Gunduz
Martijn van de Ridder
Natasja Pieterman
Erik Staffeleu
Gerard Pieter Borren



Interview:

Jolanda Aalbers

Hoofd Operatiën/Plv.
Politiechef Nationale Politie,
Eenheid Oost-Nederland

“Digitalisering mag nooit ten koste gaan van de menselijke maat.”

Maatschappelijke onrust, toenemende digitalisering en een samenleving die steeds diverser wordt. Volgens Jolanda Aalbers, hoofd Operatiën en plaatsvervangend politiechef van de Eenheid Oost-Nederland, zijn dit de ontwikkelingen die de komende jaren de grootste impact hebben op het veiligheidsdomein. Tel daarbij op dat burgers steeds meer verwachten van overheidsorganisaties, ook digitaal, en je staat als politie voor een flinke uitdaging. Hoe zorg je ervoor dat je toegankelijk, zichtbaar en menselijk blijft in een wereld die steeds digitaler wordt?

Polarisatie, digitalisering en maatschappelijke veranderingen

Het vertrouwen in instituties staat onder druk, groepen komen steeds vaker tegenover elkaar te staan en maatschappelijke spanningen nemen zichtbaar toe. “Dat heeft directe gevolgen voor het veiligheidsdomein”, zegt Aalbers. “We zien meer onvrede, afnemend vertrouwen in de overheid en groepen mensen die steeds verder uit elkaar groeien. Dat raakt uiteindelijk ook het werk van de politie. Daarnaast verandert de digitale transformatie onze wereld fundamenteel. Dat geldt niet alleen voor burgers omdat steeds meer dienstverlening online plaatsvindt, maar ook voor criminaliteit, opsporing en dienstverlening door de opkomst van nieuwe technologieën zoals kunstmatige intelligentie.”

Ook maatschappelijke veranderingen zoals klimaatdemonstraties, geopolitieke spanningen, migratiestromen en economische onzekerheid werken uiteindelijk door in het veiligheidsdomein. “Traditionele manieren van werken zijn niet langer vanzelfsprekend. De samenleving verandert en als politie zullen we daarin voortdurend moeten meebewegen.”

Dienstbaarheid als uitgangspunt

“Wij zijn een politie van de straat.” zegt Aalbers. “Dat betekent dat we altijd in verbinding willen staan met de samenleving. Juist daarom investeren we ook in digitale dienstverlening, om beter in contact te kunnen staan met de burgers. En die vorm van dienstverlening groeit: mensen vinden ons digitaal erg goed. Dat zien we terug in de cijfers. Via politie.nl hebben we jaarlijks ruim 28 miljoen keer contact met burgers, en via chatbots zo’n 400.000 keer.

“Digitalisering neemt uiteraard niet weg dat mensen ons ook via onze fysieke balies weten te vinden of via traditionele kanalen. Opvallend genoeg zien we dat het contact via telefonie bijvoorbeeld ook nog altijd groeit. Het aantal telefoontjes naar zowel het algemene politienummer als de meldkamers neemt toe, terwijl tegelijkertijd steeds meer mensen gebruikmaken van digitale kanalen. Nieuwe digitale mogelijkheden vervangen de bestaande contacten dus niet. Ze brengen ons juist in contact met nieuwe groepen. Jongeren bellen bijvoorbeeld nauwelijks nog. Voor hen is juist onze digitale dienstverlening essentieel. Daarmee ontstaat ook een nieuwe werkelijkheid waarin burgers verwachten dat zij de politie altijd kunnen bereiken op de manier die bij hen past.”

De burger centraal, maar niet onbeperkt

‘De burger centraal’ is een veel gehoorde stelling in overheidsland en klinkt nogal vanzelfsprekend. Toch is hier volgens Aalbers ook enige nuance op zijn plaats. “Wij werken uiteraard voor de samenleving. Zonder contact met burgers weten we niet wat er speelt. Dat contact is dus essentieel voor ons werk én voor onze legitimiteit als organisatie. Onze mogelijkheden zijn echter niet onbeperkt. We moeten dus voortdurend afwegen wat we willen bieden en daadwerkelijk kunnen waarmaken.”

Daarom kiest de politie voor een benadering waarin toegankelijkheid centraal staat, en tegelijkertijd ook duidelijke keuzes worden gemaakt. “Burgers moeten via verschillende kanalen contact kunnen opnemen, maar onze dienstverlening moet wél uitvoerbaar blijven”, benadrukt ze. “Het doel is niet om zoveel mogelijk contactmomenten te creëren, maar om betekenisvolle contacten mogelijk te maken.”

Digitaal intelligent, fysiek excellent

De strategie van de politie laat zich samenvatten als: digitaal intelligent en fysiek excellent. Aalbers licht toe: “Daar waar digitalisering meerwaarde biedt, wordt deze ingezet. Maar menselijk contact blijft onmisbaar. Er zijn immers situaties waarin context, emoties of specialistische kennis een belangrijke rol spelen. Denk aan een complexe zedenzaak. Dan is persoonlijk contact, maar ook de juiste expertise, essentieel. Dat kan uiteraard nooit digitaal.”

Wij willen burgers op verschillende manieren toegang geven tot de politie en voor verschillende groepen toegankelijk en nabij zijn. Door onze digitale dienstverlening verder te ontwikkelen en slimmer voor ons te laten werken kunnen wij aandacht geven aan de momenten waarop het mens-tot-menscontact – in nabijheid van elkaar – essentieel is, bijvoorbeeld bij aangifte van bepaalde delicten.

Daarom investeert de politie naast de lokale aanwezigheid van basisteams ook in andere communicatievormen die voor mensen veilig voelen. “Een goed voorbeeld is het gebruik van videobellen voor aangiftes. Burgers hoeven niet altijd meer naar een politiebureau te reizen, maar kunnen wel persoonlijk contact hebben met een politiemedewerker. Ook experimenteren we met nieuwe vormen van dienstverlening. In erschillende delen van het land lopen pilots met innovatieve politieloketten, digitale onbemande meldpunten en zogenoemde ‘politiematen’: digitale contactpunten die fysiek op een locatie staan, waarmee burgers eenvoudig in hun eigen taal met de politie kunnen spreken. Het gaat niet om of-of; het gaat om én-én. Digitalisering moet het contact gemakkelijker maken, niet vervangen.”

Inclusieve dienstverlening

Niet iedere burger is digitaal vaardig. Dat besef staat dan ook centraal bij de ontwikkeling van nieuwe dienstverleningsvormen. Volgens Aalbers is inclusie een randvoorwaarde voor succesvolle digitalisering. “Burgers moeten altijd een alternatief houden. Niet iedereen kan of wil digitaal contact opnemen. Daar moeten we rekening mee houden. We zijn ook bezig met nieuwe vormen van innovatieve politieloketten, waarin juist rekening wordt gehouden met ioen diversiteit. Denk aan meertalige toepassingen, ondersteuning via apps of andere nieuwe manieren om informatie toegankelijk te maken voor verschillende doelgroepen. We experimenteren bijvoorbeeld met een app waarbij een burger zijn eigen avatar als gesprekspartner kan kiezen. Zo zorgen we ervoor dat onze dienstverlening Ook laagdrempeliger wordt voor jongeren die ons niet meer bellen en al zeker geen politiebureau binnen lopen.”

Vertrouwen en digitale veiligheid

Digitale dienstverlening zal echter alleen succesvol zijn wanneer burgers ook vertrouwen hebben in de manier waarop hun gegevens worden verwerkt. “Veiligheid staat uiteraard centraal bij iedere digitale ontwikkeling. Of iemand nu via internet aangifte doet, videobelt of een bureau bezoekt: de basis moet hetzelfde zijn. Veilig, betrouwbaar en transparant.”

Dat vraagt niet alleen om veilige systemen, maar ook om medewerkers die weten hoe zij in een digitale omgeving moeten werken. “Bij nieuwe vormen van dienstverlening horen ook nieuwe vaardigheden, nieuwe processen en soms ook een andere manier van denken. Daarom investeren we in nieuwe technologie, maar altijd in combinatie met opleidingen en persoonlijke ontwikkeling.”

Technologie die ruimte maakt voor menselijk contact

Ook de politie werkt aan de inzet van kunstmatige intelligentie. Zo loopt er in Groningen momenteel een proef waarbij burgers voorafgaand aan een aangifte, digitaal alvast de nodige vragen beantwoorden. Aalbers: “Vervolgens verwerkt AI deze informatie tot een conceptaangifte die dan met de burger wordt besproken. Dat levert twee voordelen op. Een deel van het administratieve werk wordt geautomatiseerd zodat het gesprek erna niet meer twee uur hoeft te duren maar 45 minuten. En tijdens het gesprek blijft er meer tijd over voor de emotie en de persoonlijke kant van het verhaal.”

Volgens Aalbers ligt daar de echte kracht van technologie. “AI moet niet de mens vervangen. Het moet ervoor zorgen dat onze medewerkers meer tijd krijgen voor wat mensenwerk is. Waarom nog zoveel energie steken in een aangifte die voor de verzekering wordt opgesteld? Dat kun je gewoon digitaliseren. Administratieve handelingen kunnen dus sterk worden verminderd, waardoor politiemedewerkers meer tijd overhouden voor gesprekken, ondersteuning en persoonlijke aandacht. Daar ben ik van overtuigd.” Ook toepassingen zoals speech-to-text bieden volgens haar veel potentieel.

Vernieuwing structureel verankeren

Innovatie is belangrijk, maar experimenteren alleen is niet genoeg. De uitdaging zit volgens Aalbers vooral in het opschalen van succesvolle initiatieven. “Een pilot starten is relatief eenvoudig. Het daadwerkelijk onderdeel maken van de dagelijkse operatie is veel ingewikkelder. Daarvoor zijn structurele investeringen nodig in capaciteit, technologie en organisatieontwikkeling.”

Binnen de politie wordt dienstverlening daarom niet meer gezien als een los project, maar als een strategisch thema dat op het hoogste niveau is belegd. “Als je echt toekomstbestendig wilt zijn, moet je continu blijven kijken naar nieuwe ontwikkelingen. Wat vandaag innovatief is, kan over drie jaar alweer achterhaald zijn.”

De verbonden politie van de toekomst

Waar moet de politie de komende jaren vooral in investeren? Voor Aalbers ligt het antwoord in een combinatie van technologie en menselijkheid. “De verdere ontwikkeling van politie.nl, nieuwe AI-toepassingen en innovatieve vormen van contact zijn belangrijke bouwstenen. Maar minstens zo belangrijk blijft de fysieke aanwezigheid van de politie in de samenleving. Want juist in een tijd van maatschappelijke onrust hebben mensen behoefte aan een zichtbare politie. Dat fysieke contact blijft essentieel.”

Als zij één ontwikkeling zou mogen versnellen? Daarover hoeft zij niet lang na te denken. “AI. Niet omdat technologie een doel op zich is, maar omdat deze ruimte kan creëren voor meer aandacht voor mensen. Want wanneer technologie routinematige taken overneemt, ontstaat er tijd voor het echte gesprek. Voor luisteren, ondersteunen en verbinding maken. Uiteindelijk is dat waar ons werk om draait.”

De toekomst van burgergerichte dienstverlening ligt volgens Aalbers daarom in technologie die de menselijke maat versterkt. “Digitalisering moet ervoor zorgen dat we dichter bij burgers komen te staan. Niet verder van hen af. Dat is uiteindelijk de essentie van dienstbaarheid.”

Van cel naar samenleving: hoe overheidsorganisaties samen veiligheid en perspectief creëren door werk in detentie

Hoe versterken de werk- en leerbedrijven binnen gevangenissen de kansen van gedetineerden?

Highlights

- “Binnen beginnen om buiten te blijven”
- Werken en leren dragen bij aan het welzijn van gedetineerden door een zinvolle dagbesteding
- Ontwikkeling vraagt om een samenhang tussen werk, leren en doorstroom
- Serviceorganisatie In-Made is kan aanzienlijk meer bijdragen aan de rijksoverheid dan momenteel het geval is
- In-Made hecht veel waarde aan doorontwikkelen

Serviceorganisatie (SO) In-Made vergroot met werken en leren de veiligheid in penitentiaire inrichtingen’s en de kansen van gedetineerde burgers op een duurzame terugkeer.

Een veilig leef- en werkklimaat in detentie ontstaat niet alleen door toezicht. Het ontstaat vooral wanneer mensen een doel hebben, ritme opbouwen en zich kunnen ontwikkelen. Werken en leren maken al jaren deel uit van het dagprogramma binnen de PI’s. Het werkritme van gemiddeld 20 uur per week per gedetineerde zorgt voor rust, regelmaat en voorspelbaarheid binnen detentie. Een zinvolle en uitdagende dagbesteding voor gedetineerden zorgt voor een positieve invloed op het welzijn van gedetineerden én personeel.

Dynamiek van de werkzalen

Elke dag ontstaat er in de werkzalen van werk- en leerbedrijven een levendige dynamiek die verder gaat dan alleen productie. De werkplek fungeert als een leergemeenschap: medewerkers ontwikkelen vakmanschap, oefenen in samenwerken en leren omgaan met verantwoordelijkheid. Twee collega’s van SO In-Made, A. Huizing en P. Schattel, onderzochten waarom gedetineerden meedoen aan penitentiaire arbeid, onder andere door interviews met hen te houden. Voor veel respondenten vormt werken, ook tijdens detentie, een belangrijk onderdeel van hun dagelijks leven. Werk zorgt ervoor dat zij structuur houden in hun dagritme. Bovendien wordt het sociale aspect gewaardeerd: interactie met medegedetineerden en personeel wordt positief ervaren en de sfeer op de werkvloer is vaak minder gespannen dan op de leefafdelingen. Ten slotte bieden werk- en leeractiviteiten waardevolle afleiding. Ze helpen verveling voorkomen, wat weer bijdraagt aan meer veiligheid en een prettigere sfeer binnen de PI.

De unieke positie van In-Made

SO In-Made is een landelijke organisatie binnen Dienst Justitiële Inrichtingen (DJI) en faciliteert werken en leren in detentie. SO In-Made biedt PI’s specialistische kennis, zorgt voor landelijke samenwerking en ondersteunt bij een deel van de operationele werkzaamheden. Werken en leren vergroot ook de kansen van gedetineerden op een succesvolle terugkeer naar de arbeidsmarkt en draagt bij aan een veilig leef- en werkklimaat binnen de PI’s.

Wat werken en leren extra bijzonder maakt, is het commerciële karakter. Gedetineerden werken betaald aan opdrachten voor interne en externe klanten. Dat varieert van het produceren van meubilair voor DJI en het recyclen van defensiekleding tot het repareren van fietsen. Zo doen zij relevante werknemersvaardigheden op die direct aansluiten bij kansrijke beroepen[1] buiten de muren.

1) https://www.uwv.nl/assets-kaj/files/fd4a3668-c7e4-4344-816f-c1406286d50c/rapportage-kansrijke-beroepen-2025-2026-def.pdf

Een landelijke organisatie is hierin onmisbaar. Doordat SO In-Made centraal werkt, kunnen werk- en leerbedrijven in alle PI's gebruik maken van dezelfde kwaliteit, standaarden en ondersteuning. Deze landelijke uniformiteit vertaalt zich niet alleen naar de PI's, maar zorgt ook voor gelijke kansen voor gedetineerde burgers, ongeacht in welke inrichting zij verblijven. De landelijke sturing maakt het mogelijk om kennis te bundelen, processen te verbeteren en een aanbod te creëren dat schaalbaar is en minder afhankelijk van lokale verschillen.

Route van binnen naar buiten

Ontwikkeling bestaat nooit uit één onderdeel. Werken en leren lopen in de praktijk door elkaar en versterken elkaar. Gedetineerde burgers behalen certificaten, bouwen beroepsvaardigheden op en volgen onderwijs dat hen helpt bij een realistische stap terug in de samenleving.

De samenhang van vakonderwijs en praktijkervaring zijn structurele onderdelen van de werk- en leeromgeving. Daarbij staat niet alleen de intramurale ervaring centraal. Veel PI's zoeken naar manieren om de stap van binnen naar buiten beter te begeleiden. De wens is om leren en werken in detentie beter te verbinden met ketenpartners en mogelijkheden buiten de muren, zodat de overgang minder abrupt wordt. Dit draagt bij aan het motto "binnen beginnen om buiten te blijven".

Balans tussen maatwerk en landelijke sturing

Werken en leren in detentie vraagt om maatwerk, omdat iedere gedetineerde een eigen ontwikkelpad heeft. Door duidelijke landelijke kaders te combineren met ruimte voor lokale professionele afwegingen ontstaat een aanpak die zowel consistent als mensgericht is. Zo blijft maatwerk mogelijk, zonder de samenhang en bestuurbaarheid van een landelijke organisatie te verliezen.

Zichtbaarheid voor maatschappelijke impact

Hoewel werken en leren aantoonbaar waardevol zijn, kan de zichtbaarheid van en bekendheid met de mogelijkheden die werken in detentie kan bieden beter.

Binnen de bredere organisatie en bij andere rijksdiensten is onvoldoende bekend dat veel producten en diensten die men extern inkoopt ook binnen detentie kunnen worden geproduceerd. Denk aan het maken van keukens voor andere PI's vanuit het werk- en leerbedrijf in PI Zwolle, kastinrichting voor Rijkswaterstaat en het sorteren van afval binnen de eigen PI om bij te dragen aan de Rijksbrede doelstelling van het verminderen van restafval. Deze beperkte zichtbaarheid betekent dat kansen blijven liggen.

Meer bekendheid helpt om het maatschappelijke en economische potentieel van In-Made beter te benutten. Wanneer publieke organisaties eerder kiezen voor interne productie, ontstaat stabieler werk voor gedetineerde burgers, groeit de ontwikkelruimte en neemt de maatschappelijke opbrengst toe. Zichtbaarheid is daarom niet alleen een communicatievraagstuk, maar een bouwsteen voor een veiligere samenleving en maatschappelijk verantwoord ondernemen.

Juist het landelijke karakter van In-Made maakt dat de impact verder reikt dan een enkele PI. Wanneer de organisatie zichtbaarder wordt, herkennen andere Rijksorganisaties dat zij kunnen samenwerken met één betrouwbare partner die landelijk opereert en overal dezelfde kwaliteit levert. Dit maakt inbesteding aantrekkelijker en vergroot het maatschappelijk rendement van werken en leren in detentie.

Samen met Capgemini Invent heeft SO In-Made gewerkt aan het structureren van de werkzaamheden. Er gebeurt veel op individueel en regionaal niveau, maar voor het vergroten van de zichtbaarheid en impact is het noodzakelijk om de aanpak te bundelen rondom een aantal centrale thema's met bijpassende doelstellingen. Zo zet In-Made de komende jaren meer en meer in op het nastreven van een veilig en stimulerend leefklimaat door partnerschappen met andere overheidsorganisaties en maatschappelijke ondernemingen, naast de structurele opdrachten met bedrijven die er al zijn.

"Binnen beginnen om buiten te blijven."

Samenwerking als motor voor doorstroom

Werken en leren krijgen pas blijvende waarde wanneer ze worden verbonden met kansen buiten de muren. Samenwerking met ketenpartners als gemeenten, UWV, DJI-breed en reclassering zorgt voor een doorlopende ontwikkelketen. Wanneer gedetineerde burgers kunnen doorstromen naar vervolgonderwijs, een stage of een baan, krijgt alles wat zij binnen detentie leren betekenis. Deze samenwerking zorgt bovendien voor een meer divers aanbod aan werk- en leermogelijkheden. Het versterkt de brug tussen detentie en samenleving en vergroot de kans op duurzame re-integratie. Daarbij is een plan voor het aangaan van samenwerking met een aantal strategische partners noodzakelijk.

De arbeidsmarkt verandert snel en de samenleving digitaliseert in hoog tempo. Dat vraagt om werk- en leerbedrijven die meegaan met hun tijd. Door te investeren in moderne werkplekken, actuele machines en eigentijdse leermiddelen ontstaat een omgeving die aansluit op het werk van morgen. Nieuwe vaardigheden zoals digitale geletterdheid, logistiek inzicht of duurzaam produceren worden steeds belangrijker. Wanneer werkplaatsen deze ontwikkelingen omarmen, vergroot dat zowel de waarde van het werk binnen detentie als de kansen op aansluiting bij de samenleving na detentie. Vanuit de SO In-Made worden deze trends gemonitord om het werk en toekomstperspectief voor gedetineerde burgers aantrekkelijker te maken.

Sturen op baten voor de burger

SO In-Made is continu in ontwikkeling en werkt vanuit de overtuiging dat de organisatie zich moet blijven aanpassen aan wat PI's, gedetineerden en de maatschappij nodig hebben. Elke paar jaar wordt de organisatievorm opnieuw bekeken en worden externe ontwikkelingen meegenomen in het aanscherpen van de koers. Deze cycli van verbeteren, herijken en doorontwikkelen maken dat SO In-Made nooit stilstaat.

Werken en leren leveren veel meer op dan productie en bezetting. Ze leiden tot tastbare maatschappelijke baten die verder reiken dan de muren van de inrichting. Iedere gedetineerde die vaardigheden opdoet, een certificaat behaalt of verantwoordelijkheid leert dragen, vergroot zijn kans op een leven zonder criminaliteit. Dat betekent minder slachtoffers, minder maatschappelijke kosten en meer mensen die positief bijdragen aan de samenleving. Door deze baten expliciet mee te nemen in sturing en besluitvorming wordt zichtbaar dat investeren in ontwikkeling de samenleving rendement oplevert, ook bij andere overheidsorganisaties die samenwerken met DJI's In-Made.

Conclusie

SO In-Made staat op een belangrijk punt in haar ontwikkeling. Het werken en leren biedt grote maatschappelijke waarde, maar SO In-Made benut nog niet alle mogelijkheden. Door werken en leren sterker te verbinden, landelijke herkenbaarheid te vergroten en te sturen op ontwikkelresultaten kan SO In-Made uitgroeien tot een moderne en toekomstgerichte organisatie die veiligheid en perspectief in balans brengt.

Over de auteurs

Eva Lo-van Steenbergen
Director Zorg & Veiligheid

Eva Lo is werkzaam bij Capgemini Invent. Eva is gespecialiseerd in organisatie-inrichting en bekostiging binnen het zorg- en justitiedomein en richt zich op de ontwikkeling van een toekomstbeeld voor de Serviceorganisatie In-Made.

eva.lo@capgemini.com

https://www.linkedin.com/in/evsteenbergen/

Olivier le Blanc
Manager Intelligent Health

Olivier is werkzaam bij Capgemini Invent. Olivier is gespecialiseerd in onderzoek en digitale (zorg)oplossingen binnen het zorg en justitiedomein en is betrokken bij het uitwerken van organisatievorm van de toekomst met betrekking tot de Serviceorganisatie In-Made.

olivier-le.blanc@capgemini.com

https://www.linkedin.com/in/olivier-le-blanc/

Marja ter Horst
Hoofd Serviceorganisatie Werken en leren in detentie, Dienst Justitiële Inrichtingen (DJI)

Marja is werkzaam bij Dienst Justitiële Inrichtingen. Marja is het afdelingshoofd van de Serviceorganisatie In-Made en richt zich op gevangeniswezenbrede regie op uitvoering van diensten die een passende werk- en leerervaring in detentie ondersteunen binnen de geldende kaders.

https://www.linkedin.com/in/marja-ter-horst-b7173b10/

Van beleid naar betekenis

Hoe kunnen we de burger en professional centraal zetten in publieke transities?

Highlights

- Heb oog voor spanningen bij de inrichting van een alliantie
- Zet de burger en de professional centraal
- De menselijke factor en het gedrag zijn cruciaal voor de prestaties van de strafrechtketen

Maatschappelijke vraagstukken en transities kunnen niet binnen één ministerie opgelost worden. Samenwerking met andere overheden, maatschappelijke organisaties en bedrijven is noodzakelijk. Programma's gericht op maatschappelijke vraagstukken lopen vaak stroef en duren lang.

Tegelijkertijd komt er veel op de strafrechtketen af. Er zijn nu ongeveer 500 beleids- en wetgevingsinitiatieven voor de strafrechtketen. Voorbeelden zijn meer slachtofferrechten, de wijziging van het Wetboek van Strafvordering en de Wet seksuele misdrijven. Dat vraagt veel van de betrokken organisaties. Tegelijkertijd ziet de Algemene Rekenkamer dat er nauwelijks aandacht is voor de uitvoerbaarheid.

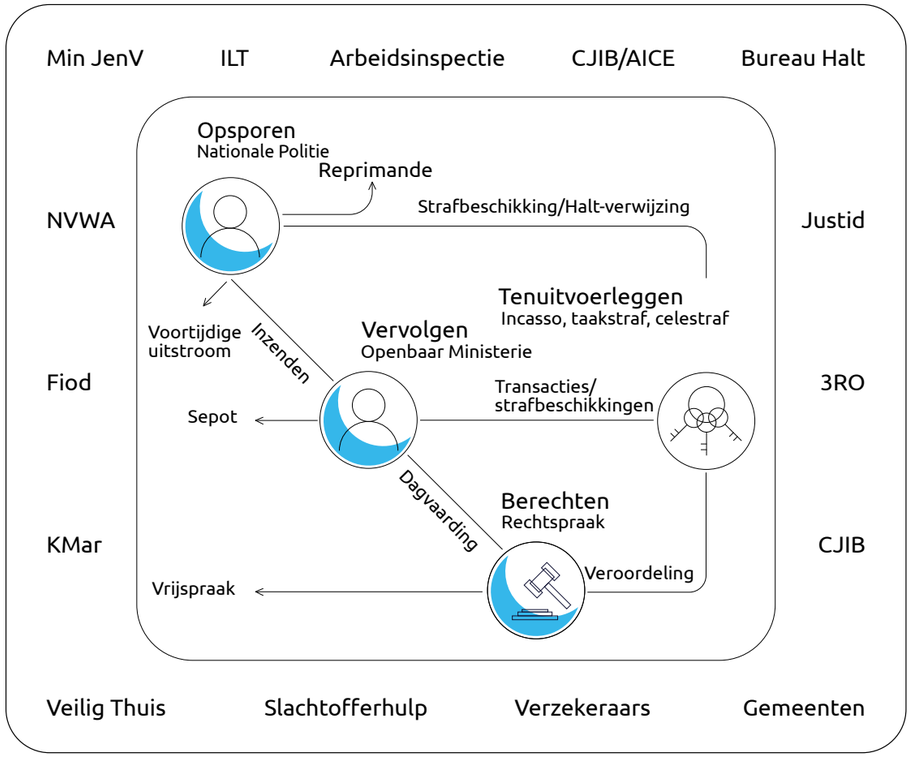
Wat is nodig voor een succesvolle samenwerking binnen een alliantie en meer aandacht voor uitvoerbaarheid?

- Gedeelde waarden?
- De inrichting van het ecosysteem van organisaties?
- Een ketenbrede dienstenoriëntatie?
- Een ontwerpende aanpak?
- De burger en professional centraal zetten?

Samenwerken in wisselende allianties

In het publieke veiligheidsdomein spelen veel vraagstukken waarbij meerdere partijen betrokken zijn. De strafrechtketen bestaat onder andere uit het ministerie JenV, Nationale Politie, Koninklijke Marechaussee, Openbaar Ministerie, Centraal Justitieel incassobureau, Dienst Justitiële Inrichtingen en vele andere partijen. Zo zijn er ook combinaties van strafrechtelijke en bestuurlijke interventies waarbij bijvoorbeeld gemeentes en de belastingdienst betrokken zijn.

De term strafrechtketen doet vermoeden dat de organisaties in een keten samenwerken. In werkelijkheid is het een ecosysteem van diverse organisaties die in wisselende allianties moeten samenwerken om het ketenbelang te behalen.



Afbeelding 1 Vereenvoudigde weergave van de strafrechtketen (Algemene rekenkamer) versus ecosysteem van organisaties

De doorlooptijden in strafzaken worden niet gehaald, waardoor het belang van de burger in het gedrang komt

De Algemene Rekenkamer geeft in haar publicatie Resultaten verantwoordingsonderzoek 2024 ministerie van Justitie en Veiligheid (Algemene rekenkamer, 21-5-2025) aan:

"Verdachten en slachtoffers die aangifte doen komen in aanraking met de strafrechtketen. Deze keten bestaat uit de fases opsporing, vervolging, berechting en uitvoering van de straf of maatregel. Om een strafzaak op tijd te kunnen afhandelen moeten de organisaties goed samenwerken, maar dat lukt onvoldoende. Er is te weinig aandacht voor het algemene (keten)belang."

Voor een tijdige afhandeling van strafzaken moeten niet alleen de afzonderlijke partijen in de alliantie hun werkprocessen goed hebben ingericht, maar ook de logistiek en samenwerking over de betrokken organisaties heen. De organisaties in het ecosysteem zijn namelijk afhankelijk van elkaar voor het leveren van de ketendienst.

In de tijd dat een zaak in behandeling is, zitten slachtoffers en verdachten in onzekerheid. Vaak gaat deze periode gepaard met stress en soms kan de situatie in deze tijd escaleren. Voor het "lik op stuk"-beleid is het van belang zo snel mogelijk een straf of maatregel op te leggen. Slachtoffers van misdrijven lijden extra emotionele schade als de strafzaak lang blijft voortduren."

Wat kunnen allianties in de strafrechtketen doen om de samenwerking te verbeteren?

Voor een waardegericht ketendienstontwerp is het van belang om een gemeenschappelijke visie te hebben over de waarde die elkaar verbindt en het ketenbelang beschrijft. Daarnaast moet er ook zicht zijn waar de waarden van de betrokken organisaties verschillen. Er zullen namelijk spanningen zijn tussen deze waarden, zogenaamde waardenspanningen.

> Het boek Allianties voor een duurzame toekomst (Jaap Boonstra, Marcos Eguiguren & Boom, 2023) geeft aan dat bij het formeren, funderen, evolueren en transformeren van allianties diverse spanningen in het spel zijn.
>
> **"Het signaleren van spanningen is een voorwaarde voor succesvolle samenwerking in waardegedreven allianties. (...) Het onderkennen van paradoxen bij het creëren en ontwikkelen van allianties kan leden in de alliantie helpen bij het omgaan met problemen, spanningen en strategische keuzes."**

Zicht op deze spanningen, die zich als paradoxen manifesteren, helpt om de dynamiek in de levensfasen van allianties te hanteren. Een spanning die in praktijk vaak voorkomt bevindt zich tussen het ketenbelang en het belang van de betrokken organisaties. De portfolio's van de betrokken organisaties zijn overvol. Moet de beperkte capaciteit ingezet worden voor ketenprogramma's of voor het verbeteren van de eigen bedrijfsvoering. Daarnaast kan het ketenbelang betekenen dat organisaties operationeel meer inspanning moeten verrichten. Daar hebben zij ogenschijnlijk zelf geen profijt van, terwijl een organisatie verderop in de keten dat wel heeft.

Een praktijkvoorbeeld betreft de alliantie rondom het afpakken van criminele geldstromen waar de Nationale Politie en het CJIB deel van uit maken. De Nationale Politie staat aan het begin van de keten bij het vastleggen van het dossier Kan weg, staat hierboven ook al. Hoe gedetailleerder het dossier wordt opgesteld, hoe succesvoller het CJIB uiteindelijk zal zijn het innen van de opgelegde ontnemingsmaatregel.

Met een ecosysteemcanvas kan goed in kaart gebracht worden welke waarden en spanningen een rol spelen, wat de betrokken organisaties zijn die gezamenlijk de ketendienst leveren en wat de onderlinge rollen (regie, operationeel, ondersteunend) zijn. In de relevante wet- en regelgeving zijn de onderlinge verantwoordelijkheden vaak beschreven. Bij veranderende wet- en regelgeving is het van belang om precies te zijn over de aard van de verandering. Is het een optimalisatie van het bestaande samenspel in de alliantie of is het een transitie waarbij verhoudingen veranderen of nieuwe spelers toetreden. Dit heeft invloed op de waardenspanning binnen de alliantie.

De aanpak van de Handreiking Keten Business Analyse (HKBA) is sterk in het beschrijven van de onderlinge samenwerking, de koppelvlakken tussen organisaties en de diensten die de organisaties aan elkaar leveren om uiteindelijk de ketendienst tot stand te brengen.

Burger en professional centraal in de ketenbrede dienstenoriëntatie

De beschrijving van ketenbrede diensten is echter vaak gericht op informatie-uitwisseling en informatiesystemen. Veelal worden transities/veranderprogramma's technisch aangevlogen. Cruciaal voor het realiseren van de ketendoelstelling en daarmee het succes van de programma's is het centraal zetten van de burger en de professional in de ketenbrede dienstenoriëntatie.

Dat vraagt om een mindset waarbij de mens centraal wordt gezet. Bouw door middel van onderzoek kennis op van de belangrijkste persona's. Een crimineel is een "klant" die zich in meer of mindere mate probeert te onttrekken aan de dienstverlening van de strafrechtketen. Slachtoffers, verdachten en veroordeelden hebben belang bij een vlotte afhandeling van de strafzaak.

Hiervoor is het belangrijk om ook oog te hebben voor de professional in de keten. Niet alleen voor de functionele behoefte van de professional maar ook voor de omstandigheden (de emotionele en sociale behoeftes) waarin deze zijn werk moet uitvoeren. Het maakt verschil of de politiebeambte de identiteit van de verdachte op het bureau kan vaststellen in een gecontroleerde omgeving.

Op straat kan het vaststellen van de identiteit met een mobiele device een stuk lastiger zijn als het regent, het donker is en het onveilig is omdat er nog omstanders zijn die zich bemoeien met de staande-/aanhouding.

Bij het centraal zetten van de professional hoort ook de focus op welk gedrag van de professional verwacht wordt. McKinsey-onderzoek toont consequent aan dat menselijke en gedragsfactoren, zoals weerstand van werknemers en gebrek aan steun van het management, de belangrijkste redenen zijn waarom tot wel 70% van de veranderingsinitiatieven binnen organisaties mislukt. Succes hangt daarbij meer af van het aanpakken van denkwijzen, overtuigingen en gedrag dan van structuren en processen alleen. Effectieve verandering vereist een focus op de "menselijke factor" door inzicht te krijgen in gevoelens, overtuigingen en motivaties, en niet alleen door nieuwe taken of systemen te definiëren, om inherente weerstand te overwinnen (McKinsey& Company, December 2021).

Diverse overheidsorganisaties experimenteren met design thinking, design sprints en een ontwerpende aanpak, omdat ze worstelen met dit vraagstuk. Een ontwerpende aanpak is een lerende, iteratieve aanpak die onzekerheid omarmt en onderzoekend is. Deze methodieken helpen bij het centraal zetten van de menselijke factor, doordat vertegenwoordigers van de verschillende belanghebbenden betrokken worden bij de probleemanalyse en scenario's voor oplossingen. Centraal in deze aanpak is ook het experimenteren en testen van oplossingen in de praktijk om verkeerde aannames over de behoeftes van belanghebbenden vroegtijdig te herkennen. Denk ook na over het ontwerpen van een feedback loop. Vaak krijgen professionals geen feedback over hoe hun werk succesvol heeft bijgedragen aan het uiteindelijke ketenresultaat. Zulke feedback levert een belangrijke bijdrage aan de waardering van de professional. Betrek daarnaast ook burgers om te toetsen of de oplossing aansluit bij hun behoefte. Voelt bijvoorbeeld een slachtoffer zich beter geïnformeerd, veiliger en/of beter begrepen?

De menselijke factor in het samenspel binnen een alliantie

Hoe kunnen we een bijdrage leveren aan succesvolle programma's voor het adresseren van maatschappelijke vraagstukken? Dit artikel is bedoeld om het onderwerp te verkennen en uit te nodigen tot reflectie en gesprek. De centrale stelling is het belang van het oog hebben voor spanningen binnen de keten bij het realiseren van de ketendienstverlening. Zet daarnaast de burger en de professional centraal in het samenspel van organisaties binnen de (wisselende) allianties door onderzoek te doen naar de behoeftes van deze belanghebbenden en hen te betrekken bij de probleemanalyse en ontwerp van oplossingen. Deze aanpak leidt tot beter zicht op de betekenis van beleid voor de belanghebbenden, een succesvollere implementatie van wet- en regelgeving en daarmee met de prestaties van de strafrechtketen.

Over de auteur

Paul Lengkeek
Ketencoördinator

Paul werkt al 20 jaar in het veiligheidsdomein. Paul is niet meer werkzaam bij Capgemini maar is nu Ketencoördinator bij Ministerie van Justitie en Veiligheid.

https://www.linkedin.com/in/paul-lengkeek-8551183/

Bestuurlijke grip op digitale risico's: sturen, kaderen en toetsen

Digitale governance ingericht voor incidenten of voor weerbaarheid?

Highlights

- Rolzuiverheid is cruciaal: zonder duidelijk eigenaarschap blijven digitale risico's tussen afdelingen vallen
- Een hybride 3LoD-3LM aanpak combineert functiescheiding met samenwerking en wendbaarheid. Dit is essentieel voor complexe digitale domeinen
- Weerbaarheid zorgt voor betere dienstverlening aan burgers, door voorspelbaarheid, uitlegbaarheid en een cultuur van structureel leren

Digitale publieke dienstverlening staat onder toenemende druk. Cyberaanvallen en verstoringen raken niet langer alleen systemen, maar direct de continuïteit van dienstverlening, het vertrouwen van burgers en de bestuurlijke legitimiteit. Tegelijkertijd stapelen nieuwe Europese verplichtingen zich op en ontwikkelen technologieën als generatieve AI en quantum computing zich sneller dan bestaande governancestructuren kunnen bijhouden. Voor bestuurders is de kernvraag daarom niet of digitalisering kansen biedt, maar hoe u aantoonbaar stuurt op risico's én publieke waarde, voordat incidenten of toezichthouders u daartoe dwingen. En hoe kunt u als bestuurder aantoonbaar 'in control' zijn over digitale risico's, zonder te vallen in incident-gedreven sturing of versnipperde silo-governance? Veel organisaties sturen nog alsof incidenten uitzonderingen zijn. In werkelijkheid is verstoring het nieuwe normaal.

Het Three Lines of Defense-model (3LoD) maakt bestuurlijke verantwoordelijkheid concreet door drie functies te onderscheiden:

- **Eerste lijn:** voert uit en beheerst risico's in de operatie (de proceseigenaar blijft eigenaar).
- **Tweede lijn:** stelt kaders, ondersteunt en monitort (bijv. CISO/CPO/CDO-functie en governance-boards).
- **Derde lijn:** toetst onafhankelijk of het stelsel in ontwerp én werking functioneert (audit/FG/andere onafhankelijke toets).

38%

Het percentage incidenten bij de overheid

Nieuwe digitale risico's vragen om een sterkere overheid

Digitale incidenten ondermijnen steeds vaker het vertrouwen in de overheid als instituut. Een DDoS-aanval op DigiD liet bijvoorbeeld zien dat burgers tijdelijk geen toegang hadden tot vitale diensten en dat kwetsbaarheid van publieke digitale infrastructuur direct zichtbaar wordt. Uit onderzoek blijkt dat de overheid met 38% van de incidenten de meest aangevallen sector in de EU is (ENISA, 2025). In dit landschap wordt van publieke organisaties verwacht dat zij toetsbaar, uitlegbaar en verantwoord omgaan met data, algoritmen en digitale risico's, juist omdat verstoring meteen doorwerkt in dienstverlening én maatschappelijke legitimiteit.

Weerbaarheid betekent hier: het vermogen om schokken op te vangen zonder continuïteit of publieke legitimiteit te verliezen. Dat vraagt om een besturingsmodel waarin strategie, uitvoering en onafhankelijke toetsing elkaar versterken. Bestuurders winnen vertrouwen door te beloven dat er nooit iets misgaat, maar door te laten zien dat risico's vooraf worden afgewogen, besluiten uitlegbaar zijn en lessen structureel worden verwerkt in beleid en uitvoering (Oldenhof, Kersing en Zoonen, 2024).

Rolzuiverheid als voorwaarde voor bestuurbare digitale risico's

Een van de grootste bestuurlijke uitdagingen is het expliciet beleggen van eigenaarschap. Digitale thema's lopen dwars door organisaties heen: privacy raakt IT, beleid en uitvoering; AI raakt juristen, IT en bestuur; cybersecurity raakt operatie, leveranciers en ketenpartners. De reflex is dan al snel 'gezamenlijke verantwoordelijkheid'. In de praktijk betekent dat vaak: vervaagde verantwoordelijkheid. Bestuurders hebben juist een model nodig dat expliciet maakt wie beslist, wie monitort en wie toetst.

Rolzuiverheid zoals Three Lines of Defence beoogt helderheid te creëren over taken, informatiestromen en escalatie. Hierdoor wordt vooraf zichtbaar wie risico's weegt, wie voorwaarden stelt en wie ingrijpt wanneer maatregelen niet werken.

Dit wordt zichtbaar bij de inzet van externe AI- of clouddiensten. Beleidsafdelingen zien het als 'IT-vraagstuk', IT ziet het als 'business-beslissing' en leveranciers verwijzen naar contracten. Zonder duidelijke scheiding tussen eerste, tweede en derde lijn blijft onduidelijk wie vooraf risico's beoordeelt, wie het go/no-go besluit neemt en wie achteraf structureel leert van incidenten. In de praktijk zien we dat AI-oplossingen worden ingezet zonder duidelijke risico-eigenaar, waarna pas bij vragen van toezichthouders discussie ontstaat.

Concreet vraagt dit dat de eerste lijn (proceseigenaren en teams) zelf risico's en afhankelijkheden beoordeelt die horen bij hun gebruik, zoals datakwaliteit, leveranciersafhankelijkheid en impact op burgers. De tweede lijn vertaalt juridische, ethische en technische kaders naar toepasbare normen en besluitcriteria. De derde lijn toetst onafhankelijk of kaders worden nageleefd en of risico's in de praktijk daadwerkelijk beheerst zijn. Deze scheiding is geen bureaucratie, maar een randvoorwaarde voor uitlegbaarheid, betrouwbaarheid en aantoonbaar verantwoord digitaal handelen.

Burgers centraal: voorspelbaarheid en uitlegbaarheid als bron van vertrouwen

Vertrouwen ontstaat niet doordat de overheid nooit faalt, maar doordat handelen voorspelbaar en consistent is. Wanneer organisaties werken volgens gedeelde principes, ontstaat uniformiteit in uitvoering. Dat maakt voor burgers én volksvertegenwoordigers inzichtelijk hoe keuzes worden gemaakt, wie waarvoor verantwoordelijk is en hoe risico's worden afgewogen (IIA, 2022).

Als de drie functies helder zijn ingericht en de dialoog tussen de lijnen serieus wordt genomen, verbetert vooral de voorspelbaarheid van dienstverlening. Burgers merken dat beslissingen beter uitlegbaar zijn, dat privacy en security vooraf zijn ingebouwd en dat bij verstoringen snel en transparant wordt gehandeld. Bestuurders zien rapportages die niet alleen incidenten tellen, maar de werking van governance laten zien: waar risico's liggen, welke maatregelen werken en welke lessen structureel zijn verwerkt.

Zonder dit fundament ontstaat interne en externe ruis: privacy, cybersecurity en data-ethiek functioneren als losse sporen. Dat creëert een 'illusion of control': beleid klopt op papier, maar uitvoering is inconsistent en voor burgers onnavolgbaar. Bestuurders hebben juist behoefte aan één stelsel waarin principes doorwerken in processen, besluitvorming en rapportages.

In de keten wordt bovendien duidelijker wie waarvoor verantwoordelijk is, ook bij leveranciers en partners. Daardoor wordt de organisatie minder afhankelijk van uitzonderingen en ad-hoc oplossingen, en groeit vertrouwen in vaste werkwijzen die hun waarde hebben bewezen.

Wanneer regulatie en governance integraal onderdeel worden van dagelijkse besturing, verschuift het gesprek van regels naleven naar maatschappelijke verwachtingen waarmaken. Weerbaarheid wordt dan zichtbaar in gedrag: integrale rapportages, duidelijke verantwoordelijkheden en een cultuur waarin incidenten systematisch worden geëvalueerd en verbetermaatregelen worden doorgevoerd.

Kritische reflectie 3LOD is een middel, geen doel

Geen enkel model garandeert succes. Als rapportages alleen registreren zonder betekenis, als controles innovatie onnodig vertragen, of als rollen zo vervloeien dat onduidelijkheid ontstaat, ondermijnt dat de beoogde weerbaarheid. Bestuurlijk vakmanschap zit in de balans: genoeg informatie voor het juiste besluit, genoeg documentatie om te leren, en steeds opnieuw het gesprek voeren over waar de grootste risico's én de meeste publieke waarde liggen. Weerbaarheid is nooit 'af'; het is de optelsom van keuzes die elke dag opnieuw worden gemaakt.

De kans op weerbaarheid groeit wanneer er volledige duidelijkheid is over wie uitvoert, wie kaders stelt en wie onafhankelijk toetst. Dat betekent bijvoorbeeld dat privacy officers niet in de eerste lijn 'mee-uitvoeren', dat CISO-functies niet afdalen tot tactisch beheer maar hun tweedelijns rol waarmaken, en dat onafhankelijke toetsers (zoals de FG in het privacy-domein) onafhankelijk blijven in positie en beoordeling. Deze scheiding is geen doel op zich, maar een voorwaarde voor uitlegbaarheid en betrouwbaarheid.

Een duurzame governance structuur voor vertrouwen

3LoD 'op papier' invoeren levert weinig op. Functies benoemen is niet genoeg; het verschil zit in het versterken van de eerste lijn: daar moet eigenaarschap over digitale risico's daadwerkelijk landen. De tweede lijn kan ondersteunen, maar kan nooit de verantwoordelijkheid van de eerste lijn overnemen; de derde lijn controleert onafhankelijk. Pas wanneer de verschuiving plaatsvindt van 'de CISO regelt het wel' naar 'de lijnverantwoordelijke stuurt expliciet op risico's' draagt 3LoD bij aan echte weerbaarheid, zeker in het veiligheidsdomein. De echte vraag is of u bereid bent eigenaarschap expliciet in de lijn te beleggen.

Over de auteurs

Albert Holl
Director AI Governance

Albert leidt een team van gedreven consultants en ondersteunt organisaties bij de implementatie van -en de Europese AI-klanten in verordening. Hij helpt klanten in uiteenlopende sectoren om wet- en regelgeving te vertalen naar werkbare governance en verantwoorde inzet van technologie. Vanuit zijn brede ervaring heeft Albert het 3LoD meerdere malen succesvol geïmplementeerd bij organisaties in de publieke sector, met specifieke aandacht voor de integratie van data-privacy binnen bestaande governance-structuren.

Albert.holl@capgemini.com

https://www.linkedin.com/in/albert-holl-fip-9041704/

Nadia Maalim
Management Consultant Data Trust

Nadia is een multidisciplinaire consultant met een achtergrond in technologie en recht. Ze heeft een sterke interesse in dataprivacy, digitale regelgeving en maatschappelijke impact, met aandacht voor bestuurlijke vraagstukken en het duurzaam verankeren van wet- en regelgeving binnen organisaties. Waarbij zij organisaties ondersteunt door complexe juridische en technische vraagstukken te vertalen naar duidelijke, toepasbare inzichten. Ze beschikt over praktische kennis van onder meer de GDPR, de AI Act, Digital Services Act en Digital Market Act.

nadia.maalim@capgemini.com

www.linkedin.com/in/nadia-m-6b034964

Interview:

Ruud Staijen

Landelijk Programmadirecteur
Datagedreven Samen
Werken bij de Politie

Grenzen aan datagedreven politiewerk

Meer data is alleen effectief als het verantwoord kan: Ruud Staijen over gegevensdeling, privacy en legitimiteit bij de politie

Publieke organisaties moeten wendbaar en weerbaar blijven onder druk van snelle technologische, juridische en maatschappelijke ontwikkelingen. Criminaliteit, contact met burgers, informatievoorziening, samenwerking met partners: steeds meer loopt via digitale sporen, kanalen en afhankelijkheden. In het veiligheidsdomein komt daar iets bij: de ruimte om te experimenteren met data is beperkt, terwijl de druk om sneller te handelen en beter te prioriteren toeneemt. Ruud Staijen, Landelijk Programmadirecteur Datagedreven Samen Werken bij de Politie: “Criminaliteit die vroeger analoog werd gepleegd, gebeurt nu digitaal. Daardoor verandert ons werk ingrijpend.”

Juist omdat digitalisering zoveel mogelijk maakt, is de vraag: hoe organiseer je datagedreven politiewerk op zo’n manier dat het Nederland veiliger maakt, zonder dat je legitimiteit en vertrouwen verliest? Staijen: “De baten van datagedreven werken en een datagedreven economie zijn hoog. Maar de kosten, denk aan privacyschending, zijn net zo hoog. Als samenleving moeten we daarom nieuwe normen bepalen: wat mag data ons letterlijk en figuurlijk kosten? Die normen zijn nu nog niet goed uitgekristalliseerd.”

Criminaliteit digitaliseert, politiewerk ook?

Staijen benoemt drie ontwikkelingen die in zijn ogen het veiligheidsdomein de komende jaren gaan bepalen. De eerste is de digitaliserende samenleving, die direct doorwerkt in het politiewerk. Staijen: “Als criminaliteit zich verplaatst, verplaatst ook de informatiepositie die je nodig hebt. Het klassieke sporenonderzoek blijft overeind, maar de aard van de sporen verandert. Sporen zijn niet meer alleen fysieke vingerafdrukken of getuigenverklaringen, maar ze bevinden zich ook in telefoons, digitale identiteiten en gedragsdata.”

De tweede ontwikkeling is schaarste op de arbeidsmarkt. Staijen: “Mensen vinden, en helemaal goede mensen, is een toenemend probleem. En deze uitdaging raakt de politie extra hard omdat de kern van ons vak mensenwerk blijft: capaciteit, kennis, kunde, gevoel. Als 70% van je budget bestaat uit menskracht, dan moet je dat budget extreem gericht inzetten als de tekorten zo nijpend blijven.”

De derde ontwikkeling gaat over normen en waarden. Technologie beweegt veel sneller dan onze gedeelde opvattingen over wat proportioneel en acceptabel is, ziet hij. “Er zijn steeds vaker situaties waarin iets technisch kan, juridisch mogelijk lijkt, maar maatschappelijk schuurt”, zegt Staijen. “Als normen niet helder zijn, en juridische kaders gemaakt zijn voor een grotendeels analoge wereld, krijg je discussie, vertraging, onzekerheid in de uitvoering en riskeer je dat het draagvlak afneemt. Terwijl juist dat draagvlak in het veiligheidsdomein groot belang is.”

Data maakt je pas slim als je kunt combineren

Wat houdt datagedreven werken in de praktijk in? Staijen: “Datagedreven werken gaat om het samenbrengen van verschillende, verspreide signalen. Door ze samen te brengen, begrijp je wat er speelt en waar je moet handelen. Criminelen laten sporen achter. Dat kunnen biologische sporen zijn, zoals DNA, vingerafdrukken of bloed. Maar het kan ook zijn dat hij ergens met zijn telefoon loopt. Een telefoon straalt altijd de dichtstbijzijnde paal aan. Als ik weet waar ingebroken is, kan ik die data bij elkaar brengen. De essentie is niet dat je ‘meer’ data nodig hebt, maar dat je verschillende datapunten kunt koppelen aan domeinkennis, op een manier die leidt tot beter begrip, meer inzicht en gerichter optreden.”

Dat levert wel een maatschappelijke spanning op: data zijn overal, maar wie is eigenaar en wie mag die data delen en wie gebruiken? Staijen: “Iedereen wil zijn eigen data voor zichzelf houden. Dat is begrijpelijk, want data kunnen gevoelig, complex en risicovol zijn om te delen. Maar het is ook een reden waarom de ketens in het veiligheidsdomein niet slimmer worden. We worden als totale keten pas slim als we relevante data met elkaar delen. Want dan kun je gaan puzzelen, signalen bij elkaar brengen en daaruit betekenisvolle informatie destilleren.”

Data verzamelen is invasief

Data zijn sporen die achterblijven door menselijke gedragingen. Als je die data verzamelt, dan is dat per definitie invasief, meent Staijen. “Het doet namelijk iets met privacy. Dataverzameling kan burgers het gevoel geven dat de overheid ze continu in de gaten houdt, als een soort Big Brother.” Digitale veiligheid gaat dus niet alleen om het voorkomen van misdaad, maar ook om het behouden van maatschappelijke legitimiteit.

“Je kunt als organisatie keurig binnen je bevoegdheden opereren en toch het vertrouwen van de samenleving verliezen, omdat burgers ervaren dat de inzet van data te veel of niet uitlegbaar is. In het veiligheidsdomein is dat geen theoretische discussie. Als vertrouwen afneemt, wordt samenwerking met burgers en maatschappelijke partners simpelweg veel lastiger. Het maakt informatie delen ingewikkelder en dat beïnvloedt de effectiviteit van je handelen als politie ook negatief. Ik ben

daarom altijd voorzichtig met stellige uitspraken over de baten van data voor onze veiligheid. Want zeker, datagedreven werken levert enorme voordelen op. Maar de keerzijde van de medaille zijn de kosten voor onze maatschappij. In onze beslissingen moeten we daarom voor alles rekening houden met het vertrouwen van onze samenleving; het is de legitimiteit voor ons handelen als veiligheidsdomein."

Wat betekent proportionaliteit?

Het is een precaire kwestie, want wat weegt zwaarder? Privacy of veiligheid? Staijen licht het toe aan de hand van de opiumwet. "Stel, iemand slikt een pilletje op een dancefeest, en die komt in aanraking met de Politie. XTC valt onder de opiumwet. Dat is strafbaar. Daar zijn heel veel bevoegdheden voor.

Ik mag in dat geval de telefoon in beslag nemen. Maar is het dan proportioneel om voor het bezit van een recreatief pilletje die telefoon volledig leeg te trekken, of om alle data op die telefoon te onderzoeken? Ik vind van niet. De Europese rechter zegt ook dat de politie een afweging moet maken. Alleen, de opsporing heeft daar concretere handvatten voor nodig en die geeft de wet op dit moment niet.

Zie hier het fundamentele dilemma van digitale middelen. Wat je kunt doen om in te grijpen, wordt steeds ingrijpender. Wat je zou moeten doen, blijft dus constant een normatieve afweging. Staijen: "En die afweging kun je niet overlaten aan ad hoc beslissingen of aan de techniek. Je moet hier eerst goed over nadenken, en het vervolgens in het normatieve, richtinggevende kader opnemen van je hele besluitvormingsorgaan."

Decennia bouwen aan normering

Bij geweld heeft de politie er tientallen jaren over gedaan om proportionaliteit als praktische routine te organiseren. Inmiddels is er een algemeen geaccepteerde geweldsladder. Staijen: "Eerst praat ik met iemand. Als die dan niet luistert, ga ik wat duwen. Daarna een tik met de wapenstok, dan pepperspray en dan pas – onder hele strikte voorwaarden – meer ingrijpende maatregelen. Daar zitten heel veel waarschuwings- en bedenkingsmomenten in. Zo ontstaat legitimiteit. Door opbouw, training, toetsing en uiteindelijk een gedeelde maatschappelijke norm over wanneer je welk middel inzet."

Bij data moet precies hetzelfde gebeuren, zegt hij. "We moeten een soort escalatieladder ontwikkelen waarbij veel waarschuwingsmomenten ingebakken zitten. Soms subtieler, soms dieper, soms op grotere schaal. Op die manier kun je ook achteraf beter verantwoorden waarom er is gekozen voor een bepaalde maatregel. In het programma steken we daarom veel energie in het versterken van het juridisch en ethisch handelen en het verhogen van de kennis en kunde van alle collega's. We hebben gekozen voor een gemeenschappelijk taal (CSAE, Collect, Store, Analyze, Engage) en dragen dat ondersteund door een Summerschool, de CSAE-papers en een opgezette CSAE-community ook breed uit. Ook hebben we een intensieve en hechte relatie met onze ketenpartner het Openbaar Ministerie, bekrachtigd in een Datagedreven Samenwerkingsconvenant. Alleen ga je snel, samen kom je verder.

"We moeten een soort escalatieladder ontwikkelen waarbij veel waarschuwingsmomenten ingebakken zitten. Soms subtieler, soms dieper, soms op grotere schaal."

Datagedreven opleidingen

Om te bouwen aan slim en rechtsstatelijk datagedreven werken heeft het programma in samenwerking met collega's uit het veld, de veldacademies, andere aanpalende programma's en de Politieacademie (PA) een opmaat naar een datagedreven werken opleidingscatalogus opgesteld. Er zijn veertien opleidingen in terug te vinden en samen met Datagedreven Opleidingscomunity probeert de PA dit te integreren in haar opleidingsaanbod.

Governance in balans

Zijn programma Datagedreven Werken beschrijft Staijen als constante balansopgave. "Het logo van ons programma Datagredreven Werken, is een wipwap. Dat betekent: je moet de balans vinden. Daar bedoel ik mee: je moet steeds afwegen wat het doel is dat je wilt bereiken en de proportionaliteit van de middelen die je daarvoor inzet. Hoe lang bewaar ik data? Wie geef ik daartoe toegang? Dat zijn fundamentele ontwerpkeuzes: bewaartermijnen, toegang, autorisaties, logging en het vermogen om achteraf te verantwoorden waarom iets is gedaan. Daar komt een tweede laag bij: hoe verkrijg je data op een manier die 'netjes' is binnen een rechtstaat? Daarvoor moet je iemand hebben die bevoegd is en toestemming geeft. Dan hebben we het over een officier van justitie of een rechter-commissaris. Datagedreven werken is niet alleen een kwestie van 'kunnen koppelen'. Het is ook een kwestie van 'mogen koppelen'.

DE VIER PROGRAMMALIJNEN

Programmalijn 1	**Programmalijn 2**	**Programmalijn 3**	**Programmalijn 4**
Bouwplaatsen	Inrichten datahuishouding	Versterken juridisch en ethisch handelen, kennis en kunde	Stroomlijnen datavoorzieningen
• LO/LX	• Datamanagement en -governance ontwerpen en beproeven	• Handelingskader verzamelen data (collect en analyze)	• Opleveren doelarchitectuur datagedreven werken
• Rotterdam/ Den Haag		• Korpsbrede opleiding data bewustzijn en -bekwaamheid	• Onderzoeksrap-portage harmonisatie van datamodellen (store)
• Oost		• Faciliteren vakgroepen	• Opschonen Transferium
Levert een beschrijving op van het standaardi-satieproces nodig voor DGSW.	Levert een inrichtingsplan voor de Data Care organisatie op.	Levert een handelingskader op voor verzamelen en analyseren van data. Zorgt voor het delen in kennis en kunde en biedt opleidingen aan.	Levert de doelarchitectuur voor DGSW.

En dat ‘mogen’ moet zichtbaar, toetsbaar en uitlegbaar zijn.”

Niet méér maar professioneler

Een groot gevaar bij datagedreven werken is dat het overzicht op data kan kwijtraken. Want alle verschillende instituten, zoals het OM, de politie of rechterlijke macht, moeten data zoveel mogelijk centraal houden. “Anders ga je repliceren”, legt Staijen uit. “Dat betekent ook dat je met meerdere kopieën gaat werken en het overzicht op je informatie kwijt bent, en de juistheid van je bron niet meer te garanderen is. Besluiten die grote consequenties hebben - ‘ga ik met een getrokken wapen naar binnen of niet‘ - moet je vanuit zekerheid organiseren. Daarvoor zijn twee wegen: 1) zorg dat je data klopt, en 2) zorg dat je mensen goed opgeleid zijn en bewust met die data omgaan. Dus niet méér technologie, maar professionelere omgaan met wat we al hebben. Dat is wat ik probeer te bereiken met ons programma.”

Het opschonen en opruimen van oude data is daarom, naast het stroomlijnen van alle dataverzamelingen en het onder architectuur gaan werken, een van de hoofdpijlers van het programma. “Daarbij ben ik positief verrast door de verkregen medewerking van alle eenheden bij het opschonen van de data. Politiemensen willen rechtsstatelijk handelen en daarbij maakt het netjes met data omgaan en wat niet meer nodig is opruimen integraal onderdeel uit van het werk.”

Datacare organisatie

Een helpende hand, monitorend oog en corrigerende hand

Verder wordt er hard gewerkt aan het neerzetten van datacare-organisatie. Praktijkervaring uit datacare-initiatieven en de pilot in de eenheid Oost Nederland maakten duidelijk wat de aard van het werk is, wie bij datacare zijn betrokken en wat nodig is om het te laten werken. Wat blijkt: veel mensen zijn al bezig met datacare, maar vaak ontbreekt de regie en verbinding. ‘Datacare is onderdeel van het politiewerk’ en ‘elke collega is zelf verantwoordelijk om integer en effectief met data om te gaan.’ Praktische ondersteuning, dat is precies wat de datacare-organisatie gaat bieden: met een combinatie van een helpende hand, een monitorend oog en een corrigerende hand.

Organisatieverandering

Datagedreven werken wordt vaak als project benaderd. Staijen vindt dat onterecht. “Ik behandel het als een manier om je organisatie in te richten. Als je werkprocessen veranderen, verandert je IT. Als je IT verandert, moet de opleiding meeveranderen, en als de opleiding verandert, praat je over tienduizenden mensen. Dan hoor ik mensen al zeggen: ‘hallo, dan moeten we 50.000 mensen opnieuw opleiden‘. Ja, dat klopt. Maar als we het niet doen, zijn de gevolgen immens. Waar we naartoe willen maak je niet werkbaar door één applicatie te kopen. Je maakt het door definities, standaarden, processen en governance bij elkaar te brengen. En dat kost nou eenmaal tijd.”

AI-veiligheid is bewijsveiligheid

Naast het veranderen van de organisatie, speelt ook betrouwbaarheid van de waarneming een steeds grotere rol. Staijen: “Als ik vroeger een rapport opstelde, moest ik zo nauwkeurig mogelijk beschrijven wat de waarneming was. Dus: ‘ik zag, ik hoorde, ik voelde, ik rook’, en dat schreef ik op. Dan zei de rechter: dit is wel of niet geloofwaardig. Maar nu zitten we regelmatig te kijken naar camerabeelden waarvan we niet meer weten of ze echt zijn. Zo worden data dus ook niet meer alleen een hulpmiddel, maar ook een bron van onzekerheid. Het totale veiligheidsstelsel moet dus weerbaarder worden. De politiemensen, de systemen, en de checks and balances. Want onze bewijsvoering kan niet leunen op aannames.

Waar nu in te investeren

Als Staijen vooruitkijkt, ziet hij naast veel kansen, ook een flinke berg werk. “De winkel moet ook openblijven”, zegt hij. Daarom kiest hij voor klein organiseren rondom werkprocessen. “Bouwplaatsen noemen we dat. Daarin spelen we met leren.” Hij wil een organisatie vormen die beter en bewuster kijkt naar data. En daar een vak van maakt. “En ik draai dat ook om: sommige dataverzamelingen op z’n kop zetten om te zien hoe het beheer er echt voor staat.”

Zijn afsluitende boodschap? “Ja, AI en automatisering bieden kansen. Maar als we daarop willen sturen, moeten we het fundament eerst op orde brengen. Let goed op je content, je data en je bewijslast. Want het is de bron van alles daarna. En als je dat niet kunt garanderen, moet je je mensen beter inzetten. De grootste winst zit niet in harder en meer verzamelen maar in beter organiseren.”

Rechtsstatelijke papers II:

Het zal nog even duren voordat we werkbare regelgeving hebben die ons - net als bij geweldgebruik - heel concreet vertelt wat proportioneel is in welke situatie. Maar we moeten nu al aan de slag met data-dilemma’s. We willen ook nu al netjes met data om kunnen gaan. Daarom heeft het Juridisch Netwerk DGSW onderzocht welke kant het recht op beweegt en welke richting de politie dus in moet slaan. Dit staat beschreven in de zes hoofdlijnen van de Rechtsstatelijke Papers II: gericht en gemotiveerd verzamelen, onafhankelijke toetsing, scheiding bruto- en nettobak, nieuwe voorwaarden voor hergebruik, kwaliteitseisen voor data, uniforme werkprocessen.

Evidence-based werken als kompas in een AI-gedreven veiligheidsdomein

Op welke wijze versterken evidence-based werken en AI elkaar bij integrale samenwerking voor een veilige samenleving?

Highlights

- Evidence-based werken (EBW) biedt een methodisch kompas gericht op ‘wat werkt’ binnen een bepaalde context
- AI versterkt EBW door het analyseproces te versnellen, verbanden te leggen en alternatieve interventies te verkennen
- EBW volgt een lerende cyclus van probleemverkenning, analyse, uitvoering, monitoring en evaluatie, waardoor interventies adaptief en aantoonbaar effectief zijn
- Integrale samenwerking tussen politie, toezicht, zorg, welzijn en bestuur wordt expliciet versterkt, mits zij hiervoor tijd en capaciteit vrijmaken en structuur aanbrengen
- De combinatie van EBW en AI versterkt de legitimiteit van sturing, besluitvorming en technologische inzet in het veiligheidsdomein

In het complexe veiligheidsdomein groeit de inzet van AI. Maar hoe zet je AI in zodat het daadwerkelijk bijdraagt aan maatschappelijke effecten? Evidence-based werken (EBW) biedt het antwoord.

Complexiteit en sturing in het veiligheidsdomein

Het veiligheidsdomein is een complex en dynamisch werkveld, waarin vraagstukken zelden eenduidig zijn. Criminaliteit en gevoelens van onveiligheid ontstaan door de wisselwerking tussen sociale, economische en ruimtelijke factoren en zijn sterk contextafhankelijk. Praktijkervaring leidt tot continue bijstelling van prioriteiten en interventiekeuzes, waardoor besluitvorming geen lineair, maar cyclisch proces is.

Veiligheid is de basis voor vertrouwen in de samenleving. Maatschappelijke ontwikkelingen zoals individualisering, digitalisering, polarisatie en internationale spanningen verklaren de toenemende aandacht voor maatschappelijke veiligheid. De verantwoordelijkheden van de diverse organisaties in het veiligheidsdomein zijn daarbij vaak overlappend.

De Wetenschappelijke Adviesraad Politie constateert bijvoorbeeld dat de politie opereert op het snijvlak van zowel juridische, sociale als organisatorische verantwoordelijkheden[1]. Bovendien staat in veiligheidsorganisaties de capaciteit veelal onder druk. Dit alles versterkt de behoefte aan professionele oordeelsvorming, effectieve en transparante besluitvorming en verantwoorde inzet van middelen bij samenwerking.

We zien dat AI daarvoor steeds vaker wordt ingezet. Publieke organisaties richten zich daarbij terecht op risicobeheersing, ethiek en juridische randvoorwaarden. Het gaat dan om risico’s zoals bias in data en algoritmen, onjuiste output en de noodzaak van transparantie, uitlegbaarheid en zorgvuldige omgang met persoonsgegevens. Minstens zo belangrijk is de vraag hoe AI aantoonbaar bijdraagt aan inhoudelijke sturingskwesties, zoals tijdig signaleren, gerichter inzetten van capaciteit en systematisch monitoren van effecten. Dat vraagt om een helder methodisch kader voor sturing op de inzet van AI.

1) Wetenschappelijke Adviesraad Politie. (2025). Navigeren in niemandsland: Verkenning van grensgebieden van de politiepraktijk. Wetenschappelijke Adviesraad Politie. https://www.wetenschappelijkeadviesraadpolitie.nl/uploads/publications/Navigeren-in-niemandsland.pdf

Evidence-based werken in het veiligheidsdomein

Evidence-based werken structureert besluitvorming door wetenschappelijke kennis, praktijkervaring en context systematisch te combineren. Het maakt expliciet welke overwegingen aan keuzes ten grondslag liggen en richt zich op aantoonbaar maatschappelijk effect. Hierdoor versterkt het de legitimiteit en navolgbaarheid van keuzes, juist wanneer middelen schaars zijn en maatschappelijke druk hoog is. Bovendien ontstaat een systematische en transparante werkwijze die samenwerking versterkt tussen de verschillende partijen: politie, toezicht, zorg, welzijn en bestuur.

EBW vindt zijn oorsprong in de geneeskunde: evidence-based medicine. Dit werd in de jaren negentig ontwikkeld door onder andere Gordon Guyatt[2] en David Sackett[3]. In deze benadering komen wetenschappelijke kennis, praktijkervaring en context samen in criteria voor een optimaal effect bij patiëntenzorg. Lawrence Sherman adopteerde het concept voor het politiedomein en introduceerde de term ‘evidence-based policing’[4]. In relatie tot het bredere veiligheidsdomein waar we ons in dit artikel op richten is de aanduiding EBW passender.

EBW sluit aan bij de groeiende aandacht voor leren en verbeteren in het veiligheidsdomein. Inzichten uit implementation science[5][6][7] laten zien dat de effectiviteit van interventies afhangt van hoe interventies worden uitgevoerd, geborgd en gemonitord. Dit onderstreept het belang van evaluatie en systematisch ontwikkelen en kennis delen.

In een domein waarin meerdere organisaties samenwerken en veiligheidsvraagstukken verschillende leefgebieden raken, biedt EBW een robuust kader voor gezamenlijke besluitvorming. Daarmee vormt het een logisch fundament voor het verantwoord en effectief inzetten van technologie zoals AI.

EBW als lerende cyclus en de versterkende rol van AI

EBW volgt een lerende cyclus, waarin probleemverkenning, analyse, uitvoering en evaluatie elkaar voortdurend beïnvloeden. Door aannames, doelen en keuzes expliciet te maken, worden mogelijkheden voor effectieve AI-inzet inzichtelijk. De inzet van AI wordt daarmee geen doel op zich, maar een middel binnen een samenhangend proces.

Door patronen te analyseren, alternatieven te genereren en effecten te monitoren versterkt AI de besluitvorming. Bovendien vergroot zij niet alleen de snelheid en diepgang van analyse, maar ook de breedte van het denken en de creativiteit van mogelijke oplossingen. EBW borgt daarbij human-in-the-loop: De professional blijft richtinggevend in normatieve afwegingen en contextduiding.

2) Guyatt, G. H., Cairns, J., Churchill, D., Cook, D., Haynes, B., Hirsh, J., ... & Tugwell, P. (1992). Evidence-based medicine: A new approach to teaching the practice of medicine. JAMA, 268(17), 2420–2425. https://doi.org/10.1001/jama.1992.03490170092032

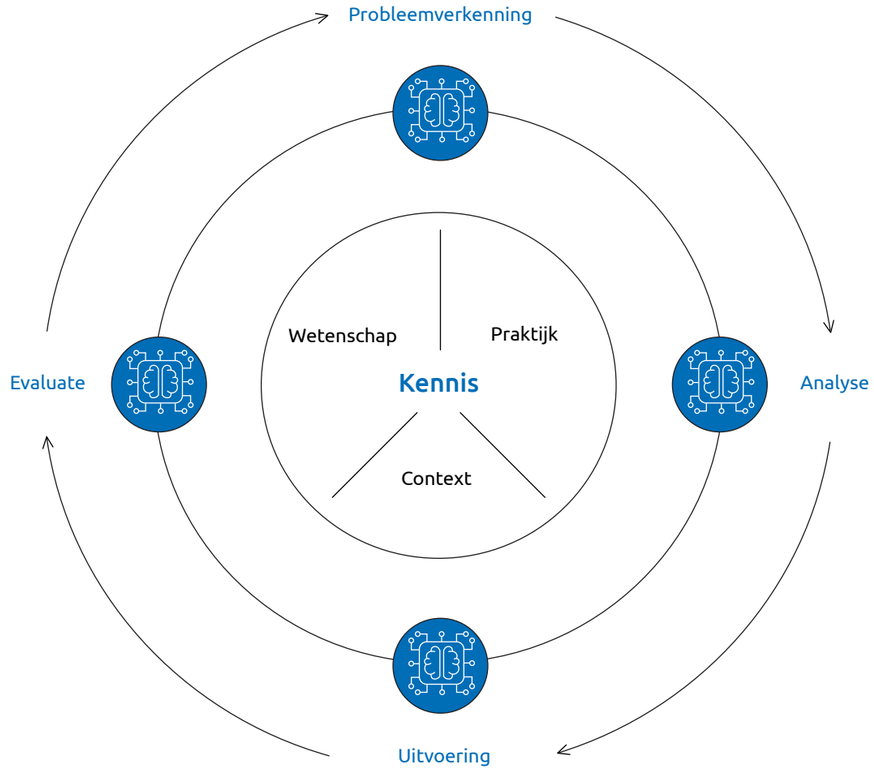
3) Sackett, D. L., Rosenberg, W. M. C., Gray, J. A. M., Haynes, R. B., & Richardson, W. S. (1996). Evidence based medicine: What it is and what it isn't. BMJ, 312(7023), 71–72. https://doi.org/10.1136/bmj.312.7023.71

4) Sherman, L. W. (1998). Evidence-based policing. Ideas in American Policing, 1, 1–15. Washington, DC: Police Foundation.

5) Del Pozo, B., Belenko, S., Pivovarova, E., Ray, B., Martins, K. F., & Taxman, F. S. (2022). Using implementation science to improve evidence-based policing: An introduction for researchers and practitioners. Policing: An International Journal, 45(1), 3–18. https://doi.org/10.1108/PIJPSM-07-2021-0104

6) Del Pozo, B., Belenko, S., Pivovarova, E., Ray, B., Martins, K. F., & Taxman, F. S. (2025). Evidence-based policing in practice: Implementation challenges and organizational adaptation. Police Quarterly, 28(2), 182–211. https://doi.org/10.1177/10986111241265290

7) Del Pozo, B., Belenko, S., Pivovarova, E., Ray, B., Martins, K. F., & Taxman, F. S. (2025). Implementing evidence-based practices in policing: Organizational barriers and facilitators. Policing: An International Journal. Advance online publication. https://doi.org/10.1080/30679125.2025.2607615



Afbeelding 1 EBW als lerende cyclus

Uitwerking van EBW op een actueel veiligheidsvraagstuk

Om concreet te laten zien hoe dit vorm zou kunnen krijgen, gebruiken we het actuele vraagstuk van jongeren en geweld in het openbare domein. Media-aandacht voor bijvoorbeeld messenbezit of explosie-incidenten met vuurwerkbommen beïnvloedt sterk de veiligheidsbeleving in de samenleving. De oorzaken van deze vormen van geweld zijn veelal multidimensionaal en variëren van omgevingsfactoren tot sociale en economische omstandigheden

De uitwerking hieronder is hypothetisch en illustreert een breder toepasbare werkwijze. Het dient ter inspiratie voor de manier waarop de gecombineerde inzet van EBW met AI meerwaarde kan hebben bij de gezamenlijke aanpak van complexe vraagstukken.

De eerste stap in het methodisch kader van EBW is probleemverkenning. Hierbij staat een gecombineerde blik centraal op incidenten en veiligheidsbeleving.

Waar de politie zich richt op vraagstukken over geweldspatronen en toezicht op normoverschrijdend gedrag in de openbare ruimte, kijken zorg- en welzijnsorganisaties primair naar kwetsbaarheid, psychosociale problematiek en gezinscontext. Het openbaar bestuur weegt deze signalen in relatie tot bestuurlijke prioriteiten en maatschappelijke onrust. EBW biedt handvatten om deze verschillende perspectieven te verbinden en samenhang te creëren in het probleembeeld. AI kan daarbij informatie uit uiteenlopende bronnen (bijv. sociale media en digitale meldingen) systematisch analyseren en verbinden, waardoor signalen van escalatie eerder worden opgemerkt. Met agentic AI kan bovendien per sector (politie, zorg, bestuur) een ‘virtueel perspectief’ worden opgebouwd, waardoor verschillen in framing expliciet worden gemaakt en besproken. Dit vergroot wederzijds begrip en versterkt de gezamenlijke probleemanalyse.

In de analysefase staat het verklaren van patronen centraal. Het gaat niet alleen om de vraag waar en wanneer jongerengeweld voorkomt, maar ook waarom bepaalde personen of groepen zich onveiliger voelen dan andere. Vanuit politie en toezicht worden verklaringen gezocht in zichtbare ordeverstoringen, concentraties van incidenten en recidivepatronen. Vanuit zorg en welzijn ligt de focus op achterliggende problematiek zoals schooluitval, psychische kwetsbaarheid, gezinsstress en sociale uitsluiting. Het openbaar bestuur bekijkt deze patronen in samenhang met maatschappelijke spanningen, media-aandacht en politieke druk. EBW stimuleert het combineren van deze perspectieven met wetenschappelijke kennis over groepsdynamiek of routine-activiteiten. AI kan daarbij grote datasets en literatuur analyseren en scenario's simuleren waarin risicofactoren samenkomen, bijvoorbeeld groepsdruk en online beïnvloeding.

Op basis van de analyse worden hypotheses geformuleerd over wat werkt om zowel geweld als onveiligheidsgevoelens te verminderen. Politie en toezichthouders kunnen inzetten op zichtbaarheid op plekken waar bewoners zich onveilig voelen. Zorg- en welzijnsorganisaties richten zich op passende begeleiding en gezinsondersteuning. Bestuurders wegen of maatregelen bijdragen aan vertrouwen en sociale cohesie. AI kan daarbij alternatieven verkennen en vergelijken, zoals mentorprogramma's, digitale leeromgevingen of (online) campagnes gericht op normstelling.
Agentic AI kan inzichtelijk maken hoe verschillende sectoren interventies beoordelen, waardoor besluitvorming explicieter en transparanter wordt. Deze voorstellen dienen steeds te worden getoetst door professionals op ethische aanvaardbaarheid, uitvoerbaarheid en effectiviteit.

Tijdens de uitvoering en monitoring worden interventies toegepast en resultaten systematisch gemonitord. Daarbij gaat het niet alleen om incidentcijfers, maar ook om percepties over (on)veiligheid van bewoners en professionals. AI kan daarbij real-time gegevens verwerken en trends detecteren in zowel objectieve als subjectieve indicatoren, waardoor bijsturen sneller mogelijk wordt. Via digitale platforms kunnen veiligheidsbelevingen continu worden gemeten en gekoppeld aan feitelijke indicatoren. Professionals kunnen zo terugkoppeling krijgen over afwijkingen en mogelijke risico's. Hierdoor ontstaat ruimte voor tijdige bijsturing van de aanpak.

In de evaluatiefase wordt vastgesteld in hoeverre interventies daadwerkelijk hebben bijgedragen aan een vermindering van geweld én een verbetering van veiligheidsbeleving. Politie kijkt naar incidentontwikkeling, zorg- en welzijnsorganisaties naar stabiliteit en ontwikkeling van jongeren, toezichthouders naar normconform gedrag en bestuur naar vertrouwen van bewoners. AI analyseert evaluatiedata en identificeert patronen die wijzen op succes of tekortkomingen. Bovendien genereert het suggesties voor bijstelling van beleid of interventies. Deze inzichten voeden de volgende cyclus, die een lerende en adaptieve aanpak oplevert.

"Succesvolle implementatie van EBW in combinatie met AI vereist een aantal randvoorwaarden."

Conclusie & discussie

De complexiteit van vraagstukken in het veiligheidsdomein en de ontwikkeling van AI vergroten het belang van professionalisering van integrale besluitvorming. De combinatie van EBW en AI biedt een kansrijke ontwikkelrichting waarin effectiviteit, legitimiteit en duurzame samenwerking centraal staan. Daarmee worden maatschappelijke effecten beter aantoonbaar en zijn betere ketenprestaties mogelijk. Hierbij blijft de professional onmisbaar voor normatieve afwegingen en contextduiding.

Succesvolle implementatie van EBW in combinatie met AI vereist een aantal randvoorwaarden. Essentieel is een stimulerende en lerende cultuur, waarin organisaties investeren in integraal samenwerken en zich blijven ontwikkelen in het bekwaam benutten van AI. Hiervoor dient actief ruimte te worden gecreëerd in tijd, capaciteit en samenwerking.

Door besluitvormingsprocessen te vernieuwen en EBW en AI te verbinden, ontstaat een werkwijze die complexe vraagstukken beter doorgrondt en gerichter aanpakt. Dit biedt het veiligheidsdomein een inspirerend perspectief voor een adaptievere, innovatievere en veerkrachtigere aanpak.

Over de auteurs

Athena van den Busken
Managing Consultant

Athena is managing consultant bij Capgemini in het Veiligheidsdomein. Athena richt zich op verandervraagstukken met een focus op de inzet van nieuwe technologie, integrale samenwerking en het versterken van professioneel handelen.

athena.vanden.busken@capgemini.com

https://www.linkedin.com/in/athena-van-den-busken

Anne Mooij
Onderzoeker politie eenheid Noord Holland

Anne is werkzaam bij de intelligence-organisatie van de Nationale Politie en richt zich op inhoudelijke en procesmatige vraagstukken rond de informatiepositie voor thema's in het politiedomein, waaronder jeugdcriminaliteit. Anne is aangesloten bij de Society of Evidence-based Policing Nederland (SEBP-NL). Haar bijdrage aan dit artikel is gebaseerd op de visie van SEBP-NL om een lerende professionele cultuur te bevorderen.

Voor wie werkt jouw model nou eigenlijk?

Hoe beinvloedt het gebruik van AI de normen en waarden waar organisaties voor staan?

Highlights

- AI-modellen zijn niet neutraal: ze weerspiegelen de data, ontwerpkeuzes en beperkingen waaruit ze zijn opgebouwd. Daardoor nemen organisaties ongemerkt wereldbeelden en waarden over in hun besluitvorming
- Organisaties moeten bewust beleid ontwikkelen om AI te laten aansluiten op hun eigen missie en maatschappelijke rol. Dat vraagt om mechanismen die de ideologische oriëntatie van modellen kritisch toetsen
- Certificering van AI-modellen is essentieel, maar complex doordat systemen zich in de praktijk anders kunnen gedragen dan in tests. Daarom zijn robuuste toetsingskaders en onafhankelijke controle nodig om betrouwbaarheid en eerlijkheid te waarborgen

AI lijkt objectief, maar draagt altijd impliciete normen en waarden mee. Deze zijn gevormd door data, ontwerpkeuzes en herkomst. Organisaties halen daarmee onbewust wereldbeelden naar binnen die invloed hebben op besluitvorming, terwijl grip en toetsing nog niet vanzelfsprekend zijn.

AI is niet meer weg te denken. Wellicht wordt het nog niet overal gebruikt, maar dat het overal impact gaat geven is wel duidelijk. Vanuit verschillende spelers zoals OpenAI, Anthropic, XAI, maar ook Microsoft en Meta worden geavanceerde AI-modellen voor iedereen wereldwijd beschikbaar gemaakt. De druk en noodzaak om hier wat mee te doen wordt steeds groter. Maar aan wiens kant staan die modellen nou eigenlijk?

Grote leveranciers claimen van alles en lijken te bewijzen dat de AI-modellen enorme betekenis hebben in de processen van vele organisaties. Maar bij vragen over specificaties worden de feiten wat dunner en worden de claims al wat meer richting vertrouwen geduwd. Maar welke ideologieën zijn er in het model vertegenwoordigd? Als we denkwerk uitbesteden, dan accepteren we impliciet de denkbeelden en overtuigingen van een andere partij. Zijn we wel bewust van welke denkbeelden dat zijn? En accepteren we daarmee deze invloeden in onze besluitvormingsprocessen?

Het op maat bouwen van een Large Language Model (of LLM) is complex en kostbaar, terwijl er gestandaardiseerde pakketoplossingen beschikbaar zijn.

Dus waarom zouden we maatwerkoplossingen bouwen voor generieke toepassingen zoals notulen schrijven, vertaalwerk of deskresearch? Van een standaardoplossing mag worden verondersteld dat het klopt. Dus bewijs en onderbouwing van de correcte werking is bij boekhoud- en HR-systemen intussen relatief eenvoudig. Tegelijkertijd bepaalt de notulist de waarheid en zitten er potentieel spannende nuanceverschillen tussen verschillende talen. Google maar naar een plaatje van een ‘fietser’ en een ‘cyclist’. Hoewel ‘cyclist’ de correcte vertaling is van fietser, wordt het verschil tussen een Nederlands en Amerikaans wereldbeeld onmiddellijk zichtbaar.

Maar nu komt AI. Met de introductie van op industriële schaal ingeleerde one-size-fits-all mega-modellen halen we ook onbewust een groot aantal fundamentele keuzes onze organisaties en onze samenleving binnen. AI-modellen dragen een impliciete ideologische oriëntatie met zich mee. Wanneer we AI-systemen inzetten voor personeelsbeoordeling dan accepteren we de managementfilosofieën, wereldbeelden en mensbeelden die in het systeem zijn ingebakken.

pakketoplossingen toepassen betekent het accepteren van keuzes van anderen.

De periode sinds de lancering van ChatGPT in november 2022 laat zien dat we met z'n allen verschillende AI-modellen wel heel makkelijk accepteren zonder dat we de specificaties kennen of begrijpen.

Wanneer een model wordt ingeleerd, wordt er een aantal principiële keuzes gemaakt. Om drie van die keuzes uit te lichten: de datakeuze, de inrichtingskeuzes en eventuele beperkingskeuzes op de output. Dit zijn niet de enige keuzes, maar wel de keuzes die het meest vormend zijn in hoe een model zich gedraagt.

1 De data

De eerste keuze is welke data worden er gebruikt. Worden de data op een bewuste manier gekozen of wordt het hele internet gebruikt?

Ongefilterd data verzamelen is makkelijk. Door te stellen dat meer beter is en dat alles wat de mensheid voort heeft gebracht ertoe doet klinkt heel verlicht, maar in essentie is het een goedkoop excuus om geen keuzes te maken. Het kost een hoop energie en bakken met rekenkracht om het te verwerken. Maar die is voor de grote spelers als Meta, Amazon en Microsoft, ruimschoots voorhanden.

Curatie vergt het maken van zorgvuldige keuzes. Welke data zijn nodig voor de essentie van hoe het model wordt gebruikt? Hoort daar de volledige Wikipedia in thuis? En fundamentalistische religieuze geschriften? Politieke manifesten? Economische doctrines? Dystopische science fiction en fantasy opussen? Of een darkweb pagina met een groeiende bak aan propaganda vanuit onsympathieke statelijke actoren?

En wanneer die data erbij horen, in welke verhoudingen staan die dan ten aanzien van de functies waarvoor het model gebruikt gaat worden. Voor een gedachtenprikkelende conversatie met een chatbot kan elk van deze bronnen een interessante bijdrage leveren, maar willen we ze ook betrekken bij het vaststellen van verzekeringspremies? Of de inkoop van grondstoffen? Of het opstellen van de HR-strategie voor de komende 10 jaar. Of misschien een mailtje om de buren te feliciteren?

2 De Inrichting

De tweede keuze gaat over het inrichten van het model: het tunen. Ergens moet iemand bepalen of het model zich op de juiste manier ontwikkelt. Iemand moet bepalen wat goed en fout is. En bij wiskunde is dat makkelijk. Het is binair: het is goed of het is fout. Maar als het gaat over moraliteit, ideologie, ethiek, of interpretaties over wat wettelijk toegestaan of niet, dan hangt het er nog wel vanaf wie die keuzes maakt. Bij de vraag of iets een goede weergave is van bijvoorbeeld een tafel, hangt af van wat ons referentiekader is. Een Japanner heeft daar wellicht een ander beeld bij dan een Nederlander. De ene tafel is niet beter dan de andere, maar ze zijn waarschijnlijk wel anders.

Een ander voorbeeld kan vanuit economische overtuigingen komen. Wat is een goede manier van geld verdienen? Volgens een econoom als Milton Friedman is dat, waarbij bedrijven tot de grenzen van de wet winst moeten maximaliseren en de wet daarbij wellicht aangepast moet worden. Bepaald anders is de Doughnut Economy van Kate Raworth die zich primair richt op duurzaamheid en maatschappelijke verantwoordelijkheid. Wat is goed vanuit een hyper-kapitalistisch Amerikaans perspectief, een meer sociaal-democratisch Europees perspectief of een sino-communistisch Chinees perspectief?

En dan waag ik me nog niet aan religie, fundamentalistische politieke overtuigingen of in welke mate geweld acceptabel is of niet. In essentie bepaalt de tuner wat goed gedrag van het model is, langs een duizelingwekkend aantal parameters die niet gedeeld worden met de afnemers.

3 De vangrails

Tot slot harde en zachte guardrails.

De harde guardrails beperken de uitkomsten van een model. Mag het model input accepteren en output genereren over potentieel controversiële onderwerpen? Denk aan seks, geweld, drugs, racisme en alle onderwerpen die gevoelsmatig geen plaats hebben in een IT-systeem. Dat klinkt logisch, tot organisaties zoals politie, hulpverlening en gezondheidszorg erachter komen dat het door hen gekozen AI-systeem het niet over hun onderwerpen wil hebben.

Veel modellen hebben woordfilters binnen hun guardrails die bijvoorbeeld medische termen als mogelijk scheldwoord zien. We hebben immers in het Nederlands de traditie om nare ziektes en geslachtskenmerken als beledigende krachttermen te gebruiken. Deze zogenoemde profanity filters vervangen dan deze potentieel aanstootgevende woorden met sterretjes en lakken ze virtueel weg uit een gespreksverslag. Ook zijn er guardrails die geen functioneel onderscheid tussen geslacht of etniciteit toestaan. Voor een toepassing in openbaar vervoer is dat prima, voor een webshop wordt het al wat onhandiger. Maar in medische context is het onderscheid van vitaal belang. Met andere woorden: veel hard gecodeerde guardrails lijken volledig voorbij te gaan aan de context van de toepassing.

Naast de harde guardrails zijn er ook zachtere guardrails. Noem het ontmoedigingen in het model om over bepaalde onderwerpen uit te wijden. Denk hierbij aan onzedelijke onderwerpen, drugsgebruik en geweldsoverwegingen. In de meeste openbare en commerciële toepassingen zullen die ontmoedigingen geen probleem zijn. Maar bij bijvoorbeeld strafrechtelijke toepassingen is wat onhandig als het model die onderwerpen blijft afhouden zonder dat de gebruiker dat weet.

AI-beleid

Elke organisatie zal een AI-beleid moeten formuleren om verantwoord bij hun mission statement te blijven. Daarbij moeten diverse perspectieven worden afgewogen. Perspectieven die elk hun hindernissen hebben om tot een goed geïnformeerde en betrouwbaar onderbouwde keuze te komen.

Hoe wordt er gekeken naar Large Models waarin met een sleepnet alle mogelijke data, inclusief toxische data, opgenomen zijn, versus Small Models die zijn getraind op strikt relevante en gecureerde data?

Hoe wordt een ideologische ijking gedaan? En hoe wordt gewaarborgd dat de ideologische oriëntatie overeenkomt met de eigen vision en mission statement en (bedrijfs-) cultuur?

Hoe interfereren hard gecodeerde guardrails met de gewenste toepassingen?

President Trump noemt Anthropic ‘woke leftist’ omdat zij vanuit hun ethische overwegingen hun model niet willen laten gebruiken voor gewelddadige militaire toepassingen. Diezelfde overwegingen zullen voor veel organisaties een reden zijn om de Anthropic modellen juist wel te gebruiken. Grok en XAI maken het mogelijk om politiek of seksueel geladen content te genereren die weinig met de feitelijke werkelijkheid gemeen heeft.

Hoe worden de eigenschappen van de verschillende gekozen modellen tegenover elkaar gebalanceerd? En wordt er gebruik gemaakt van een diversiteit in modellen of wordt gekozen voor een digitale monocultuur?

Het ligt voor de hand dat een AI-model impliciet overtuigingen meebrengt die in lijn zijn met die van de publicerende organisatie. Microsoft zal een model uitbrengen wat voldoet aan hun standaarden. Grok gedraagt zich in lijn van het gedrag van een excentrieke en megalomane multimiljardair. Deepseek zal zich houden aan de regels van de Chinese Volksrepubliek. Geen van deze partijen zullen hun ingrediënten vermelden op de bijsluiter. Toch zullen we daar inzicht in moeten hebben voordat deze modellen een sleutelrol krijgen binnen het AI-beleid van een organisatie en daarmee in onze maatschappelijke verhoudingen.

Dat betekent dat we een soort van alignment-test nodig hebben hebben die AI-modellen profileert en hun gedrag en voorkeuren in kaart brengt. Wellicht zelfs certificerende instanties die de veiligheid van de modellen toetsen en, zoals een KEMA-keurmerk, onderbouwd vertrouwen geven dat de modellen voldoen aan wat wij ervan mogen verwachten.

Voor dit moment is het al lastig om certificeringsdimensies te formuleren. We gaan er niet komen met tests en criteria die we voor mensen opstellen bij persoonlijkheidstests of sollicitatieprocedures. Dit soort tests lijken voor de hand te liggen, want de user interface van een model oogt zo menselijk dat het natuurlijk aanvoelt om de modellen als mens te behandelen. Maar het woord ‘natuurlijk’ geeft al aan dat het niet van toepassing is. Een AI is per definitie niet natuurlijk, al willen we dat graag geloven.

Digital Dieselgate

Waar getest wordt, wordt gefraudeerd. Waar geavanceerde tests worden ingezet, wordt geavanceerd gefraudeerd. Dat klinkt logisch, tot waarbij de boardcomputer van auto’s signaleerden dat ze getest werden op een rollerbank, en vervolgens een ander motorgedrag gingen laten zien. Alles om maar door de uitstoottests te komen.

De eerste signalen dat een AI-model zich anders gedraagt in een test zijn al wat ouder. Dat mag een indicatie zijn dat AI-modellen zich niet makkelijk laten certificeren. Hoe generieker, groter en geavanceerder een model is hoe moeilijker het is om onderscheidende karakteristieken te identificeren. Daarnaast is het in het belang van de publicerende instanties dat hun model goedgekeurd wordt. Daar verdienen zij immers hun geld mee. De al dan niet bewuste neiging om te frauderen wordt daarmee wel erg verleidelijk. En welbeschouwd hebben de Techbedrijven nog wel een paar punten te laten zien waar het ethisch gedrag betreft.

Conclusie

AI-modellen hebben door de manier waarop ze gebouwd zijn een impliciete ideologische oriëntatie. Dit komt voort uit de datakeuzes waarop een AI-model getraind is, de manier waarop getraind en getuned is en de harde guardrails die door de leverancier worden opgelegd in het model.

Gebruikende organisaties introduceren daarmee deze ideologieën in hun bedrijfsvoering en daarmee in hun positie in de samenleving.

Om tot een geïnformeerde en verantwoorde keuze van een of meerdere AI-modellen te komen moeten er dimensies worden geformuleerd waarop deze modellen worden beoordeeld.

Elke organisatie zou een AI-policy moeten opstellen en handhaven. Hierin moet worden bepaald hoe AI in het hart van hun bedrijfsvoering past. Hoe past AI in de backofficeprocessen, in het voortbrengingsproces en in het vervullen van de mission statement. En vooral ook hoe en met welke onderbouwing worden daar verantwoorde keuzes gemaakt.

Met de haast om AI-oplossingen te adopteren nemen organisaties al dan niet bewust risico’s om impliciete gedachtegangen en besluitvormingscriteria in te bedden in hun werkzaamheden en daarmee in hun rol in onze samenleving. Bij onoordeelkundig gebruik heeft dat langdurige gevolgen voor onze maatschappelijke veiligheid.

Want… voor wie werkt jouw model nou eigenlijk?

Over de auteur

Henk Vermeulen
Innovation Activist

Henk is een gepassioneerd innovatie activist. Met al 40 jaar een actief ‘geek’ hart en 30 jaar IT-ervaring, gaat hij graag met technologie aan de haal om te zien wat de betekenis kan zijn. Hij heeft talloze concepten geformuleerd die de mogelijkheden verkennen. Want: “je moet overmorgen verkennen om morgen relevant te zijn, anders kan je vandaag alleen maar doen wat je gisteren ook al deed”.

https://www.linkedin.com/in/henkvermeulen/

Data Mesh bij Defensie: dataproducten voor een effectieve krijgsmacht

Hoe helpt Data Mesh Defensie om optimaal gebruik te maken van data?

Highlights

- De krijgsmacht digitaliseert en maakt steeds meer gebruik van data
- Om dit te faciliteren, moeten dataproducten fit for use beschikbaar zijn
- De organisatorische benadering die hiervoor kan zorgen, heet Data Mesh
- In de Data Mesh-gedachte wordt data behandeld als asset en worden de voordelen van centrale en decentrale modellen samengebracht
- Met Data Mesh kan Defensie interoperabiliteit en waardecreatie door AI maximaliseren om zo een effectievere krijgsmacht te worden

Het behandelen van data als asset en het snel en fit for use beschikbaar stellen van dataproducten helpt Defensie interoperabiliteit en waarde uit AI te maximaliseren.

De transformatie naar een informatiegestuurde krijgsmacht is in volle gang. Bij Defensie genereren, verwerken, gebruiken en delen operationele eenheden, stafafdelingen, onderhoudsteams en shared-service organisaties steeds vaker en steeds meer data. Om die data optimaal te benutten, moet deze fit for use beschikbaar zijn. De manier om dit te realiseren? Data Mesh.

Het Amerikaanse Ministerie van Defensie is al met deze organisatorische verandering gestart: zij implementeren Data Mesh om onder andere op grote schaal AI-toepassingen te kunnen gebruiken en om interoperabiliteit tussen alle militaire domeinen mogelijk te maken (CJADC2: Combined Joint All-Domain Command and Control), iets wat ook voor de Nederlandse krijgsmacht cruciaal is om effectief te opereren.

In dit artikel wordt beschreven wat Data Mesh is, hoe het werkt en hoe het Defensie kan helpen dataproducten fit for use beschikbaar te stellen om zo een volgende stap te zetten richting informatiedominantie. Vorig jaar deelden we in Trends in Veiligheid al het belang van kwalitatief hoogwaardige data in het streven naar informatiedominantie: het vermogen om sneller, beter en slimmer informatie te verzamelen, verwerken en verspreiden dan een tegenstander. Eén van de sleutels? Goed georganiseerde data governance waar data eigenaren en data stewards zorgdragen voor “hun” data zodat het effectief en verantwoord gebruikt kan worden voor strategische, operationele en tactische doelen. Het vormt op die manier de basis voor waardecreatie door technieken als AI.

Naast die goed georganiseerde basis is meer nodig: data kan pas waarde leveren als het gebruikt wordt in besluitvormingsprocessen. Om hierin te voorzien, dienen dataproducten fit for use beschikbaar te zijn. Dit betekent dat data eenvoudig, veilig en in consumeerbare (kwalitatief, begrijpelijk, vindbaar, afgebakend) producten gebruikt moet kunnen worden bij het maken van beslissingen. Die beslissingen zijn legio en verschillen van het maken van passende planningen tot het analyseren van veiligheidsincidenten, het bestellen van voldoende geschikt materieel en het maken van tactische beslissingen in het veld: iedereen maakt gebruik van data. En iedereen wil die data direct beschikbaar hebben.

Centraal georganiseerde modellen zijn vaak onvoldoende schaalbaar en flexibel om deze urgente en groeiende databehoefte duurzaam te ondersteunen. Tegelijkertijd kan een volledig decentraal model zorgen voor versplintering en risico’s op het gebied van eigenaarschap, definities en het delen van data. Specifiek dit laatste is cruciaal voor een krijgsmacht die multi-domein (land, lucht, zee, cyber en space) en joint (met partners) optreedt. Maar hoe moet het dan wel georganiseerd worden? Data Mesh kan uitkomst bieden, waarin data beschouwd wordt als asset of product, met een eigenaar en afspraken over o.a. betekenis, kwaliteit en gebruiksvoorwaarden.

Wat is Data Mesh?

Data Mesh is een organisatorische en architecturale benadering van data, waarbij dataverantwoordelijkheid verdeeld wordt over domeinteams, terwijl een centraal (platform) team zorgt voor gezamenlijke afspraken over semantiek, kwaliteit, beveiliging en uitwisseling. Het beschouwen van data als asset of (waardevol) product zorgt voor eigenaarschap en de juiste zorg van de juiste mensen: inhoudelijke zorg van de domeinteams en technische ondersteuning en centrale afspraken vanuit het centrale platform. Het platform zelf dwingt dergelijke afspraken zo veel mogelijk automatisch af. Denk bijvoorbeeld aan het automatisch stoppen van toegang zodra de termijn van een Data Sharing Agreement afloopt, het continu doen van datakwaliteitschecks en het verplicht toevoegen van relevante metadata (zoals data eigenaar, betekenis en classificatie) bij het publiceren van data op het dataplatform.

Laten we wat beter naar de vier kenmerken van Data Mesh kijken:

01 De data as a product-gedachte betekent dat data beschouwd wordt als iets dat waarde heeft (een asset) en geconsumeerd wordt. Hiermee heeft de dataproduct-owner dus de gebruiker (of klant) in gedachte. Waar voorheen datasets beschikbaar gesteld werden (attributen, tabellen, extracten), worden binnen Data Mesh fit for use dataproducten beschikbaar gesteld: een afgebakend en direct bruikbaar product met een herkenbare naam, zoals Apache-onderhoudsplanning of personeelsrooster.

02 Domeingedreven dataverantwoordelijkheid houdt in dat domeinteams end-to-end verantwoordelijk zijn voor hun dataproducten. De mensen die de bedrijfsvoering begrijpen, beheren ook de data, zowel functioneel als technisch. Dit zorgt ervoor dat keuzes over interpretatie en prioriteit op de juiste plek belegd worden. Naast het feit dat deze mensen het domein het beste kennen (interpretatie), weten zij vaak ook waar en hoe de data de meeste waarde kan toevoegen (prioriteit). Zo wordt de onderhoudsplanning van een wapensysteem gemaakt door teams binnen het materieel-logistieke domein, mogelijk gebruikmakend van een dataproduct uit het personeelsdomein met de werkroosters en skills van onderhoudsmedewerkers.

03 Een centraal, faciliterend platform (team) stelt de domeinteams in staat autonoom dataproducten te bouwen. Het centrale platform stelt hiervoor gestandaardiseerde tooling beschikbaar. Dataproducten worden technisch op het centrale platform beschikbaar gesteld. Het platform stelt kaders aan de dataproducten: wanneer is iets een fit for use dataproduct?

04 Federated computational governance zorgt voor gedeelde, schaalbare én (deels) automatische governance. De kaders die het centrale platform stelt, worden automatisch afgedwongen door het platform. De naleving hiervan gebeurt continu decentraal door de domeinteams.

Hoe kan dit werken binnen Defensie?

Defensie is ingericht in procesdomeinen, zoals Operaties, Materieel-logistiek, Personeel & Gezondheidszorg en Financiën & Control. Deze functionele indeling leent zich goed voor het decentraal beleggen van dataverantwoordelijkheid. Per domein kan een data eigenaar verschillende dataproduct-owners aansturen die end-to-end verantwoordelijk zijn voor de verschillende dataproducten.

Eén van de uitdagingen bij Defensie is dat de organisatie ook (en bovenal) is ingedeeld in verschillende defensieonderdelen: Luchtmacht, Landmacht, Marine, Marechaussee en ondersteunende onderdelen. Deze onderdelen opereren deels paars – Defensiebreed (vertegenwoordiging van alle “kleuren”) - maar ook deels individueel en autonoom. Dat maakt dat er binnen de procesdomeinen ook aandacht dient te zijn voor de verschillende kleuren, zoals bijvoorbeeld een paars dataproduct over (defensiebrede) materiële gereedheid en eventueel specifieke aanvullingen voor een fregat van de Marine.

Een dataproduct is opgebouwd uit data. Deze data zelf dient o.a. beschikbaar, betrouwbaar, volledig en begrijpbaar te zijn (zie ook het artikel over data governance in Trends in Veiligheid 2024-2025). De Data Mesh-gedachte gaat een stap verder en stelt medewerkers in staat direct gebruik te maken van hoogwaardige dataproducten ter ondersteuning van hun doelen. Gebruikers hoeven dus niet zelf de juiste attributen en tabellen samen te voegen maar kunnen direct gebruikmaken van een gedefinieerd product

Voorbeelden van dergelijke dataproducten met bijbehorende doelen zijn:

- MQ-9 Intelligence Surveillance Reconnaissance (ISR) t.b.v. het opbouwen van situational awareness.
- Materiële voorraad t.b.v. het voorbereiden van uit te voeren onderhoud.
- Uitputting van financiële middelen t.b.v. het maken van een project- of programmaplanning.
- Medewerkersgegevens t.b.v. het uitbetalen van salarissen.

"Data Mesh zorgt ervoor dat zulke administraties, of dataproducten, beschikbaar gesteld kunnen worden aan afnemers, op centraal en decentraal niveau."

Het dataproductteam binnen het procesdomein zorgt voor dataproducten voor de verschillende Defensieonderdelen, terwijl het platform (team) dit op een veilige en schaalbare manier faciliteert. Het centrale team zorgt voor zaken als infra, opslag en tooling zodat dit consistent is voor de hele organisatie.

Hoe draagt Data Mesh bij aan waardecreatie?

Data leidt pas tot waarde zodra het wordt omgezet tot informatie en gebruikt wordt in besluitvormingsprocessen. Zo kan bijvoorbeeld een feilloze voorraadadministratie tot waarde leiden omdat het ondersteunt bij juiste en tijdige beslissingen op het gebied van onderhoudsplanning en aanschaf van nieuw materiaal en leidt scherpe situational awareness, opgebouwd uit verschillende sensordata, tot waarde omdat de operator in het veld op het juiste moment de juiste beslissing kan nemen (zie ook het artikel van Johan de Jong over het gebruik van inlichtingendata in het militaire besluitvormingsproces).

Data Mesh zorgt ervoor dat zulke administraties, of dataproducten, beschikbaar gesteld kunnen worden aan afnemers, op centraal en decentraal niveau. Deze interoperabiliteit zorgt voor effectievere samenwerking tussen de verschillende Defensieonderdelen. De dataproducten zelf vormen de input voor AI-toepassingen. Is de kwaliteit van die input hoog, zal de output dat veelal ook zijn. Door data te behandelen als een asset en dataproducten fit for use beschikbaar te stellen, maximaliseer je de waardecreatie door AI.

Welke stappen kan Defensie nu al zetten?

Om dataproducten beschikbaar te stellen, is het belangrijk dat er nauwe samenwerking ontstaat tussen de dataproducttеams en de (potentiële) gebruikers van de dataproducten. Het opzoeken van deze samenwerking is een eerste stap waar direct mee gestart kan worden (en waar u nooit mee stopt). Om vervolgens echt werk te maken van Data Mesh kan de volgende benadering gehanteerd worden:

1. Kies 1-2 dataproducten binnen een domein dat relatief volwassen is en ontwikkel deze zodat ze door potentiële afnemers geconsumeerd kunnen worden.
2. Definieer wat fit for use betekent: wanneer is iets een consumeerbaar dataproduct? Wat zijn de eisen? Denk hierbij bijvoorbeeld aan nauwkeurigheid, volledigheid, actualiteit en betrouwbaarheid, maar ook aan toegankelijkheid, veiligheid en de manier van beschikbaar stellen van het dataproduct.
3. Richt een centraal platform op met bijbehorende federated computational governance: waar de eerste dataproducten volledig decentraal ontwikkeld kunnen worden (zonder centrale ondersteuning) zit de kracht van Data Mesh juist in de federatieve governance, waarbij decentraal ontwikkeld wordt met behulp van centrale ondersteuning.
4. Schaal op: kies geleidelijk meer domeinen en dataproducten om te ontwikkelen en beschikbaar te stellen. De domeinteams én het centrale platformteam kunnen zo organisch groeien en leren.

Het doorlopen van bovenstaande stappen is cruciaal in de ontwikkeling van Data Mesh. Om dit echt te doen slagen is het van belang dat Defensie dit organisatorische vraagstuk volledig omarmt: data moet behandeld worden als asset. Alleen door deze culturele omslag te maken kan de potentiële waarde van data benut worden.

Conclusie

Data Mesh zorgt voor het beschikbaar stellen van dataproducten, die vervolgens geconsumeerd kunnen worden door verschillende Defensieonderdelen (multi-domein) en partners (joint) om te gebruiken bij het maken van beslissingen. Dit federatieve stelsel (centraal beschikbaar stellen en decentraal gebruiken) zorgt voor interoperabiliteit en effectieve samenwerking tussen verschillende onderdelen. Doordat dataproducten per domein fit for use beschikbaar zijn, wordt de tijd die het kost om tot inzichten te komen middels AI en zo waarde te creëren flink verkort, in de bedrijfsvoering én in de operatie door bijvoorbeeld dataproducten met ISR-data. In veel organisaties gaat de meeste tijd in de ontwikkeling van AI-producten namelijk naar het beschikbaar maken, combineren en schoonmaken van data. Binnen Data Mesh gebeurt dit één keer en kunnen dataproducten vervolgens worden hergebruikt. Door klein te beginnen en iteratief uit te breiden kan Defensie met Data Mesh nu een volgende stap zetten richting informatiedominantie en een effectievere krijgsmacht.

Over de auteur

Jeroen Jeschke
Expert datagedreven werken

Jeroen is werkzaam bij Capgemini Insights & Data. Hij is een expert op het gebied van datagedreven werken en werkt momenteel als projectmanager aan een organisatiebrede data governance implementatie bij het Ministerie van Defensie.

jeroen.jeschke@capgemini.com

https://www.linkedin.com/in/jeroenjeschke/

Enterprise Agentic Intelligence voor het veiligheidsdomein

Werken onder architectuur maakt Enterprise Agentic Intelligence toepasbaar en veilig

Highlights

- Enterprise Agentic Intelligence maakt mensen vrij voor hun kerntaken
- Werken onder architectuur zorgt dat de risico's bewaakt worden
- Werken onder architectuur stuurt stapsgewijze en verantwoorde invoering
- Begin waar de volgende drie samenkomen: impact in de bedrijfsvoering, veilige uitvoerbaarheid en noodzaak dat mensen meer tijd aan kerntaken kunnen besteden

Nieuwe technologische ontwikkelingen, zoals AI-agenten, bieden het veiligheidsdomein kansen om uitvoeringskracht te vergroten en professionals te ontlasten.

Tijd vrij voor kerntaken dankzij Enterprise Agentic Intelligence

Het veiligheidsdomein staat onder druk: uitvoerende professionals besteden een groeiend deel van hun tijd aan administratie, verantwoording en afstemming. Dit gaat ten koste van inzet in de praktijk. Uit verschillende rapporten blijkt dat deze uitvoeringsdruk een combinatie is van personeelskrapte en organisatorische complexiteit[1][2][3]. Dit staat op gespannen voet met maatschappelijke verwachtingen rond wijkgericht politiewerk, toezicht, opsporing, vervolging en hulpverlening.

Enterprise Agentic Intelligence (EAI) adresseert precies die spanning door digitale collega's in te zetten die daarvoor geschikte werkzaamheden overnemen, leren van feedback en actief samenwerken met menselijke collega's.

Stel je voor: een AI-agent verwerkt automatisch meldingen van overlast die via verschillende kanalen binnenkomen. Dit maakt een agent vrij die uren kwijt is aan het handmatig invoeren, filteren en doorzetten van deze meldingen. De AI-agent sorteert, analyseert de informatie direct en koppelt relevante dossiers automatisch aan lopende zaken. Hierdoor kan de agent zich sneller richten op acute incidenten in de wijk, en de toezichthouder sneller inspelen op patronen.

1) De Koning, J., Gravesteijn, J., & De Vleeschouwer, E. (2019). Werkbelasting en werktevredenheid bij de politie? Een onderzoek onder wijkagenten en teamchefs (SEOR Working Paper 2019/1). Rotterdam: SEOR. [SEOR-Worki...de-politie | PDF]

2) Oprins, E., 't Hart, M., & Dhondt, S. (2022, maart). Doorbraak in schreeuwend personeelstekort vraagt nieuw perspectief (NPOV Whitepaper). Soesterberg: TNO/NPOV. [oprins-202...-doorbraak | PDF]

3) Nationale Politie. (2024). Jaarverantwoording 2023 – Thema: Politiecijfers 2024. Den Haag: Nationale Politie.

Wat is Enterprise Agentic Intelligence (EAI)?

EAI is een organisatiebreed stelsel van autonome AI-agents, digitale collega's in kern- en ondersteunende processen, die waarnemen, besluiten en handelen binnen vooraf gedefinieerde grenzen, in samenwerking en onder toezicht van mensen.

Kernonderdelen van elke AI-agent

01 Hulpmiddelen: uitvoeren van concrete taken (documenten opstellen, dataverwerking, aansturen van apparatuur).

02 Redeneren: snelle patroonherkenning én zorgvuldige, stapsgewijze afwegingen met large language models voor doordachte ondersteuning.

03 Geheugen & leren: korte- en langetermijngeheugen en continue aanpassing op basis van feedback, zodat eerdere ervaringen worden benut voor het verbeteren van de uitvoering van zijn taak.

In multi-AI-agent-opstellingen werken digitale en menselijke collega's samen. Het doel daarvan is het optimaliseren van processen en het verhogen van de slagkracht binnen het veiligheidsdomein. Het is dus een samenwerking waarin AI-agenten routinematige taken uitvoeren, en mensen zich richten op complexere situaties en besluitvorming.

EAI is een nieuwe en veelbelovende ontwikkeling binnen het gebruik van large language models geavanceerde AI-taalprogramma's die de 'motor' vormen achter AI-agents. De technologie en de bijbehorende standaarden bevinden zich nog in een fase van voortdurende ontwikkeling. Succesvolle EAI-invoering is echter geen druk op de knop: het vraagt een doordachte aanpak.

Onder architectuur naar betrouwbare AI in de uitvoering

De nieuwheid van deze technologie brengt risico's met zich mee bij de integratie in de dagelijkse bedrijfsprocessen, het beheren van informatie en de acceptatie ervan door medewerkers en burgers. Goed verandermanagement is dus een voorwaarde.

Enterprise architectuur speelt een sleutelrol in het beheersen van de risico's en een stapsgewijze en verantwoorde invoering. Het slaat de brug tussen vier essentiële vragen:

- **Strategie:** Waar willen we naartoe met EAI en welk voordeel verwachten we ervan?
- **Bedrijfsvoering:** Wat verandert EAI aan sturing en toezicht van onze processen?
- **Gegevens:** Hoe borgen we de gegevenskwaliteit en vertrouwelijkheid?
- **IT:** Welke systemen en tools zijn benodigd om deze verandering te ondersteunen?

Door te werken onder architectuur worden keuzes consistent gemaakt.

Door deze integrale benadering ontstaat er een fundament voor duurzame innovatie in het veiligheidsdomein. Digitale AI-agenten fungeren als katalysator voor procesverbetering, waarbij ze niet alleen de administratieve lasten verlichten, maar ook bijdragen aan een snellere besluitvorming en een hogere kwaliteit van dienstverlening.

Waar te beginnen met AI-agenten? Een praktisch selectiekader

Een succesvolle strategie is om taken voor AI-agenten te kiezen die snel aantoonbare waarde leveren, passen in de bestaande bedrijfsprocessen en voldoen aan publieke waarden. Begin klein en meetbaar en stuur daarbij vanuit proces en architectuur, niet vanuit tooling.

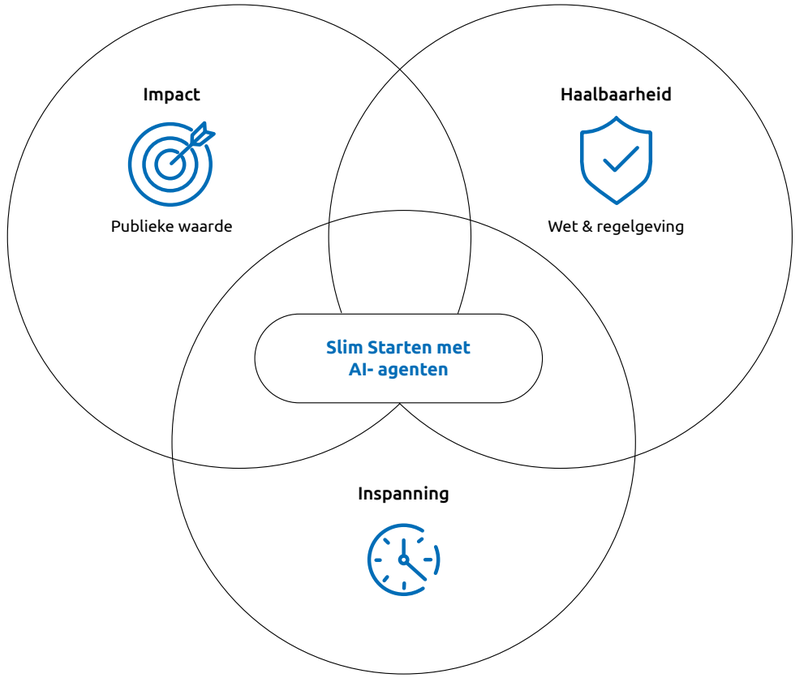
Daarbij geldt een eenvoudige vuistregel: gebruik AI-agenten uitsluitend voor afgebakende, laag-variabele ondersteuning zonder directe rechtsgevolgen (zoals zoeken, samenvatten en dossieropbouw). Zet ze niet in waar empathie, discretionaire bevoegdheid of wettelijk mandaat vereist is (bijv. slachtofferzorg, GRIP-opschaling, sancties/dwangmiddelen). De mens beslist en is eindverantwoordelijk; de AI-agent adviseert transparant (logging, escalatie) en wordt kleinschalig en meetbaar ingevoerd.

Taken worden geselecteerd op basis van drie criteria:

Impact: kortere doorlooptijden, minder fouten, betere dienstverlening, lagere kosten/lasten.

Haalbaarheid: technische en organisatorische realiseerbaarheid binnen wet- en regelgeving, beschikbaarheid van data en draagvlak.

Inspanning: benodigde tijd, middelen en verandercapaciteit voor implementatie en beheer.



Afbeelding 1 Een praktisch selectiekader voor AI-agenten

Impact (wat levert het op?)

We beoordelen de impact op vier punten die de slagkracht en kwaliteit van de rechtsstaat vergroten en de uitvoeringslast verlagen:

- **Schaalbaarheid:** is de aanpak inzetbaar in meerdere teams of onderdelen?
- **Tijdsbesparing bij vastleggen, terugvinden en overdracht:** door stappen als intake, uitwerken en samenvatten te automatiseren.
- **Kwaliteit en betrouwbaarheid:** minder fouten, betere dossiers en een goed te volgen spoor.
- **Publieke waarde:** sneller en beter handelen verhoogt veiligheid, verbetert dienstverlening en versterkt rechtszekerheid en vertrouwen.

Haalbaarheid (kunnen we dit nu verantwoord doen?)

We toetsen haalbaarheid op vier punten die rechtmatigheid borgen, risico's beperken en de uitvoering voorspelbaar maken:

- **Procesafspraken en uitzonderingen:** staan stappen en werkinstructies vast en zijn uitzonderingen vooraf beschreven?
- **Gegevens en toegang:** is de juridische grondslag in orde en is de privacy-toets gedaan (DPIA)? Gebruiken we alleen noodzakelijke gegevens, zijn ze helder ingedeeld en gelabeld, en is toegang tot context , referentie en basisgegevens geregeld?
- **Controleerbaarheid en kwaliteit:** blijft de mens aan het stuur en zijn besluiten uitlegbaar en herstelbaar? Leggen we handelingen aantoonbaar vast (wie–wat–wanneer), gelden duidelijke uitvoeringsregels en volgen we kengetallen zoals nauwkeurigheid, volledigheid en doorlooptijd?
- **Risico en veilige uitvoering:** werken we volgens afgesproken ontwerpprincipes, testen we eerst in een afgeschermde proefomgeving, en zijn terugvalopties en escalatieroutes voor toezicht op AI-toepassingen vooraf geregeld?

Inspanning (wat kost het om te starten?)

Bij het inschatten van de startinspanning hanteren we de volgende criteria:

- **Documentatie**: Is het huidige proces volledig, actueel en begrijpelijk beschreven? Is dit inclusief alle uitzonderlijke situaties?
- **Koppelingen met andere systemen**: Hoeveel koppelingen zijn nodig en bestaan er standaardkoppelingen? Is de benodigde gegevensuitwisseling haalbaar?
- **Verandergereedheid**: Is het eigenaarschap belegd? Zijn training, begeleiding en toezicht geregeld, en zijn de ondernemingsraad en privacyfunctionaris tijdig betrokken?
- **Klein beginnen**: Starten we met een beperkte proef in één stap van een keten, met duidelijke doelen, meetpunten en vooraf afgesproken stop- en opschaalcriteria?

Slim starten met EAI: concreet resultaat zonder complexiteit

De uiteindelijke selectie van taken voor AI-agenten komt tot stand na een analyse van de bestaande processen. De ideale eerste toepassing bevindt zich op het snijvlak waar de elementen impact, haalbaarheid en inspanning samenkomen:

- substantiële impact op de bedrijfsvoering
- een veilige en heldere uitvoerbaarheid
- én een beheersbare inzet van mensen en middelen.

Begin slim: ambitieus, met focus en vertrouwen

Kies een EAI-project dat snel zichtbaar resultaat oplevert en niet te complex is. Richt je op een praktische toepassing met duidelijke opbrengsten om vertrouwen te winnen. Het AI Witness-project toont aan dat klein beginnen met focus zorgt voor snelle successen en meer enthousiasme.

IT voor EAI: soeverein en wendbaar

Voor EAI zijn nieuwe hulpmiddelen en systemen nodig. Omdat in het veiligheidsdomein vaak met vertrouwelijke informatie wordt gewerkt, is soevereiniteit een randvoorwaarde: de organisatie moet zeggenschap hebben over waar gegevens staan, wie erbij kan en hoe ze worden gebruikt. De systemen die EAI mogelijk maken, waaronder grote LLMs, moeten aan die eisen kunnen voldoen. Tegelijkertijd is de technologie achter EAI volop in ontwikkeling. Daarom kiezen we voor doen én leren: gecontroleerd experimenteren in afgebakende omgevingen, nog geen onomkeerbare leverancierskeuzes maken en stap voor stap opschalen zodra veiligheid, kwaliteit en meerwaarde aantoonbaar zijn. Zo blijft er ruimte om keuzes bij te stellen op basis van nieuwe inzichten, ervaringen uit pilots en technologische vooruitgang.

Van visie naar uitvoering

EAI kan de balans tussen het teveel aan administratie en de nood aan inzet op kerntaken herstellen. Door expliciet te sturen vanuit strategie, bedrijfsvoering, gegevens en IT, en door klein, transparant en meetbaar te beginnen, worden risico's beheerst en ontstaat een solide basis om verantwoord op te schalen. Deze aanpak waarborgt soevereiniteit, controleerbaarheid en publieke waarde.

Dit artikel laat zien dat een enterprise architectuurbenadering daarbij essentieel is om deze kansen te verzilveren. Niet als rem op innovatie, maar als richtinggevend kader: door te starten vanuit bestaande processen, verantwoordelijkheden expliciet te beleggen, risico's inzichtelijk te maken en toepassingen klein, transparant en meetbaar te introduceren. Voor organisaties in het veiligheidsdomein ligt hier een duidelijke oproep: benut de mogelijkheden van AI-toepassingen door ze onder architectuur te ontwikkelen, zodat publieke waarde, beheersbaarheid en de menselijke maat structureel geborgd blijven in de uitvoering. Hiermee wordt een eerste, concrete stap gezet in een bredere ontwikkeling waarin AI-toepassingen steeds verder zullen doorwerken in de inrichting en uitvoering van het veiligheidsdomein.

Over de auteurs

Maurice Driessen
Principal consultant & Chief architect

Maurice is principal consultant en chief architect met een achtergrond in enterprise- en solution-architectuur binnen de publieke sector. Hij is de afgelopen vijf jaar als architect betrokken geweest bij de digitalisering van de forensische onderzoeksketen, met een focus op samenhang tussen processen, informatievoorziening en technologie binnen het veiligheidsdomein.

maurice.driessen@capgemini.com

https://www.linkedin.com/in/mauricedriessen/

Michael Stoelinga
Principal consultant & Senior architect

Michael is principal consultant en senior architect met ruime ervaring in digitaliseringsvraagstukken binnen de publieke sector. Hij werkt op het snijvlak van architectuur, governance en organisatieverandering en is betrokken bij complexe trajecten binnen het veiligheids en bestuursdomein, met aandacht voor uitvoerbaarheid en publieke waarden.

michael.stoelinga@capgemini.com

https://www.linkedin.com/in/mstoelinga/

Interview:

Wim Pieter Huijsman

Directeur bedrijfsvoering
bij de Landelijke Meldkamer
Samenwerking

De toekomst van werk in het veiligheidsdomein vraagt om andere keuzes

Wat gebeurt er als het werk waarvoor je organisatie ooit is ingericht, volledig verandert?

En dan niet per se door één grote disruptie, maar door een optelsom van technologische ontwikkelingen, geopolitieke verschuivingen en veranderende verwachtingen van burgers. Dan ontstaat er een situatie waarin niet alleen systemen moeten worden aangepast, maar ook het denken over werk zelf. Voor Wim-Pieter Huijsman, directeur bedrijfsvoering bij de Landelijke Meldkamer Samenwerking (LMS), zijn dit soort vraagstukken dagelijkse kost. In zijn loopbaan bij onder meer TNO, Defensie en de politie zag hij hoe technologie en organisatieontwikkeling steeds opnieuw schuren, botsen en opnieuw hun weg moeten vinden. “Ik kijk altijd naar drie elementen,” zegt hij. “Wat wil je bereiken als organisatie, welke technologie heb je daarvoor nodig en welke rol speelt de mens daarin? Als je die drie in samenhang bekijkt, ontstaan er realistische oplossingen. Voor Wim-Pieter Huijsman, directeur bedrijfsvoering bij de Landelijke Meldkamer Samenwerking (LMS), zijn dit soort vraagstukken dagelijkse kost. In zijn loopbaan bij onder meer TNO, Defensie en de politie zag hij hoe technologie en organisatieontwikkeling steeds opnieuw schuren, botsen en opnieuw hun weg moeten vinden. “Ik kijk altijd naar drie elementen,” zegt hij. “Wat wil je bereiken als organisatie, welke technologie heb je daarvoor nodig en welke rol speelt de mens daarin? Als je die drie in samenhang bekijkt, ontstaan er realistische oplossingen.”

Digitale soevereiniteit

Een van de meest ingrijpende verschuivingen die Huijsman ziet, vindt plaats in het internationale speelveld. De geopolitieke ontwikkelingen hebben volgens hem directe gevolgen voor hoe organisaties omgaan met technologie en data. “We zien dat de vanzelfsprekendheid van internationale afhankelijkheden afneemt. Waar we jarenlang konden bouwen op vaste verhoudingen, bepalen landen en machtsblokken veel nadrukkelijker hun eigen positie. Dat geldt ook voor Europa. Dan moet je opnieuw nadenken over je afhankelijkheden, wat de impact daarvan is en hoe je die mogelijk opnieuw moet inrichten.”

Afhankelijkheden zitten niet alleen in energie of grondstoffen, maar ook in digitale infrastructuur. “Als jouw kritische systemen draaien op technologie van een partij buiten jouw invloedsfeer, dan heb je al een groot risico. Niet omdat het geheid een keer misgaat, maar vooral omdat je het systeem niet volledig zelf in de (eigen) hand hebt. En in het veiligheidsdomein is soevereiniteit fundamenteel. Je wilt en móet zelf kunnen bepalen hoe je systemen functioneren, hoe je data wordt gebruikt en wie daar toegang toe heeft. De huidige ontwikkelingen vragen dus om andere keuzes dan we tien jaar geleden zouden maken.”

Als technologie sneller ontwikkelt dan de toepassing

Ook de rol van technologie groeit in een tempo dat moeilijk bij te houden is en dat geldt zeker voor kunstmatige intelligentie. Volgens Huijsman zit de complexiteit echter niet in de technologie zelf, maar vooral in de toepassing ervan. “Er wordt veel gesproken over wat AI allemaal kan en gaat doen. En terecht, want de ontwikkelingen gaan snel. Maar als je kijkt naar hoe AI daadwerkelijk wordt toegepast in organisaties, dan zie je dat dat vaak stokt. Bij heel specifieke toepassingen werkt AI uitstekend, denk aan beeldanalyse of medische diagnostiek. Daar is de opdracht namelijk heel duidelijk en kun je AI zeer gericht trainen.Maar zodra je AI in een complexere context wilt toepassen, waarin het onderscheid tussen ‘waar en onwaar’ genuanceerd ligt of als interpretaties en afwegingen worden gevraagd, dan zie je dat hallucinaties op de loer liggen. Een mooi voorbeeld is de juridische context waar inmiddels advocaten zijn berispt omdat ze in de stukken die ze bij de rechtbank hadden ingediend antwoorden van een AI-systeem zonder controle hadden overgenomen. Op het moment dat de rechters de stukken lazen bleek dat passages uit wetteksten aan de verkeerde wetsartikelen waren gekoppeld of dat het AI-systeem zelf een interpretatie van de wet als bestaand wetsartikel had opgevoerd. Het onderstreept de noodzaak om de uitkomsten van deze systemen telkens weer te verifieren en het niet op de mooie blauwe ogen te geloven.”

Dat betekent volgens Huijsman niet dat de technologie minder relevant is voor complexere omgevingen. Integendeel. Maar het vraagt wel om een andere benadering. “Je moet AI niet zien als vervanger van werk, maar als versterker van processen. En daar hoort altijd een vorm van menselijke controle bij. Zeker in een domein als het onze, waar data en informatie direct impact kunnen hebben op mensenlevens.”

Data gebruiken zonder eigenaar te worden

Ook de omgang met data verandert, ziet Huijsman. “Waar organisaties voorheen vooral gericht waren op verzamelen en beheren, verschuift de focus nu naar gebruik en verantwoordelijkheid. Organisaties worden steeds terughoudender om data van anderen te beheren. Vooral omdat de verantwoordelijkheid die erbij komt kijken steeds groter wordt.”

Die verantwoordelijkheid is niet alleen juridisch, maar ook maatschappelijk meent hij. “Op het moment dat er iets misgaat, denk aan een datalek, of een hack, dan ben jij als organisatie aansprakelijk. Daardoor gaan organisaties steeds bewuster

om met wat ze wel en niet willen doen of beheren.” De uitdaging zit volgens Huijsman daarom in het vinden van nieuwe vormen van samenwerking. “Hoe kun je wel gebruikmaken van data, zonder dat je automatisch eigenaar wordt? Dat is een vraag waar veel organisaties nu mee worstelen.”

Veiligheid en dienstbaarheid

De combinatie van digitale veiligheid en dienstbaarheid is een extra ingewikkeld vraagstuk binnen al deze ontwikkelingen. Organisaties moeten niet alleen veilig opereren, maar ook toegankelijk en responsief zijn richting burgers. “Dat zijn twee bewegingen die niet altijd vanzelfsprekend samengaan,” zegt Huijsman. “Aan de ene kant wil je maximale veiligheid en controle. Aan de andere kant wil je het burgers zo gemakkelijk mogelijk maken om meldingen te doen.”

Digitalisering als middel, niet als doel

Huijsman ziet dat burgers steeds meer snelheid, gemak en beschikbaarheid verwachten. De uitdaging voor organisaties als LMS zit dan ook niet zozeer in het digitaliseren zelf, maar vooral in de manier waarop dat gebeurt. “Onze dienstverlening wordt almaar digitaler. En voor veel mensen is dat ook prettig. Ze willen zelf bepalen wanneer en hoe ze contact opnemen: telefonisch, via een website of een app bijvoorbeeld. Maar niet iedereen begrijpt wat digitale systemen vragen of vereisen. Denk aan digitale vaardigheden maar ook de omgang met je gegevens.”

Volgens Huijsman dragen organisaties daarom ook een grotere verantwoordelijkheid dan voorheen. “Er is nog steeds een grote groep burgers die veel minder kennis heeft van digitale systemen. Ze zijn er simpelweg niet mee opgegroeid. Organisaties als de onze hebben de verantwoordelijkheid om hun systemen zo in te richten dat ze veilig te gebruiken zijn, ook als een gebruiker dat niet volledig overziet.”

Huijsman vervolgt: “Digitalisering zou juist ruimte moeten creëren om de minder digitaal vaardige burger beter te bedienen. Wij willen onze digitale kanalen daarom zo intuïtief maken dat mensen er zelfstandig mee uit de voeten kunnen. Zo speel je ook meteen meer capaciteit vrij voor de situaties waarin persoonlijk contact nodig is, zeker als iedere seconde telt. Voor een meldkamer is de juiste balans tussen digitaal en persoonlijk contact extreem belangrijk. Onduidelijk ingerichte processen kunnen leiden tot verkeerde of te late meldingen, en dus leiden tot zeer ernstige situaties. Daarom moet je dit soort processen ook zeer bewust inrichten, met oog voor de verschillen in vaardigheden, behoeften, je eigen beschikbare capaciteit en digitale mogelijkheden.”

Het werk verandert

Volgens Huijsman vereist digitalisering ook dat het traditionele denken in functies en rollen op de schop moet. “We moeten meer gaan denken vanuit expertises. Welke kennis en vaardigheden heb je nodig om een bepaalde taak uit te voeren? Die expertise kan op verschillende manieren worden ingevuld. Door een mens, maar ook door een systeem of een AI-oplossing. Of een combinatie daarvan. Het gaat erom dat je op het juiste moment de juiste expertise beschikbaar hebt. Bij een meldkamer kunnen we bepaalde meldingen afhandelen vanuit de beschikbare kennis in een digitale oplossing, en soms is juist menselijke expertise nodig. Ook zal de mens altijd ‘in the loop’ zitten bij bepaalde besluitvorming. De komst van nieuwe technologieën zal het werk van mensen zeker veranderen, maar niet doen verdwijnen.”

“Het gaat erom dat je op het juiste moment de juiste expertise beschikbaar hebt.”

Leren terwijl het werk verandert

Voor professionals wordt leren en ontwikkelen daarom een continu proces. “Technologie én bijbehorende dreigingen blijven zich ontwikkelen. Daar moeten wij mee leren omgaan. Aan de ene kant moet je mensen in het hier en nu bijscholen. Aan de andere kant moet je vooruitkijken en nadenken over wat er straks nodig is.” Dat vooruitkijken gebeurt volgens Huijsman steeds vaker via scenario’s. “Je probeert je voor te stellen: wat als dit gebeurt? Wat betekent dat voor mijn organisatie? Welke expertise heb ik dan nodig? Kortom, de combinatie van mensen, technologie en organisatie.”

Weerstand als signaal

Veranderen roept ook vaak weerstand op. Dat is volgens Huijsman echter niet per se problematisch. “Als je mensen vraagt of er iets moet veranderen, dan zegt iedereen ‘ja!’. Maar als je vraagt wie er wat precies (zelf) gaat veranderen, dan wordt het stil. Dat is heel menselijk. Dan helpt het om veranderingen kleiner en concreter te maken. In plaats van één groot einddoel te stellen, werk je met kleine stappen. Je bouwt iets, test het, leert ervan en past het aan. Dat maakt het gemakkelijker om mensen mee te nemen in een verandering.”

De valkuil van zekerheid

Die aanpak komt voort uit zijn visie op wat werk in de toekomst voor mensen betekent. “We denken te weten hoe ons werk er over een paar jaar uitziet, maar de werkelijkheid is dat die toekomst continu verandert. Als mensen zijn we gewend om te denken in een ‘ist’ en een ‘soll’ situatie. Dus: dit is waar ik nu sta, en daar wil ik naartoe. Maar die ‘soll’-situatie bestaat eigenlijk helemaal niet. Tegen de tijd dat je daar bent, is de wereld namelijk alweer veranderd. Er is dus geen zekerheid en dat geldt dubbel voor iedereen die werkt in het veiligheidsdomein.”

Streven naar zekerheid is dan ook een valkuil, meent hij. “Als je te veel vasthoudt aan hoe het nu is, of hoe het moet worden, dan mis je mogelijk de signalen dat het anders loopt. We moeten meer gaan denken en werken vanuit beweging. Waar wil je naartoe en hoe pas je je onderweg aan? Dat vraagt om continu bijleren en bijsturen. Werk vanuit ambities en ontwikkel je stap voor stap. En accepteert dat ontwikkeling nooit ‘af’ is.”

De kunst van relevant blijven

Wat betekent dat concreet voor organisaties in het veiligheidsdomein? Volgens Huijsman draait het uiteindelijk om één vraag: hoe blijf je relevant? “Die vraag geldt voor organisaties én voor iedere werknemer. Als je niet meer relevant bent, dan moet je veranderen. Niet over twee jaar, maar nu. Waar je precies gaat uitkomen, ligt dus niet vast. Ik ben ervan overtuigd dat degenen die in de toekomst relevant zijn, in staat zijn om onderweg steeds de juiste keuzes te blijven maken en tijdig bij te sturen in het werk dat ze te doen hebben.”

Over de Landelijke Meldkamer Samenwerking

De Landelijke Meldkamer Samenwerking (LMS) beheert voor alle hulpdiensten de meldkamers en zorgt voor een netwerk van tien operationeel en technisch met elkaar verbonden meldkamerlocaties. Het netwerk wordt een landelijk beheerd en is 24/7 bereik- en beschikbaar voor de veiligheidsregio/brandweer, politie, ambulance en Koninklijke Marechaussee om hun meldkamerfuncties te kunnen uitoefenen. Dit doet LMS als een zelfstandig onderdeel binnen de politieorganisatie met een eigen sturing, budget en medewerkers.

Humanoids als toekomst van de strafrechtketen: de nieuwe collega op straat

Hoe geven we humanoids een verantwoorde plek als nieuwe collega in het veiligheidsdomein?

Highlights

- Humanoids zijn geen toekomstvisie, maar een reële volgende stap
- Het veiligheidsdomein wordt hun meest zichtbare werkveld
- Menselijk oordeel blijft normatief leidend
- Praktijkvoorbeelden laten kansen én grenzen zien
- FAIR is noodzakelijk voor legitimiteit en vertrouwen

Humanoids staan op het punt zichtbaar te worden in het veiligheidsdomein. Niet als vervangers van professionals, maar als collega's. Wie nu geen kaders ontwikkelt, laat technologie straks het tempo bepalen.

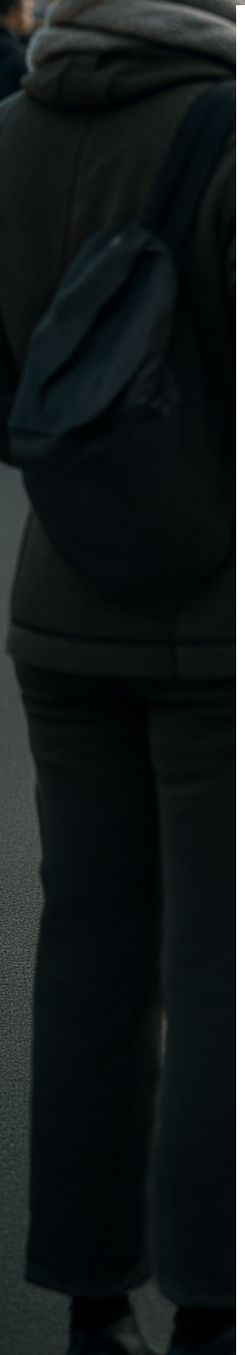
De nieuwe collega op straat staat al om de hoek

Stel je een avond voor in een druk uitgaansgebied. De sfeer is levendig en de alcohol vloeit rijkelijk. De politie houdt toezicht maar de capaciteit staat onder druk. Tussen het publiek beweegt een humanoid zich zichtbaar en rustig voort. Hij observeert en onderneemt actie wanneer dat nodig is: hij registreert druktepatronen, spreekt mensen vriendelijk aan wanneer de spanning oploopt, begeleidt individuen weg uit risicovolle situaties en waarschuwt collega's zodra hij tekenen van escalatie detecteert. Een aanwezige, voorspelbare en niet-emotionele collega die helpt om het overzicht te bewaren, vroegtijdig in te grijpen en zo de veiligheid in het desbetreffende gebied te vergroten.

Wat hier opvalt, is niet alleen wat de humanoid ziet, maar vooral hoe hij handelt. Hij interpreteert gedrag, spreekt mensen aan en grijpt actief in wanneer normen worden overschreden. Dat betekent dat hij wel oordeelt en, binnen vooraf vastgestelde kaders (FAIR-methodologie, zie verderop), ook sancties oplegt. Toch is zijn rol niet die van een menselijk autoriteitsfiguur die vanuit emotie, intuïtie of relationele afwegingen kan handelen. Zijn kracht ligt juist in zijn constante en voorspelbare werkwijze: dezelfde rustige benadering, dezelfde gecontroleerde afstand, dezelfde consequent toegepaste maatregelen. Die voorspelbaarheid werkt stabiliserend in een omgeving waar emoties, groepsdynamiek en impulsiviteit gemakkelijk kunnen escaleren. Hierdoor biedt de humanoid een vorm van objectieve ordehandhaving die menselijke professionals ondersteunt op momenten waarop zij onder hoge druk moeten opereren.

Dit scenario is geen sciencefiction. In verschillende landen worden humanoid-achtige robots al ingezet in publieke ruimtes voor toezicht, informatievoorziening en crowd management. De technologie ontwikkelt zich razendsnel en beweegt zich steeds nadrukkelijker richting de fysieke leefwereld. Juist het publieke veiligheidsdomein is daarbij een logisch eerste werkveld: hier komen capaciteitsdruk, risico's en maatschappelijke verwachtingen samen. De vraag is dan ook niet of humanoids hun intrede doen, maar hoe wij willen dat zij naast ons komen te staan.

Humanoids zijn fysieke robots met een mensachtige vorm en bewegingscapaciteit, ontworpen om te functioneren in omgevingen die primair voor mensen zijn ingericht. Anders dan software, camera's of drones zijn zij zichtbaar aanwezig, bewegen zij zich autonoom door de ruimte en kunnen zij direct interacteren met burgers en professionals. Dat maakt hun impact fundamenteel anders. Niet omdat ze slimmer zijn, maar omdat ze lichamelijk aanwezig zijn.



Een humanoid is geen onzichtbare assistent, maar een ‘iemand’ in de publieke ruimte.

Waar eerdere technologie vaak ‘achter de schermen’ opereerde, staat de humanoid letterlijk in ons midden. Hij kijkt, luistert, registreert en handelt. Daarmee wordt technologie niet alleen een hulpmiddel, maar een actor met gezagssymboliek. Zelfs zonder formele bevoegdheden roept zijn aanwezigheid vragen op: wie kijkt hier mee, waarom en namens wie? Dat maakt humanoids wezenlijk anders dan AI-toepassingen in dossiers of besluitvorming. Een humanoid is geen onzichtbare assistent, maar een ‘iemand’ in de publieke ruimte. Precies daar zit zowel de kracht als de spanning: technologie wordt onderdeel van sociale interactie en daarmee van normatieve betekenisgeving. Dit betekent dat de aanwezigheid van humanoids niet alleen functioneel is, maar ook van invloed is op de manier waarop burgers technologie als normaal, acceptabel en legitiem gaan ervaren in de publieke ruimte.

Waar humanoids zichtbaar impact gaan maken: het veiligheidsdomein

Het publieke veiligheidsdomein is bij uitstek een domein waar humanoids zichtbaar en impactvol ingezet zullen worden. Niet gedreven door technologie, maar door de noodzaak om met minder mensen meer veiligheid te waarborgen. Juist hier zijn de opgaven het scherpst: schaarste aan personeel, toenemende complexiteit, maatschappelijke verharding en de behoefte aan zichtbare, continue aanwezigheid dwingen dit domein om nieuwe vormen van ondersteuning te verkennen. Tegelijkertijd is dit het domein waar legitimiteit en vertrouwen cruciaal zijn. Dat maakt elke technologische interventie hier meteen ook een morele en rechtsstatelijke keuze.

Daarbij verschilt het veiligheidsdomein fundamenteel van andere sectoren waar humanoids al worden verkend, zoals zorg en welzijn. Waar een patiënt in de zorg doorgaans geholpen wil worden en dus meewerkt, heeft het veiligheidsdomein daarnaast ook te maken met weerstand, tegenwerking en normoverschrijdend gedrag. Dat betekent dat een humanoid hier niet alleen moet ondersteunen, maar ook moet omgaan met situaties waarin gezag wordt betwist of actief wordt afgewezen.

Juist in die context wordt de inzet van humanoids complexer en gevoeliger. Niet alleen omdat zij handelen in potentieel conflictvolle situaties, maar ook omdat hun aanwezigheid direct raakt aan vragen over autoriteit, proportionaliteit en acceptatie. Waar technologie in de zorg vooral ondersteunend wordt ervaren, kan zij in het veiligheidsdomein ook als controlerend of dwingend worden geïnterpreteerd. Dat maakt de manier waarop humanoids worden ontworpen, ingezet en gelegitimeerd hier wezenlijk anders.

Humanoids kunnen bijdragen aan toezicht, observatie en informatievoorziening op plekken waar menselijke inzet risicovol, beperkt of niet continu haalbaar is. Hun waarde ligt niet alleen in het ondersteunen van overzicht en veiligheid, maar ook in het uitvoeren van bepaalde, vooraf gedefinieerde handelingen en beslissingen die binnen hun operationele kaders vallen. Denk daarbij niet alleen aan signaleren en informeren, maar ook aan daadwerkelijk ingrijpen: het aanspreken van personen, het sturen van gedrag of het toepassen van eenvoudige interventies in situaties waar snelheid en consistentie essentieel zijn.

Deze handelingen staan niet los van de mens, maar functioneren naast en in samenhang met het menselijke oordeel. In eerste instantie opereren humanoids vooral als collega’s naast professionals, waarbij de mens leidend blijft in beoordeling en besluitvorming. In een verdergaande toepassing kunnen zij delen van het uitvoerende handelen overnemen, binnen duidelijk afgebakende kaders en onder menselijke verantwoordelijkheid.

Daardoor verandert de rol van professionals geleidelijk. Zij worden minder gericht op directe uitvoering en meer op het bepalen van kaders, het monitoren van handelen en het maken van afwegingen. De mens blijft degene die het geheel duidt, keuzes legitimeert en verantwoordelijkheid draagt, terwijl de humanoid zorgt voor continuïteit, consistentie en directe respons waar dat nodig is.

Die verschuiving is fundamenteel. Het werk verandert niet doordat technologie slimmer wordt, maar doordat het menselijke oordeel explicieter centraal komt te staan. Professionals worden regisseurs van complexe situaties, niet uitvoerders van vaste handelingen. Dit vraagt van professionals een andere manier van denken en handelen.

Van uitvoerder naar regisseur: hoe humanoids het veiligheidsdomein drastisch veranderen

Stel je voor: in het uitgaansgebied van een middelgrote stad wordt een pilot uitgevoerd. De humanoid beweegt zich zichtbaar door de menigte en opereert daarbij grotendeels autonoom. Hij herkent druktepieken, afwijkend gedrag en potentiële escalaties op basis van vooraf door mensen geprogrammeerde criteria. Wanneer risico’s toenemen, onderneemt hij direct actie: hij spreekt mensen aan, stuurt groepen bij, blokkeert doorgangen of past andere interventies toe die binnen zijn mandaat vallen. Tegelijkertijd communiceert hij zijn observaties en ingrepen naar menselijke collega’s, die zich strategisch kunnen positioneren of achteraf kunnen beoordelen of hij juist heeft gehandeld.

Wat hier vooral speelt, is legitimiteit. De humanoid neemt wel degelijk besluiten en voert maatregelen uit, maar doet dit binnen een menselijk ontworpen kader. Hij vervangt niet het menselijk gezag, maar neemt delen van het operationele handelen over, waardoor dat gezag effectiever en gerichter kan worden ingezet. Voor professionals betekent dit minder reactieve handelingen en meer regie over het geheel. Voor burgers ontstaat een nieuwe vorm van toezicht: consistent, voorspelbaar en minder afhankelijk van individuele interpretaties, emoties of de druk van het moment.

De inzet van humanoids verschuift niet alleen het werk, maar ook de aard van verantwoordelijkheid in het veiligheidsdomein. Waar professionals voorheen direct handelden, bepalen zij nu in toenemende mate vooraf de kaders waarbinnen gehandeld wordt en toetsen zij achteraf of dat handelen gerechtvaardigd was. Dat betekent dat het zwaartepunt van het werk verschuift van uitvoeren naar verantwoorden. Niet alleen wat er gebeurt is relevant, maar vooral waarom het gebeurt en of dat uitlegbaar en proportioneel is. Het menselijk oordeel blijft daarin onmisbaar. Niet omdat de humanoid niet kan oordelen, maar omdat het uiteindelijke handelen, juist in een domein waarin gezag, proportionaliteit en context centraal staan, altijd een menselijke verantwoording vraagt.

Tegelijk ontstaan nieuwe rollen: toezichthouders op de besluitvorming van de humanoids, specialisten in ethiek en legitimiteit, en professionals die verantwoordelijk zijn voor het vertalen van maatschappelijke waarden naar technologische inzet. De toekomst van werk wordt niet geautomatiseerd, maar normatief verdiept: het verschuift van handelingen uitvoeren naar criteria bepalen, beoordelen en legitimeren. Routinewerk wordt geautomatiseerd: de menselijke taak wordt júist inhoudelijk zwaarder, analytischer en meer waardegedreven.

Een tweede voorbeeld maakt duidelijk hoe ver technologische inzet kan gaan. Systemen kunnen patronen herkennen, jurisprudentie analyseren en zelfs strafvoorstellen genereren. Tegelijkertijd ligt de impact van humanoids niet alleen aan het einde van de keten, maar juist ook aan het begin. Denk aan het vastleggen van bevindingen in systemen, het automatisch structureren van informatie en het direct doorzetten van relevante gegevens naar het Openbaar Ministerie of de rechter. Dit kan het strafproces aanzienlijk versnellen en de druk op capaciteit binnen de keten verlagen.

Een blik in de toekomst

In een verdergaande toepassing zou een humanoid deze functies kunnen combineren en daadwerkelijk als rechter optreden. Hij beoordeelt feiten, past relevante wetgeving toe en formuleert een uitspraak, volledig binnen vooraf door mensen vastgestelde juridische en ethische kaders.

Deze ontwikkeling zal zich niet in één keer voltrekken, maar in fasen. In eerste instantie ondersteunt de humanoid de menselijke professional bij analyse en voorbereiding. Vervolgens kan hij, in samenwerking met de mens, delen van het beoordelingsproces uitvoeren. In een verdergaande fase kan de humanoid binnen duidelijk afgebakende kaders zelfstandig uitspraken formuleren, die door menselijke professionals worden getoetst en bekrachtigd.

Het oordeel is daarmee niet per definitie minder zorgvuldig, maar anders georganiseerd: elke beslissing wordt getoetst door menselijke juridische professionals, die verantwoordelijkheid dragen voor proportionaliteit, motivering en maatschappelijke positionering. De humanoid voert delen van de rechtspraak uit op een manier die transparant en reproduceerbaar is, maar altijd binnen menselijke kaders.

Tegelijkertijd brengt deze ontwikkeling ook reële risico's met zich mee. Eerdere toepassingen van technologie in het recht hebben laten zien dat systemen bestaande biases kunnen versterken, met discriminatoire uitkomsten als gevolg. Juist doordat beslissingen systematisch en consistent worden genomen, kan schijnobjectiviteit ontstaan, terwijl onderliggende aannames niet neutraal zijn.

In deze vorm wordt rechtspraak niet 'ontmenselijkt', maar anders georganiseerd. Het menselijke element verschuift van oordeelvormer naar kadersteller en toetser. Professionals bepalen de normatieve grenzen, controleren de consistentie en bewaken de legitimiteit van de uitspraken.

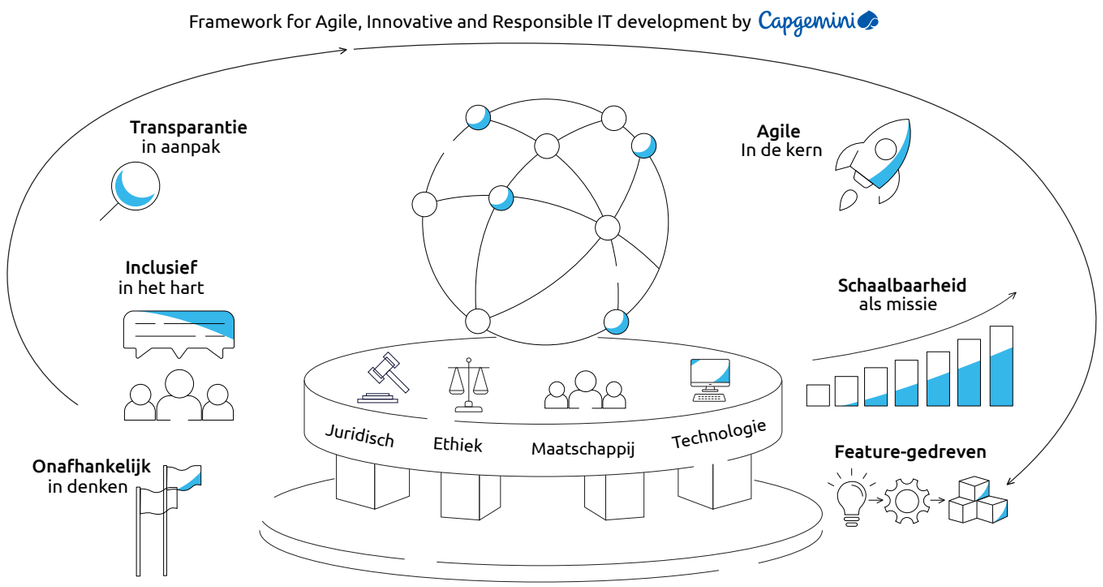
Dit voorbeeld laat zien dat humanoids niet alleen ondersteunend kunnen zijn, maar ook primaire juridische taken kunnen uitvoeren. Het dwingt ons expliciet te bepalen welke waarden we in het recht willen borgen en hoe menselijke verantwoordelijkheid vorm krijgt in een systeem waarin zowel mens als technologie oordelen. Niet alles hoeft door mensen te worden gedaan, maar alles moet wél door mensen gewaarborgd blijven.

FAIR als voorwaarde voor vertrouwen

De inzet van humanoids vraagt om meer dan technologische innovatie alleen. Juist omdat zij zichtbaar handelen in de publieke ruimte, moeten vooraf duidelijke keuzes worden gemaakt over wat zij mogen doen, hoe zij dat doen en wie daarvoor verantwoordelijk is.

Hiervoor is een gestructureerde aanpak nodig. Het Framework for Agile, Innovative and Responsible IT development biedt zo'n kader.[1] FAIR staat voor een integrale benadering waarin functionele, acceptatie-, inbeddings- en rechtsstatelijke aspecten samenkomen. Het helpt organisaties om niet alleen te kijken naar wat technologisch mogelijk is, maar vooral naar wat verantwoord, uitlegbaar en maatschappelijk acceptabel is.

1) https://www.capgemini.com/nl-nl/oplossingen/fair-by-capgemini/



Vier disciplines als fundament • Multidisciplinair • Feature-gedreven • 360º Perspectief

In de praktijk betekent dit dat bij elke toepassing van humanoids vanaf het begin wordt nagedacht over grenzen, verantwoordelijkheden en risico's. Juridische, ethische, technische en maatschappelijke perspectieven worden niet achteraf toegevoegd, maar vormen vooraf het uitgangspunt van ontwikkeling en inzet. Daarmee wordt voorkomen dat technologie sneller beweegt dan de normen die haar zouden moeten begrenzen.

Cruciaal daarbij is dat de verantwoordelijkheid altijd menselijk blijft. Niet de humanoid, maar de organisatie die hem inzet is aanspreekbaar op het handelen. Dat vraagt om duidelijke governance, transparantie en continue toetsing van beslissingen en effecten.

FAIR maakt daarmee het verschil tussen technologie die wordt toegepast en technologie die bewust wordt ingezet. Zonder zo'n benadering dreigt de humanoid een ondoorzichtige actor te worden. Met FAIR kan hij uitgroeien tot een uitlegbare, begrensde en verantwoordelijke collega in het veiligheidsdomein.

"Zonder zo'n benadering dreigt de humanoid een ondoorzichtige actor te worden."

Conclusie

Humanoids worden de nieuwe collega in het veiligheidsdomein. Zichtbaar, handelend, ondersteunend en onvermijdelijk. Niet als vervangers van professionals, maar als versterkers van capaciteit, veiligheid en informatiepositie. Hun komst markeert een kantelpunt: technologie staat niet langer op afstand, maar is fysiek aanwezig en handelend naast ons.

Juist daarom vraagt deze ontwikkeling om meer dan innovatiekracht. Zij vraagt om richting, begrenzing en moed om keuzes expliciet te maken. Humanoids dwingen ons na te denken over wat we menselijk werk vinden, waar gezag vandaan komt en wie verantwoordelijkheid draagt wanneer technologie handelt in onze naam.

Wie nu investeert in kaders, pilots en normatieve afwegingen, behoudt regie. Wie wacht, laat technologie het tempo bepalen. Met een kader als FAIR kunnen humanoids uitgroeien tot betrouwbare collega's die het veiligheidsdomein versterken, zonder de waarden waarop het rust te ondermijnen.

De humanoid staat al om de hoek. De vraag is niet of hij binnenkomt, maar of wij klaar zijn om hem verantwoord te ontvangen.

Over de auteurs

Anne-Sophie Fritschij
Market Lead Justitie & Veiligheid en Business Advisor

Anne-Sophie is gespecialiseerd in de verbinding tussen strafrecht, beleid en praktijk. Ze adviseert over complexe vraagstukken binnen de strafrechtketen, met speciale aandacht voor wetgeving, ketensamenwerking en innovatieve toepassingen van technologie.

https://nl.linkedin.com/in/anne-sophie-fritschij

anne.sophie.fritschij@capgemini.com

Puck Bijleveld
Innovation Lead en Business Advisor

Puck is gespecialiseerd in het aanjagen van innovatie binnen het publieke domein. Ze werkt aan technologiegedreven vernieuwing en nieuwe werkwijzen, en verbindt beleid, uitvoering en business om innovatie daadwerkelijk in de praktijk te laten landen.

https://www.linkedin.com/in/puck-bijleveld-987bbb34

puck.bijleveld@capgemini.com

Een wankel kaartenhuis: Waarom AI-innovatie geen ROI oplevert

AI-succes is geen magie, het vereist een fundament van samenhangende rollen, processen en compliance.

Highlights

- Leiders die verandering omarmen, vormen de brug tussen legacy en een toekomstgerichte organisatie
- Leiderschap bepaalt de AI-visie, maar organisatiecultuur bepaalt of die visie daadwerkelijk schaalbaar wordt
- Betrouwbare data, scherp gedefinieerde verantwoordelijkheden en geïntegreerde compliance vormen het fundament dat nodig is om AI tot een echte transformatieve drijvende kracht te maken
- De grootste blinde vlek in het dreigingslandschap: de organisatorische kwetsbaarheid

Organisaties investeren miljoenen in AI- innovaties in de verwachting van bijna onmiddellijke impact. Toch worden veel AI-initiatieven voortijdig stopgezet. Data blijkt vaak niet klaar te zijn voor AI, rollen zijn onduidelijk en compliance is reactief ingericht. Daardoor blijven organisaties hangen in pilots in plaats van brede, schaalbare waarde te realiseren. AI-projecten falen zelden door technologie maar, omdat organisatorische gereedheid als nagedachte is behandeld.

Voor groei uit AI-innovaties is krachtig leiderschap noodzakelijk. Georganiseerde, hoogwaardige data vormt de basis, maar echte schaalbaarheid ontstaat pas wanneer governance en compliance zijn verankerd in de bedrijfsvoering: duidelijke rollen, gestructureerde verantwoordelijkheid en gestandaardiseerde processen die geen ruimte laten voor interpretatie.

Volgens Gartner faalt tot

70%

van de AI-initiatieven om ROI te leveren

Meetbare Return On Investment (ROI) wordt niet door technologie alleen gedreven; het vraagt om een cultuur van innovatie en teams die verantwoordelijkheid nemen. AI-succes vraagt om mensgerichte vaardigheden: vertrouwen, samenwerking en de bereidheid om innovatie als gezamenlijke missie te omarmen.

Visionair leiderschap: de aanjager van verandering

Organisaties investeren flink in AI, met het doel snel te transformeren.

Maar wat begint als een “cool tech” experiment of strategisch initiatief, komt direct onder druk te staan bij gebrek aan een robuust fundament. Een onduidelijke businesscase of eigenaarschap kan de voortgang ernstig belemmeren en vertrouwen ondermijnen.

Volgens Gartner faalt tot 70% van de AI-initiatieven om ROI te leveren.[1] De oorzaak? AI-initiatieven worden vaak gedreven door urgentie of concurrentiedruk, zonder dat er een goede beoordeling is gedaan van de interne gereedheid. Wanneer het fundament zwak is, wordt het initiatief vroeg of laat onhoudbaar of simpelweg irrelevant.

Visionair leiderschap is daarom essentieel om AI-initiatieven te ontwikkelen tot strategische versnellers in plaats van kostbare terugslagen. Klassieke besluitvormingsmodellen zijn ontworpen voor voorspelbare omgevingen, terwijl AI-volatiliteit complexiteit en nieuwe risico’s introduceert. Wie vasthoudt aan verouderde paradigma’s komt tekort; wie verandering omarmt, vormt de brug tussen legacy en toekomst: oude processen ter discussie stellen, experimenten stimuleren en laten zien dat innovatie veerkracht en groei versterkt.

Succes in het AI-gedreven tijdperk draait niet om brede ervaring of technische certificeringen, maar om mensgericht leiderschap. Verbindingen bouwen creëert vertrouwen, nieuwsgierigheid stimuleert continu leren en openheid versterkt samenwerking. Deze kwaliteiten creëren culturen waarin innovatie daadwerkelijk tot bloei komt, terwijl gefragmenteerde of risicomijdende mindsets zelfs de meest geavanceerde initiatieven kunnen ondermijnen.

Tegenwoordig is de bedrijfscultuur geen soft factor meer, het is de doorslaggevende factor voor duurzame waardecreatie. Leiders richten zich vaak primair op financiële prestatie indicatoren, terwijl de echte gamechanger ligt in de organisatiedynamiek, betrokkenheid en gezamenlijke missie. Wanneer teams verbonden en zelfsturend zijn, verandert cultuur de ROI in blijvende waardecreatie.

Singapore toont dit treffend aan in een opvallende AI-implementatie. Onder de National AI Strategy 2.0 investeerde de overheid eerst in datafundamenten, opleidingen en governance over meerdere agentschappen heen, nog vóór AI breed werd opgeschaald. Door gestructureerde datapijplijnen, duidelijke verantwoordelijkheden en kaders zoals de Model AI Governance Framework en AI Verify te prioriteren, zorgde Singapore dat teams zowel kansen als risico’s van AI begrepen.[2]

Organisatorische Gereedheid

Hoewel visie, missie, risicobeheer en financiering belangrijke pijlers blijven, dienen senior management en AI governance commissies verder te gaan dan traditionele managementtools om de effectiviteit van AI-innovatie te beoordelen. Instrumenten zoals KPI’s, risicoanalyses en administratieve scorecards passen niet goed bij de intrinsieke aard en dynamiek van AI. Om betrouwbare inzichten te genereren, heeft AI een robuust fundament nodig: accurate, consistente data, gedragen door gestructureerde en duidelijke processen en voortdurend getoetst aan compliancevereisten. Om die reden zijn extra validaties en gereedheidscontroles essentieel naast de standaard managementtools.

Processen binnen de bedrijfsvoering kunnen niet als geïsoleerde activiteiten functioneren. De output van het ene proces vormt de input van het volgende. Wanneer die verbindingen zwak of inconsistent zijn, raakt het ecosysteem gefragmenteerd: datakwaliteit daalt, verantwoordelijkheid vervaagt en besluitvorming vertraagt. Pas wanneer processen helder gekoppeld zijn, ontstaat traceerbaarheid, voorspelbaarheid en vroegtijdige signalering van afwijkingen. In zulke omgevingen kan AI volledig tot zijn recht komen.

Hoewel deze elementen de conceptuele basis vormen voor organisatorische gereedheid, laten verschillende voorbeelden zien wat er misgaat wanneer AI zonder deze voorwaarden wordt uitgerold. Het Nederlandse SyRI fraudedetectiesysteem stortte bijvoorbeeld in, toen gefragmenteerde datasets, ontbrekende metadata en gebrekkige governance leidden tot duizenden onterechte fraudemeldingen.[3] Dit leidde uiteindelijk tot de val van het kabinet in 2021. Deze mislukking was niet technologisch van aard, maar organisatorisch: onduidelijk eigenaarschap, zwak databeheer en onvoldoende toezicht lieten systemische fouten ongehinderd escaleren.

Schaalbare bedrijfsvoering met een Uniform Procesmatrix

Een effectieve manier om processen te verbinden en helder inzichtelijk te maken hoe input en output door de organisatie stromen, is het ontwikkelen van een

1) https://www.linkedin.com/pulse/ai-solution-architecture-2026-why-most-roi-fails-before-mohanraj-0nghc

2) https://www.mckinsey.com/featured-insights/future-of-asia/singapores-smart-leap-digital-minister-teo-on-ai-transformation

3) https://www.fastcompany.com/91346333/why-governments-ai-dreams-keep-turning-into-digital-nightmares-and-how-to-fix-that

Uniform Procesmatrix, ondersteund door proceseigenaren. Met een uniforme en goed geborgde werkwijze kan de organisatie inefficiënties sneller identificeren, overdrachtsmomenten versterken en structurele verbeteringen over teams heen realiseren. Wanneer deze discipline wordt verankerd in de dagelijkse operatie, stapelen procesinzichten zich op tot snellere verbetercycli, hogere kwaliteit en het vermogen om capaciteiten met vertrouwen en voorspelbare cadans op te schalen.

Onderstaand voorbeeld uit een recent project illustreert hoe processen via hoofdproducten met elkaar verbonden zijn: de belangrijkste output van het ene proces, vormt de input voor het volgende. Dit voorbeeld van een Uniform Procesmatrix binnen cybersecurity is generiek van aard en kan eenvoudig worden aangepast aan de context, behoefte en sector van uw eigen organisatie.

Products	From					
To	**Process**	**Cybersecurity Compliance**	**Cybersecurity Risk Management**	**Cybersecurity Strategy**	**Cybersecurity Architecture**	**Cybersecurity Monitoring, Reporting and Improvement**
	Cybersecurity Policies Standards, Guidelines	1. Regulatory and framework requirements catalogue 2. Policy to control frameworks mapping requirements (clear linkage to operational procedures) 3. Required evidence and auditability criteria 4. Control assessments of implemented controls & compliance metrics for implemented policies 5. Regulatory updates for policies reviews & testing	1. Company Cybersecurity risk assesment results 2. Risk treatment decisions & response plans 3. Risk scenarious and use cases 4. Risk appetite translation into policy requirements 5. Risk ownership & accountability inputs 6. Risk indicators and policies effectivness feedback	1. Cybersecurity Strategy 2. Policy Architecture & Hierarchy 3. Policy scope and coverage requirements 4. Cybersecurity framework implementation plan (roadmap, for policy alignment)	1. Target security architectural design 2. Refference architecture & patterns 3. Security requirements (for policy development) 4. Technology standards and aproved solutions 5. Architecture decision records and exceptions 6. Security archictecture Maturity assesments & Roadmaps input	1. Metrcis and reports for testing policies & standards 2. Trend and root-cause analysis 3. Incident lessons learned 4. Improvement plans (for policy updates)
	Cybersecurity Compliance		1. Enterprise Cybersecurity Risk register 2. Risk ratings, scenarious and top risks narratives 3. Compliance oversight documentation; risk appetite and tolerance interpretation 4. KRI's and treshholds 5. Risk treatment decisions and status 6. Emerging Risks & forward looking scenarious	1. Cybersecurity Startegy 2. Risk appetite and tolerance statements 3. Regulatory and standarts positioning statements 4. Strategic Risk register and top Cyber risks 5. Target Maturity and Capability roadmap 6. Annual Cybersecurity objectives and KPI's 7. Governance, roles and decision authorities	1. Target security architecture plan 2. Current architecture state report 3. Architecture-defined rules for secure design decisions 4. Controls and responsabilities models 5. Technology standarts and approved security solutions	1. Ongoing status of regulatory, framework, and internal compliance obligations. 2. Findings & remediation status 3. Status dashboards for compliance performance and early warning indicators (KPI's & KRI's) 4. Assurance status, audit support documentation 5. Residual risk status 6. Trend analysis (for strategic planning)

Voordelen van de Uniform Procesmatrix:

- Stimuleert breder en integraal denken binnen het management en biedt een helder overzicht van het volledige procesecosysteem.
- Verhoogt de betrokkenheid van stakeholders en verbindt operationele doelen met strategische richting, wat samenwerking tussen afdelingen versterkt.
- Creëert de basis voor scherpere voorspellingen en strategische reacties op verschuivingen in de sector of het werkveld.
- Brengt inefficiënties, hiaten en nieuwe kansen aan het licht voor optimalisatie, innovatie of automatisering.

Hoe datakwaliteit de Uniforme Procesmatrix versterkt

AI is zo sterk als de data waarop het is gebouwd. Dat vraagt om betekenisvolle databronnen, goede metadata en samenwerking tussen business, data-eigenaren, governance, IT, cybersecurity en compliance. Geen enkele AI-oplossing kan slechte data compenseren.

Nadat processen, rollen, input en output zijn vastgesteld, is het essentieel om de data die door deze processen lopen zo te organiseren dat de betekenis wordt behouden. Hierdoor kunnen systemen onderling communiceren en zorgen metadata voor voldoende context, waardoor AI de informatie juist kan interpreteren.

Het bereiken van hoogwaardige datakwaliteit vraagt om nauwe samenwerking:

- De business levert de data.
- De data-eigenaren bewaken consistentie.
- Governance stelt definities en standaarden vast.
- Het IT-team implementeert systeemcontroles.
- Het cybersecurityteam beschermt integriteit, beschikbaarheid en vertrouwelijkheid.
- Het complianceteam bewaakt organisatiebrede en wettelijke vereisten.

Samen zorgen deze functies ervoor dat het proces¬ecosysteem draait op betrouwbare en gevalideerde informatie.

Om AI-innovaties betrouwbaar te maken voor leiders, moeten organisaties een fundamentele vraag durven te stellen. Dit is de vraag of hun data echt geschikt is voor het doel dat wordt nagestreefd. Dit gaat veel verder dan routinecontroles.

AI-systemen lopen vast wanneer onderliggende data incoherent zijn, context missen of processen niet op elkaar aansluiten.

Het vereist duidelijkheid over de volledigheid, consistentie, nauwkeurigheid én metadatakwaliteit van de informatie die uw organisatie voedt. Metadata bieden AI de benodigde context: hoe data door processen bewegen, hoeze worden geïnterpreteerd en hoe ze moeten worden gebruikt voor aanbevelingen of inzichten.

Naarmate processen, eigenaarschap en regelgeving evolueren, moeten validatie en gereedsheidscontroles herhaald worden. Regelmatige datakwaliteitsreviews houden informatie stabiel en bruikbaar, waardoor AI zich snel kan aanpassen, compliance kan ondersteunen, en betrouwbare begeleiding kan bieden in dynamische omgevingen. Zelfs de meest geavanceerde AI-oplossingen kunnen zwakke of gefragmenteerde datafundamenten niet corrigeren.

De onzichtbare dreiging: Waarom AI faalt zonder organisatorische integriteit

Leiders focussen vaak op externe dreigingen: bad actors, ransomwaregroepen en statelijke actoren die kritieke systemen onder druk zetten. Deze risico's zijn reëel en kunnen catastrofale impact hebben op kritieke entiteiten en vereisen daarom proactief beheer. Maar een eenzijdige focus daarop creëert een strategische blinde vlek, waarbij interne organisatorische kwetsbaarheid onopgemerkt blijft.

Externe dreigingen zijn zichtbaar en traceerbaar; interne zwaktes zijn stil, systemisch en veelal complexer. AI-systemen lopen vast wanneer onderliggende data incoherent zijn, context missen of processen niet op elkaar aansluiten.

Neem bijvoorbeeld een scenario waarin een externe actor een bekende kwetsbaarheid probeert te benutten. Een SOC-eenheid detecteert dit vrijwel direct. Maar wanneer de geïntegreerde AI-agent inconsistente interne data aan de detectieketen doorgeeft, zoals verouderde voorraadinventarisaties, onbetrouwbare identiteitsgegevens of foutieve loggingsgegevens, kan het systeem:

- de dreiging aan de verkeerde asset toewijzen
- de ernst of het type incident onjuist classificeren
- activiteit koppelen aan de verkeerde data-eigenaren
- kritieke alerts onderdrukken omdat de basisdata onjuist zijn

Zonder sterke datafundamenten kan zelfs een AI-gestuurd SOC geen betrouwbare intelligentie leveren. AI schiet niet tekort door technologie, maar omdat het functioneert binnen een suboptimaal organisatorisch ecosysteem.

Wanneer leiderschap, cultuur, data, processen en compliance niet zijn uitgelijnd, verandert AI in een wankel kaartenhuis: fragiel, instabiel en gedoemd om onder zijn eigen ambitie te bezwijken.

Echt AI-succes vereist een diep en robuust structureel fundament:

- Visionair leiderschap dat richting geeft en voorbeeldgedrag toont
- Een veerkrachtige, innovatiegedreven cultuur die leren en verantwoord experimenteren ondersteunt
- Hoogwaardige, goed beheerde en betrouwbare data die AI een solide en contextuele basis biedt
- Processen met expliciete verantwoordelijkheid, die de organisatie end-to-end verbinden
- Geïntegreerde compliance en governance die stabiliteit waarborgen naarmate AI opschaalt

Zonder deze samenhangende pijlers is verzwakking van AI-initiatieven onvermijdelijk: signalen vervagen, inzichten verliezen waarde en besluitvorming wordt onbetrouwbaar.

Maar wanneer governance, cultuur en compliance als één geïntegreerd systeem opereren, wordt de organisatie antifragiel, in staat om verstoring niet alleen op te vangen, maar er structureel sterker uit te komen. In zo'n omgeving ontwikkelt AI zich van risicovol experiment tot een herhaalbare, schaalbare groeiversneller: een betrouwbare katalysator voor veerkracht, innovatie en duurzame ROI.

Over de auteurs

Inga Ociaş
Senior Cybersecurity & Privacy Consultant bij Capgemini CSU

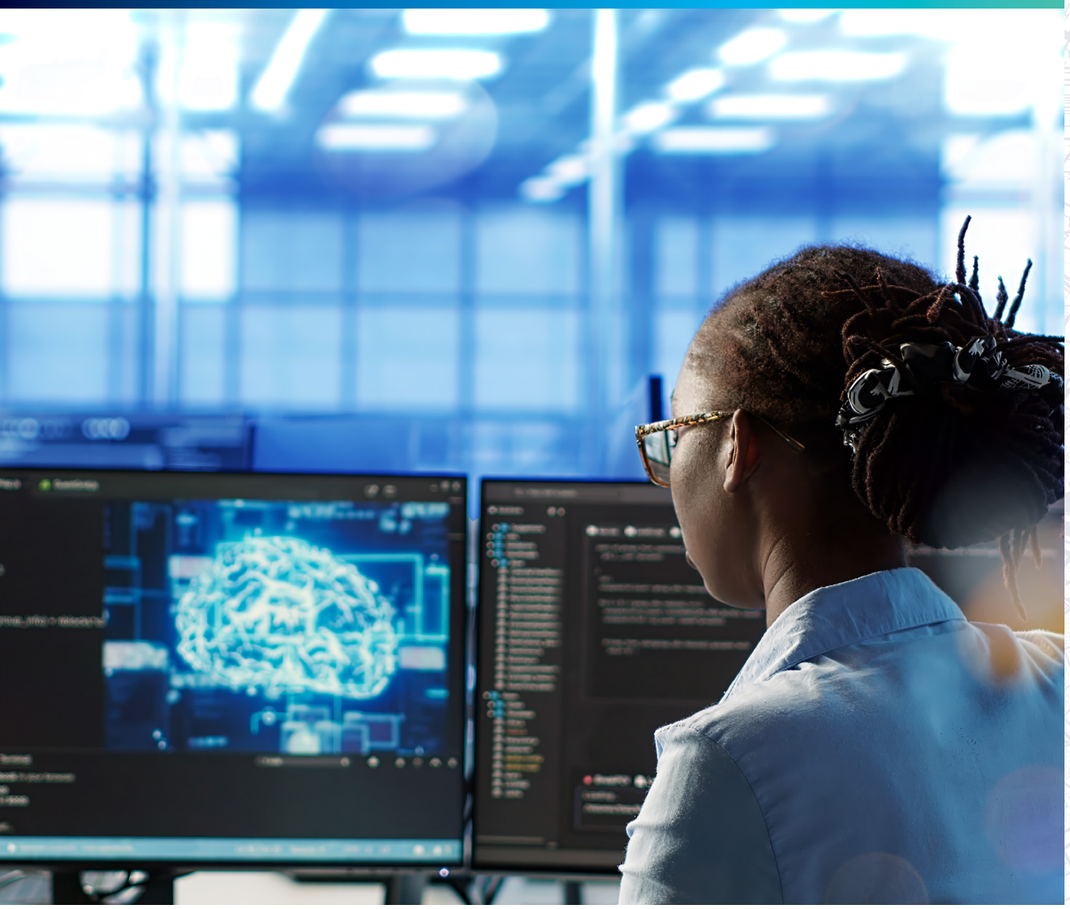
Inga is gespecialiseerd in compliance, organisatorisch herontwerp en AI governance. Zij combineert haar achtergrond in de financiële sector met sterke interpersoonlijke vaardigheden om organisaties te begeleiden in veilige, strategische transformatie.

https://nl.linkedin.com/in/inga-cocias-68769821

inga.cocias@capgemini.com

Cyber Resilience Act: Nieuwe spelregels voor digitale veiligheid bij publieke veiligheidsorganisaties.

Wat betekent de Cyber Resilience Act voor publieke veiligheidsorganisaties?



Highlights

- Eerste EU-wet met cybersecurity-eisen voor alle digitale producten
- Verplicht “security by design & default” en tijdige beveiligingsupdates
- Gefaseerde invoering tot eind 2027, meldplicht gaat in september 2026 van start; volledige naleving voor nieuwe producten verplicht vanaf december 2027
- Security als kwaliteitslabel en kans
- Uitdagingen met legacy en processen, maar pragmatische oplossingen mogelijk

Europa kan zich opmaken voor een nieuwe verordening: in december 2027 zal de Cyber Resilience Act (hierna: CRA) van kracht worden. Deze verordening legt de verplichting tot security by design, tijdige updates en kwetsbaarhedenbeheer primair bij fabrikanten en leveranciers van digitale producten. Publieke veiligheidsorganisaties, zoals Defensie en Politie, krijgen onder de CRA zelf geen directe wettelijke verplichtingen opgelegd. De impact voor hen is indirect, maar wel aanzienlijk, omdat zij afhankelijk worden van aantoonbaar veilige producten, tijdige updates en transparante communicatie van hun leveranciers.

De CRA verschuift daarmee de formele verantwoordelijkheid naar de fabrikant, maar vergroot tegelijkertijd de operationele verantwoordelijkheid van de gebruiker om hier tijdig en adequaat op te handelen.

Van vrijwillig naar verplicht: wat verandert er door de CRA?

De CRA is de eerste EU-verordening die horizontale cybersecurity-eisen oplegt aan alle “producten met digitale elementen”. Dit betreft zowel hardware als software (European Commission, 2023). Denk aan apparaten die met het internet verbonden zijn (het Internet of Things, IoT), communicatiesystemen, operationele IT-systemen. Alles wat direct of indirect met een netwerk verbonden kan worden valt eronder. Dit is een omslag: de CRA verlegt de focus van beleidsmatige normen en best practices (ISO27001 en Baseline Informatiebeveiliging Overheid, BIO) naar direct afdwingbare wettelijke eisen aan digitale producten.

Fabrikanten moeten aantonen dat hun product “cybersecure” is voor marktintroductie. Concreet houdt dit onder andere in:

- **Security by design & default:** Producten moeten ontworpen en ontwikkeld zijn met geschikte beveiliging tegen relevante risico’s. Ze mogen niet met bekende kwetsbaarheden op de markt komen en dienen standaard veilige instellingen te hebben (ENISA & JRC, 2023).
- **Levenslange zorgplicht:** De leverancier blijft verantwoordelijk voor de veiligheid gedurende de verwachte gebruiksduur. Dit betekent een plicht tot het tijdig beschikbaar stellen van beveiligingsupdates en het monitoren op nieuwe kwetsbaarheden. Minimale supportperiode is vijf jaar, of langer indien de levensduur dat vereist (Ministerie van EZK, 2025).
- **Conformiteit en CE-markering:** Voor het eerst komt er een CE-markering voor cyberbeveiliging. Fabrikanten moeten een EU-conformiteitsverklaring opstellen waarin ze verklaren aan alle essentiële eisen te voldoen. Zo’n verklaring kan meestal via zelfbeoordeling, maar risicovollere productcategorieën vereisen een externe audit door een aangewezen instantie (Notified Body) (European Commission, 2023). De CE-markering maakt voor gebruikers direct zichtbaar dat een product aan de CRA voldoet.
- **Meldplicht bij incidenten:** Vanaf 11 september 2026 moeten fabrikanten incidenten en actief misbruikte kwetsbaarheden binnen 24 uur melden bij het Nationaal Cyber Security Centrum (NCSC) (Ministerie van EZK, 2025). Ook moeten getroffen gebruikers worden geïnformeerd en geadviseerd. Hoewel deze meldplicht al geldt, treedt de rest van de CRA-verplichtingen, inclusief de CE-markering, pas op 11 december 2027 volledig in werking.
- Handhaving en sancties: In Nederland houdt de Rijksinspectie Digitale Infrastructuur (RDI) toezicht op de naleving van de CRA. Niet-conforme producten kunnen van de markt worden geweerd. Bovendien kunnen forse boetes worden opgelegd tot €15 miljoen of 2,5% van de wereldwijde jaaromzet van de leverancier (Digitale Overheid, 2024). Dit benadrukt de ernst: non-compliance is geen optie zonder consequenties.

CRA binnen het veiligheidsdomein: wat brengt deze wet mee voor publieke veiligheidsorganisties?

De CRA legt de formele meldplicht voor ernstige incidenten en actief misbruikte kwetsbaarheden bij de fabrikant van digitale producten; publieke veiligheidsorganisaties krijgen onder de CRA zelf geen directe wettelijke meldplicht.

Fabrikanten zijn verplicht om gebruikers tijdig te informeren over kwetsbaarheden en incidenten. Publieke veiligheidsorganisaties moeten op basis daarvan hun interne incidentprocessen activeren en kunnen, afhankelijk van andere wetgeving zoals de Network and Information Security Directive 2 (NIS2), alsnog een eigen meldplicht krijgen.

De CRA verplicht fabrikanten om digitale producten standaard veilig op te leveren. Voor publieke veiligheidsorganisaties betekent dit dat zij deze veilige instellingen in de praktijk moeten gebruiken, beheren en waar nodig bewust aanpassen.

Security by default werkt zo door van het product naar de organisatie: niet als nieuwe wettelijke plicht, maar als praktische randvoorwaarde voor veilig gebruik.

1. **Digitale veiligheid als randvoorwaarde voor de operatie** Voor politie, defensie en andere publieke veiligheidsorganisaties is betrouwbare technologie essentieel. De CRA benadrukt dat dat deze betrouwbaarheid begint bij cybersecurity. Een niet-geüpdatete camera of drone kan immers een ingang zijn voor sabotage met potentieel fysieke gevolgen. Door de CRA wordt cyberveiligheid een harde randvoorwaarde: operationele continuïteit vergt onder meer aantoonbaar beveiligde digitale producten. Wel blijft het belangrijk dat organisaties deze producten niet blind vertrouwen op basis van de CE-markering, maar actief toetsen of configuraties, instellingen en beheermaatregelen aansluiten op hun eigen gebruikers en omgeving. In de praktijk zullen veiligheidsorganisaties strenger moeten toezien op de IT-beveiliging van al hun materieel. In de praktijk kan dit ertoe leiden dat politienetwerken alleen nog nieuwe devices toelaat met CE-markering of dat Defensie van leveranciers eist dat ook toeleveranciers van logistieke systemen hun software-lifecycle aantoonbaar op orde hebben. Op strategisch niveau versterkt de structurele aandacht voor ketenveiligheid de weerbaarheid van de organisatie: minder zwakke schakels in de keten betekent minder kans op verstoringen. Bovendien draagt deze aandacht bij aan data-integriteit en -vertrouwelijkheid.
2. **Versterkt vertrouwen en reputatie** Voor organisaties met een kritische rol op het gebied van veiligheid ligt het voor de hand dat hun beveiliging goed op orde is. Door actief aan de CRA te voldoen, kunnen zij dat vertrouwen zichtbaar maken. Een CE-markering op de ingezette apparatuur laat zien: wij nemen uw veiligheid serieus. Dit werkt twee kanten op: intern ontstaat trots en een cultuur waarin cybersecurity een normaal onderdeel van professioneel werken is; extern kunnen organisaties transparanter rapporteren over hun cybervolwassenheid. Denk aan jaarverslagen waarin vermeld wordt hoeveel procent van de gebruikte systemen CRA-gecertificeerd is, een nieuwe kwaliteitsindicator. Zo wordt security een ‘kwaliteitslabel’ (zie afbeelding hieronder).
Dit biedt ook kansen richting samenwerkingspartners (bijvoorbeeld internationale missies of ketenpartners): men spreekt dezelfde taal van eisen en certificaten, wat samenwerking vergemakkelijkt omdat men op elkaars digitale betrouwbaarheid kan rekenen. Hierdoor wordt samenwerking soepeler en ontstaat een sterker Europees blok dat digitaal op elkaar kan vertrouwen. Dit is een belangrijke factor in een wereld van snel veranderende geopolitieke verhoudingen.

3. **Kansen voor wendbaarheid en innovatie**
   Leveranciers zullen steeds meer concurreren op beveiligingsaspecten om het meest veilige product op de markt te brengen. Dit kan leiden tot nieuwe functionaliteiten waar veiligheidsorganisaties van zullen profiteren. Denk aan betere encryptie, efficiëntere update-mechanismen of ingebouwde incidentlogging. Daarnaast dwingt de CRA leveranciers en/of producenten om hun architecturen te moderniseren: het kan een stok achter de deur zijn om bestaande systemen versneld te vervangen door moderne, veilige alternatieven. Dit verhoogt de wendbaarheid en weerbaarheid op langere termijn, omdat nieuwere systemen vaak flexibeler en toekomstbestendiger zijn.

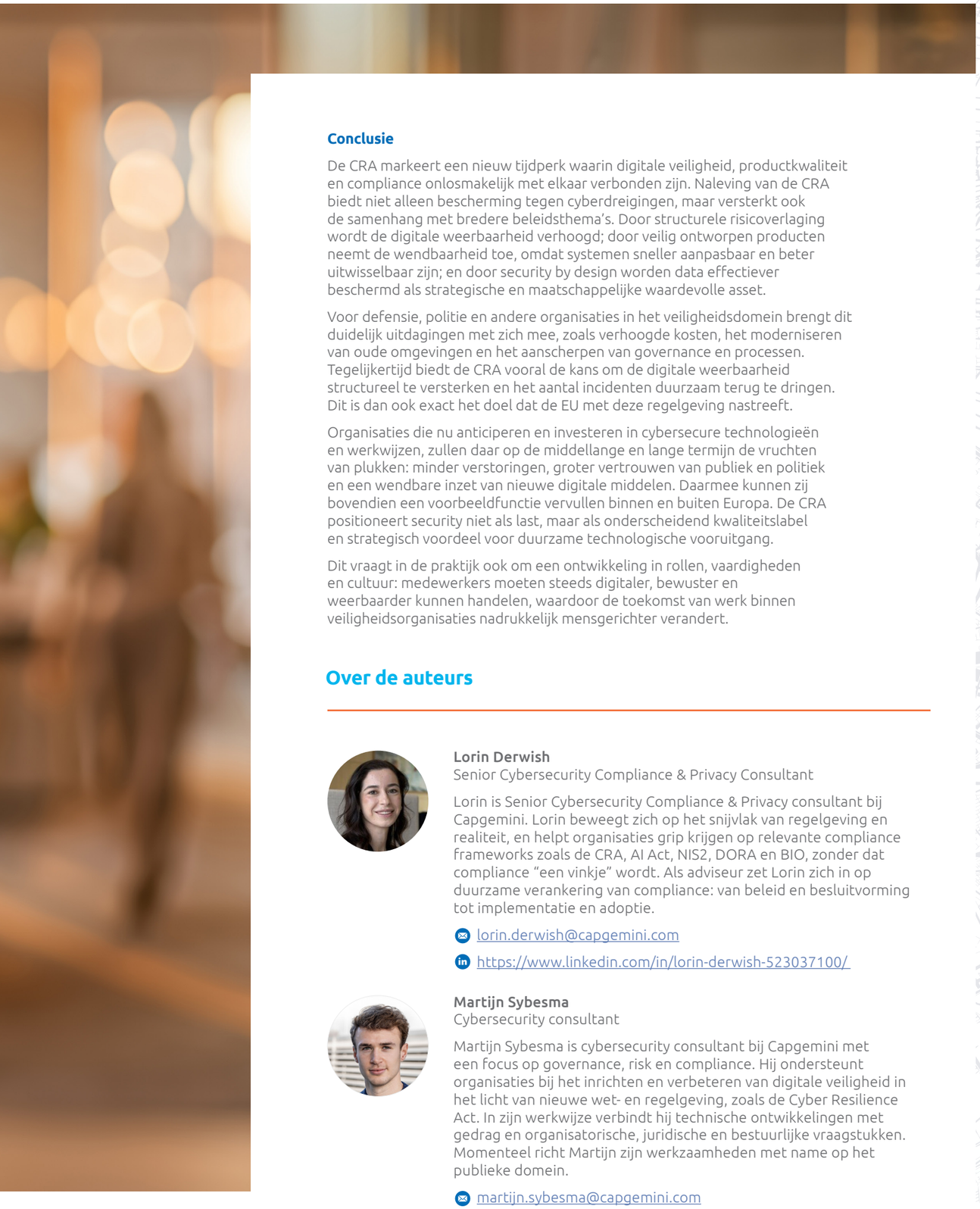
   Een ander aspect is dat door de CRA de samenwerking en uitwisselbaarheid van gegevens verbetert. Dit leidt tot het resultaat dat publieke diensten in verschillende EU-landen makkelijker elkaars technologie kunnen overnemen of gezamenlijk eisen opstellen, omdat de cybersecurity aspecten van technologie overeenkomen. Voor Nederlandse veiligheidsorganisaties met internationale taken, zoals de EU-/NAVO-missies en Interpol-samenwerking, betekent dit een sterke basis: zij voldoen aan Europees verankerde normen die mogelijk wereldwijd richtinggevend worden (European Commission, 2023). Kortom, de CRA kan een middel zijn voor innovatie met security als fundament.

4. **Security als proces en cultuur**
   Een subtiele maar belangrijke kans is dat de CRA helpt om binnen organisaties de focus te verleggen van eenmalige beveiligingsprojecten naar een continu proces. Omdat leveranciers nu updates moeten blijven leveren, zullen veiligheidsorganisaties hun update- en configuratiebeheer ook structureel moeten inbedden. Dit leidt tot vaste werkwijzen. Denk aan het maandelijks doorvoeren van updates in plaats van ad-hoc. Dit zal uiteindelijk de algehele cyberhygiëne bevorderen.

De uitdagingen

Zoals eerder vermeld, levert het voldoen aan de CRA voordelen op. Tegelijkertijd kunnen er ook verschillende uitdagingen ontstaan:

Budgetdruk De CRA kan veiligheidsorganisaties op korte en middellange termijn op extra kosten jagen. Denk aan budgetdruk door het langer moeten onderhouden van bestaande systemen, het versneld vervangen van producten die niet aan de CRA-eisen voldoen en strengere vereisten voor inkoop, contractbeheer en verantwoording. Organisaties moeten aantoonbaar vastleggen dat producten voldoen aan de CRA en dit integreren binnen bestaande kaders zoals BIO, NIS2 en aanbestedingsregels, wat governanceprocessen complexer maakt.	**Acties:** • Veranker CRA-eisen structureel in inkoop-, contract- en lifecycle management, zodat kosten en verplichtingen vroegtijdig inzichtelijk worden. • Harmoniseer CRA-verplichtingen met bestaande kaders zoals BIO en NIS2, om dubbel werk en bestuurlijke onduidelijkheid te voorkomen. • Maak eigenaarschap expliciet binnen governancestructuren, zodat duidelijk is wie financieel en inhoudelijk verantwoordelijk is voor productconformiteit.
Kennis Voor de implementatie van de CRA is gespecialiseerde kennis nodig over product- en softwarebeveiliging, kwetsbaarhedenbeheer en Europese regelgeving. Omdat deze expertise schaars is, zijn instellingen vaak afhankelijk van leveranciers en moeten zij extra investeren in opleiding en bewustwording. De CRA biedt een impuls om structureel kennis op te bouwen binnen de organisatie.	**Actie:** Borg basiskennis over productveiligheid, beveiligingsupdates en kwetsbaarheden binnen IT, security en inkoop, zodat leveranciers effectief kunnen worden aangestuurd en risico's tijdig worden herkend.
Continuiteit Daarnaast werken veel veiligheidsorganisaties met langlopende, missiekritische systemen en contracten die moeilijk aan te passen zijn aan nieuwe CRA-eisen. Dit leidt tot een spanningsveld tussen de noodzaak om tijdig beveiligingsupdates door te voeren en het waarborgen van operationele continuïteit en stabiliteit.	**Actie:** Breng missiekritische systemen en langlopende contracten in kaart en bepaal tijdig waar vervanging, uitzonderingen of juist risicoacceptatie nodig zijn richting 2027. Actieve betrokkenheid van management en bestuur is daarbij belangrijk om bewuste keuzes te maken binnen operationele veiligheidsorganisaties.
Compliance ≠ veiligheid Een belangrijk aandachtspunt is daarbij dat compliance niet gelijkstaat aan veiligheid. Daarbij schuilt het risico dat organisaties veronderstellen dat producten door security by design en security by default standaard veilig inzetbaar zijn, terwijl in de praktijk validatie van configuraties, omgevingsafstemming en structurele monitoring noodzakelijk blijven. De CRA stelt een wettelijk kader vast, maar echte cyberweerbaarheid vereist dat organisaties voortdurend risico's beoordelen en actief handelen. Dit betekent ook dat rollen, vaardigheden en governance moeten worden versterkt, zodat medewerkers digitale producten effectief kunnen controleren, configureren en beheren op veiligheid.	**Acties:** • Voer regelmatig controles uit op configuraties en omgevingen, óók bij producten die aan de CRA voldoen. • Maak continue monitoring en periodieke risicobeoordelingen tot een standaard deel van het beheer. • Leg rollen, bevoegdheden en verantwoordelijkheden rondom product- en leveranciersrisico's beter vast, zodat veiligheid zowel juridisch als operationeel wordt gegarandeerd.



Conclusie

De CRA markeert een nieuw tijdperk waarin digitale veiligheid, productkwaliteit en compliance onlosmakelijk met elkaar verbonden zijn. Naleving van de CRA biedt niet alleen bescherming tegen cyberdreigingen, maar versterkt ook de samenhang met bredere beleidsthema's. Door structurele risicoverlaging wordt de digitale weerbaarheid verhoogd; door veilig ontworpen producten neemt de wendbaarheid toe, omdat systemen sneller aanpasbaar en beter uitwisselbaar zijn; en door security by design worden data effectiever beschermd als strategische en maatschappelijke waardevolle asset.

Voor defensie, politie en andere organisaties in het veiligheidsdomein brengt dit duidelijk uitdagingen met zich mee, zoals verhoogde kosten, het moderniseren van oude omgevingen en het aanscherpen van governance en processen. Tegelijkertijd biedt de CRA vooral de kans om de digitale weerbaarheid structureel te versterken en het aantal incidenten duurzaam terug te dringen. Dit is dan ook exact het doel dat de EU met deze regelgeving nastreeft.

Organisaties die nu anticiperen en investeren in cybersecure technologieën en werkwijzen, zullen daar op de middellange en lange termijn de vruchten van plukken: minder verstoringen, groter vertrouwen van publiek en politiek en een wendbare inzet van nieuwe digitale middelen. Daarmee kunnen zij bovendien een voorbeeldfunctie vervullen binnen en buiten Europa. De CRA positioneert security niet als last, maar als onderscheidend kwaliteitslabel en strategisch voordeel voor duurzame technologische vooruitgang.

Dit vraagt in de praktijk ook om een ontwikkeling in rollen, vaardigheden en cultuur: medewerkers moeten steeds digitaler, bewuster en weerbaarder kunnen handelen, waardoor de toekomst van werk binnen veiligheidsorganisaties nadrukkelijk mensgerichter verandert.

Over de auteurs

Lorin Derwish
Senior Cybersecurity Compliance & Privacy Consultant

Lorin is Senior Cybersecurity Compliance & Privacy consultant bij Capgemini. Lorin beweegt zich op het snijvlak van regelgeving en realiteit, en helpt organisaties grip krijgen op relevante compliance frameworks zoals de CRA, AI Act, NIS2, DORA en BIO, zonder dat compliance "een vinkje" wordt. Als adviseur zet Lorin zich in op duurzame verankering van compliance: van beleid en besluitvorming tot implementatie en adoptie.

lorin.derwish@capgemini.com

https://www.linkedin.com/in/lorin-derwish-523037100/

Martijn Sybesma
Cybersecurity consultant

Martijn Sybesma is cybersecurity consultant bij Capgemini met een focus op governance, risk en compliance. Hij ondersteunt organisaties bij het inrichten en verbeteren van digitale veiligheid in het licht van nieuwe wet- en regelgeving, zoals de Cyber Resilience Act. In zijn werkwijze verbindt hij technische ontwikkelingen met gedrag en organisatorische, juridische en bestuurlijke vraagstukken. Momenteel richt Martijn zijn werkzaamheden met name op het publieke domein.

martijn.sybesma@capgemini.com

https://www.linkedin.com/in/martijn-sybesma-a60412205/

Bronnen

- Digitale Overheid. (2024, 14 oktober). Europese Raad keurt Cyber Resilience Act goed [Nieuwsbericht]. Ministerie van Binnenlandse Zaken. (Belangrijkste punten en boetes CRA).
- ENISA & Joint Research Centre. (2023). Cyber Resilience Act Requirements – Standards Mapping. Luxemburg: Bureau voor publicaties EU. (Technische mapping van CRA-eisen aan standaarden).
- European Commission. (2023, 1 december). Cyber Resilience Act – Questions and Answers. Geraadpleegd van EU Commission Press Corner Q&A 22-5375. (Achtergrond, inhoud en doelen CRA, incl. samenhang met NIS2).
- European Parliament. (2024, 20 december). EU Cyber Resilience Act (Legislation in Progress Briefing, 4e ed.). Brussel: EPRS. (Overzicht CRA, tijdlijn: inwerking 2024, toepasbaar vanaf 11 dec 2027).
- Ministerie van Economische Zaken en Klimaat. (2025, 11 maart). Internetconsultatie Uitvoeringswet Verordening cyberweerbaarheid is begonnen [Nieuwsbericht]. Rijksoverheid. (Schade cybercrime €5,5 biljoen in 2021; ingangsdata meldplicht 11-09-2026 en naleving 11-12-2027; rol NCSC).
- NCSC & Digital Trust Center. (2025, 7 april). Vijf basisprincipes voor digitale weerbaarheid [Nieuwspublicatie]. Nationaal Cyber Security Centrum. (Praktische stelregels om cyberweerbaarheid te vergroten, ter ondersteuning van organisaties).

Interview:

Arie Franke
Kwartiermaker Directie Strategie en Beleid bij het Openbaar Ministerie

“Weerbaarheid begint niet bij technologie, maar bij mensen”

Het Openbaar Ministerie bevindt zich midden in een digitale transformatie. Nieuwe technologieën zoals AI en quantum computing bieden kansen, maar brengen ook nieuwe risico’s met zich mee.

Volgens Arie Franke, kwartiermaker en directeur strategie & beleid IVOM, draait de transformatie om één vraag: hoe zorg je ervoor dat de rechtsstaat blijft functioneren in een wereld die steeds digitaler en complexer wordt? “Als burger moet je erop kunnen vertrouwen dat rechtsgelijkheid, rechtvaardigheid en de betrouwbaarheid van het Nederlandse strafrecht overeind blijven. Dat is uiteindelijk waar weerbaarheid voor ons om draait.

Een digitale rechtsstaat

De digitalisering van de strafrechtketen nam de afgelopen jaren een enorme vlucht. Waar een papieren proces-verbaal vroeger het centrale bewijsmiddel bevattte, krijgen digitale bronnen een steeds prominentere rol. “Camerabeelden, bodycam-opnamen, audiobestanden en andere digitale gegevens worden steeds belangrijker binnen opsporing en vervolging,” vertelt Franke. “Dat heeft grote gevolgen voor de manier waarop de strafrechtketen functioneert. Straks kunnen multimedia , zoals een filmpje zelf het bewijsmiddel zijn. Dat betekent dat je niet meer praat over documenten, maar over enorme hoeveelheden digitale informatie die veilig, betrouwbaar en controleerbaar beschikbaar moeten blijven. Daarmee groeit ook de afhankelijkheid van digitale infrastructuur.”

Toch is veel van de onderliggende structuur nog gebaseerd op processen die ooit voor een papieren werkelijkheid zijn ontworpen. “Het Wetboek van Strafvordering is meer dan honderd jaar oud en wordt nu vernieuwd. Wat we bij het OM en binnen de keten jarenlang hebben gedaan, is papieren processen digitaliseren. Maar inmiddels zijn we op een punt gekomen waarop de mogelijkheden van technologie verder gaan dan de processen waarop onze systemen zijn gebaseerd.”

Het OM weet uit ervaring hoe sterk processen inmiddels verweven zijn geraakt met digitale voorzieningen. Volledig terugvallen op papier is geen realistische optie meer. “We hebben ervaren dat je bepaalde processen simpelweg niet meer kunt uitvoeren zonder digitale ondersteuning. De werkelijkheid is dat we afhankelijk zijn geworden van digitale infrastructuur. Dat inzicht heeft het denken over onze weerbaarheid fundamenteel veranderd.”

De continuïteit van weerbaarheid

Voor Franke betekent weerbaarheid het vermogen om maatschappelijke taken te kunnen blijven uitvoeren, ook wanneer systemen worden verstoord. “Onze bedrijfsprocessen moeten robuust genoeg zijn om verstoringen op te vangen. Hierin is de ICT-inbreuk die wij vorig jaar zomer als OM doormaakten een pijnlijk voorbeeld. Niet alleen technisch, maar ook organisatorisch moet je robuust zijn. Dat gaat verder dan cybersecurity alleen. Het raakt ook cultuur en governance, maar ook transparantie. Je moet altijd kunnen verantwoorden waar informatie vandaan komt, hoe deze wordt verwerkt en wie toegang heeft gehad. Die transparantie is essentieel voor het rechtsproces.”

Veel organisaties investeren pas serieus in weerbaarheid nadat een incident heeft plaatsgevonden. Volgens Franke ligt juist daar een belangrijke les. “Je kunt nooit volledig inzicht hebben in alle kwetsbaarheden van je omgeving. Maar je kunt je er wél op voorbereiden. Dat vraagt om een andere manier van kijken naar risico’s.”

Waar risicomanagement vroeger vooral draaide om het identificeren van risico’s, ligt de nadruk nu steeds meer op bestuurlijke keuzes. “Bestuurders moeten weten welke risico’s zij accepteren en welke consequenties daarbij horen. Daarvoor is meer nodig dan rapportages en risicoanalyses. Scenario’s moeten worden geoefend, noodprocessen getest en verantwoordelijkheden helder vastgelegd. Een plan op papier is niet voldoende. Pas wanneer je gaat oefenen, ontdek je wat er in de praktijk gebeurt. Juist die vertaalslag van theorie naar praktijk vormt de kern van weerbaarheid.”

Mensen maken het verschil

Hoewel technologie vaak centraal staat in discussies over digitale veiligheid, ligt de sleutel uiteindelijk bij het gebruik ervan door mensen. “Technologie ontwikkelt zich sneller dan organisaties kunnen voorspellen. Processen worden steeds verder gestandaardiseerd. Maar leiderschap, bewustzijn en cultuur bepalen uiteindelijk hoe weerbaar een organisatie werkelijk is. Want je kunt de beste systemen hebben, maar als mensen niet begrijpen welke risico’s zij lopen, blijft een organisatie kwetsbaar.”

Opvallend genoeg ontstaat die kwetsbaarheid vaak juist in periodes waarin alles goed lijkt te gaan. “Wanneer de druk afneemt, worden mensen vanzelf minder alert. Dan ontstaat het risico. Daarom investeert het OM nadrukkelijk in bewustwording en het versterken van een cultuur waarin digitale veiligheid onderdeel is van het dagelijkse werk.”

Vijf prioriteiten voor een weerbaar OM

Om richting te geven aan die ontwikkeling heeft het OM de veelheid aan initiatieven teruggebracht tot vijf strategische prioriteiten. “Onze eerste prioriteit is stabiliteit: wat vandaag werkt, moet betrouwbaar blijven functioneren. De tweede is digitale weerbaarheid. Nieuwe systemen, processen en voorzieningen worden standaard beoordeeld op hun weerbaarheid tegen verstoringen. Daarnaast prioriteren we de modernisering van de IT-omgeving, de verbetering van de gegevens- en informatiehuishouding en de verdere professionalisering van onze IV-organisatie.”

“Deze koers is vastgelegd in een bredere i-visie, i-strategie en i-plan. Door keuzes te maken ontstaat focus. En focus is noodzakelijk om daadwerkelijk vooruitgang te boeken.”

Een keten van afhankelijkheden

Een belangrijk kenmerk van de moderne strafrechtketen is dat zij steeds meer is veranderd van een lineair proces naar een digitaal ecosysteem. “Politie, Openbaar Ministerie, rechtspraak, ministeries en tal van andere organisaties wisselen voortdurend onderling gegevens uit. In een gemiddelde strafzaak zijn soms tientallen partijen betrokken voordat een zaak bij de rechter terechtkomt.”

Dat biedt kansen, maar creëert ook nieuwe kwetsbaarheden. “Een organisatie kan haar eigen beveiliging uitstekend op orde hebben, maar blijft afhankelijk van keuzes die elders in de keten worden gemaakt. Je kunt als organisatie besluiten bepaalde technologie niet te gebruiken, maar als ketenpartners andere keuzes maken, kunnen die alsnog gevolgen hebben voor jouw risico’s. Daarmee verschuift digitale weerbaarheid steeds meer van een organisatievraagstuk naar een ecosysteemvraagstuk.”

Digitale soevereiniteit versus samenwerking

Die wederzijdse afhankelijkheden leiden regelmatig tot dilemma’s. “Vanuit technologisch perspectief ligt samenwerking vaak voor de hand. Gezamenlijke voorzieningen kunnen efficiënter en veiliger zijn. Tegelijkertijd spelen binnen de strafrechtketen ook andere belangen. Zo zijn autonomie en digitale soevereiniteit belangrijke waarden.”

Dat betekent dat organisaties soms bewust kiezen voor eigen systemen en eigen infrastructuur, ook wanneer dat vanuit IT-perspectief minder efficiënt lijkt. “De vraag die voortdurend terugkomt is dan ook: ‘waar wil je zelfstandig blijven en waar kun je gezamenlijk optrekken?’”

Leveranciers als strategische partners

Volgens Franke wordt de rol van leveranciers de komende jaren belangrijker dan ooit. “Een deel van de kennis en expertise bevindt zich buiten de overheid. Waar we samenwerking met marktpartijen vroeger vooral bekeken vanuit opdrachtgeverschap, ontstaat steeds meer een partnerschapsmodel. Dat vraagt ook iets van de overheid zelf.”

Overheidsorganisaties moeten voldoende kennis behouden om de juiste vragen te kunnen stellen en de juiste keuzes te maken. “We hebben in het verleden soms gedacht dat alleen regie voeren voldoende was. Maar als je zelf niet begrijpt waarover het gaat, wordt regie lastig. We moeten in de keten leveranciers meer als strategische partners gaan zien, waarbij alle partijen hun waarde bijdragen.”

“Digitale weerbaarheid verschuift steeds meer van een organisatievraagstuk naar een ecosysteemvraagstuk.”

Nieuwe risico’s aan de horizon

Wat zijn de risico’s van morgen? Franke denkt dan niet alleen aan cybercrime maar ook aan ontwikkelingen rondom energievoorziening, datacentercapaciteit en chiptekorten. Die kunnen grote gevolgen hebben voor de digitale weerbaarheid van Nederland.

“We vinden het vanzelfsprekend dat rekenkracht altijd beschikbaar is. Maar die beschikbaarheid staat niet onbeperkt vast. De groei van AI vergroot die afhankelijkheid. Nieuwe toepassingen vragen om steeds meer opslagcapaciteit, rekenkracht en energie. Daar is nu nog relatief weinig aandacht voor in informatiebeveiliging, maar dit soort ontwikkelingen kunnen op termijn grote impact hebben.”

Een ander risico heeft te maken met de complexiteit van het strafrechtproces zelf. “Anders dan veel publieke organisaties heeft het OM niet één duidelijke gebruiker. Wij hebben te maken met slachtoffers, verdachten, advocaten en andere ketenpartners met uiteenlopende belangen. Slachtoffers hebben vaak behoefte aan meer inzicht en informatie over de voortgang van een zaak. Advocaten en verdachten hebben weer volledig andere belangen en behoeften. Digitale informatievoorziening vraagt dus om een zorgvuldige afweging tussen toegankelijkheid en rechtsstatelijke verantwoordelijkheden.”

De uitdaging van morgen

De komende jaren zal het OM blijven investeren in kennis, capaciteit en executiekracht. Niet alleen om nieuwe technologie te ontwikkelen, maar ook om bestaande systemen veilig en betrouwbaar te houden. “De aandacht gaat vaak naar het nieuwe, maar wat vandaag draait, moet morgen ook nog functioneren. We hebben dus mensen nodig die niet alleen plannen maken, maar die ook veranderingen kunnen realiseren. Want executiekracht wordt de komende tijd minstens zo belangrijk als visie.”

Als Franke één ontwikkeling zou mogen versnellen, dan is dat bewustzijn. Meer specifiek: security by design en security by default als vanzelfsprekend onderdeel van iedere beslissing. “Want uiteindelijk wordt een weerbare organisatie niet bepaald door technologie alleen. Echte weerbaarheid ontstaat pas wanneer veiligheid onderdeel wordt van hoe mensen denken, samenwerken en beslissingen nemen. En daar ligt onze grootste opgave voor de komende jaren: het bouwen van een strafrechtketen die digitaal sterk is, en tegelijkertijd ook veerkrachtig genoeg is om het vertrouwen in de rechtsstaat te blijven beschermen.”

Kan je weerbaar zijn zonder censuur?

Staat de samenleving voor een groter risico bij een overheid die meer gaat modereren en daarmee als beperkend kan worden gezien, of bij een overheid die vrijwel niets doet terwijl buitenlandse kwaadwillende actoren actief de publieke opinie beïnvloeden?

Highlights

- Desinformatie heeft aantoonbare maatschappelijke effecten
- Desinformatie is bewezen grootschalig en internationaal georganiseerd
- Het probleem van desinformatie is urgent, maar er is terughoudendheid om niet beschuldigd te worden van censuur
- De vraag is niet of we moeten handelen, maar hoe we dat kunnen doen
- Technologie is beschikbaar en noodzakelijk als tegenkracht Om dit te faciliteren, moeten dataproducten fit for use beschikbaar zijn

Digitale beïnvloeding en desinformatie zijn geen abstracte risico's meer, maar een onderdeel van het publieke debat. Onderzoekers en veiligheidsdiensten waarschuwen dat buitenlandse actoren proberen invloed uit te oefenen op verkiezingen en maatschappelijke discussies, ook in Nederland. Via sociale media worden bestaande spanningen versterkt, vaak met behulp van nepaccounts, gecoördineerde campagnes en emotioneel geladen boodschappen die inspelen op actuele thema's. Die dynamiek roept fundamentele vragen op. Hoe bescherm je een open samenleving tegen manipulatie zonder de vrijheid van meningsuiting te ondermijnen? En wat zijn de gevolgen van niets doen, wanneer beïnvloeding zich grotendeels onzichtbaar voltrekt? Dit artikel verkent hoe desinformatie werkt, waarom monitoring alleen onvoldoende is en waar de spanning ligt tussen vrijheid, veiligheid en digitale weerbaarheid.

Onderzoekers waarschuwen dat buitenlandse partijen proberen invloed uit te oefenen op Nederlandse verkiezingen[1]. Volgens Post-X Society[2] is bij eerdere verkiezingen digitale inmenging waargenomen, onder meer via trollenlegers en nepaccounts uit landen als Nigeria, Ghana en Ivoorkust die vooral uiterst rechtse boodschappen verspreidden. Deze accounts versterken thema's die bij lokale verkiezingen spelen, zoals asielzoekerscentra en windmolens, waardoor sociale media deze berichten extra onder de aandacht brengen. De zorgen hierover worden gedeeld door zowel de Tweede Kamer als het kabinet.

1) 1 Nos: https://nos.nl/artikel/2605853-zorgen-over-trollenlegers-en-andere-inmenging-rond-verkiezingen

2) 2 Post-X Society, 2025, Eindrapport: verkiezingen onder druk, urgentie actie nodig

Desinformatie en het effect op mensen

Desinformatie is vaak effectief omdat zij inspeelt op emoties en intuïtieve oordeelsvorming. Onderzoek van Pennycook et al. (2021)[3] laat zien dat misleidende berichten regelmatig zijn vormgegeven om sterke gevoelens op te roepen, zoals angst, boosheid of morele verontwaardiging. Wanneer mensen een bericht lezen dat emotioneel geladen is, zijn zij eerder geneigd het voor waar aan te nemen en te delen, vooral wanneer zij afgaan op hun eerste gevoel in plaats van bewuste reflectie. Dit effect doet zich vooral voor bij misleidende of onjuiste informatie en veel minder bij feitelijk correcte berichtgeving.

Deze psychologische dynamiek helpt verklaren waarom desinformatie zich vaak sneller verspreidt dan correcties. In situaties van onzekerheid of crisis sluit emotioneel geframede informatie aan bij bestaande zorgen en overtuigingen, waardoor zij richting kan geven aan het publieke debat voordat feiten volledig zijn vastgesteld. socialmediaplatforms versterken dit effect doordat hun verdienmodel is gericht op aandacht en interactie. Sensationele en polariserende inhoud genereert meer betrokkenheid en wordt daardoor algoritmisch vaker verspreid, ongeacht de feitelijke juistheid ervan[4].

Juist deze combinatie van emotionele framing en platformdynamiek maakt desinformatie moeilijk te bestrijden met correcties achteraf en verklaart waarom vroege signalering en patroonherkenning van belang zijn.

De beïnvloeding en versterking op social media past in een breder patroon van georganiseerde desinformatiecampagnes. Daarbij worden trollenlegers, bots en gecoördineerde sociale mediacampagnes ingezet om twijfel, wantrouwen en maatschappelijke tegenstellingen te versterken. Onderzoek naar buitenlandse beïnvloeding rond onder andere de Amerikaanse presidentsverkiezing van 2016[5] onlinegesprekken[5].

Ook in de Nederlandse context zijn deze mechanismen zichtbaar. Analyses van onder andere de coronapandemie laten zien hoe buitenlandse en binnenlandse actoren via sociale media en Telegram alternatieve verhalen verspreiden, vaak verpakt in een schijn van expertise. Tijdens de coronapandemie bleek dat burgers die vaker misleidende informatie over het virus tegenkwamen minder bereid waren om officiële richtlijnen van de overheid te volgen[6]. Dit uitte zich onder meer in een lagere naleving van overheidsmaatregelen en adviezen, wat laat zien dat desinformatie niet alleen percepties beïnvloedt, maar ook kan doorwerken in daadwerkelijk gedrag, met gevolgen voor publieke veiligheid en overheidsoptreden.

3) Pennycook et al., 2021, The psychology of fake news

4) Van Dijck, https://www.uu.nl/organisatie/verdieping/de-desinformatie-business

5) https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations

6) Hameleers & Vlieghart, 2021, De verspreiding en effecten van desinformatie tijdens de COVID-19-pandemie

Desinformatie en het recht

Een belangrijk spanningspunt is dat desinformatie op zichzelf niet strafbaar is en dat een individueel bericht doorgaans weinig maatschappelijke impact heeft. De invloed ontstaat juist door de grootschalige en gecoördineerde verspreiding van veel vergelijkbare berichten, vaak door verschillende accounts of trollenlegers. Hoewel deze berichten afzonderlijk geen strafbare inhoud bevatten, kan hun gezamenlijke effect leiden tot polarisatie, wantrouwen en maatschappelijke ontwrichting.

Het Nederlandse strafrecht biedt slechts beperkt aanknopingspunten om hiertegen op te treden. Strafbepalingen zoals opruiing (artikel 131 Wetboek van Strafrecht) zien toe op de inhoud van individuele uitingen, bijvoorbeeld wanneer expliciet wordt opgeroepen tot strafbaar of gewelddadig handelen. Veel desinformatie blijft onder deze drempel, omdat er geen sprake is van strafbare inhoud per afzonderlijk bericht. Tegelijkertijd is het massale beïnvloedingseffect juridisch moeilijk aan te pakken, omdat justitie individuen vervolgt en niet het collectieve effect van duizenden op zichzelf legale uitingen.

Geen wetgeving, maar monitoring

De Nederlandse wetgeving biedt momenteel weinig ruimte voor een strafrechtelijke aanpak van desinformatie. In de Rijksbrede strategie tegen desinformatie erkent de minister van Binnenlandse Zaken[7] de risico's van (buitenlandse) desinformatie, met name rond verkiezingen, maar kiest het kabinet nadrukkelijk voor monitoring, signalering en preventie. De focus ligt daarbij op samenwerking tussen betrokken partijen, het vergroten van digitale weerbaarheid en Europese regelgeving, zoals de Digital Services Act, waarbij vooral online platforms verantwoordelijk worden geacht.

Censuur of beperking van burgers

Desinformatie veroorzaakt niet altijd directe schade, maar kan wel ongemerkt polarisatie, wantrouwen en maatschappelijke onrust voeden. Dat roept een ongemakkelijke vraag op: hoever moet Nederland gaan om burgers te beschermen tegen digitale beïnvloeding? En wat gebeurt er als we besluiten om helemaal niet in te grijpen?

In andere domeinen vinden we begrenzing heel normaal, zoals bijvoorbeeld het oproepen tot geweld, terrorisme of haatzaaien. Niemand noemt die grenzen censuur. Maar bij desinformatie ligt dat gevoeliger. Een bericht is vaak gewoon een mening, maar duizend berichten, slim afgestemd op elkaar, kunnen wel degelijk een samenleving richting geven. Toch beoordeelt de wet vooral die losse uitingen, niet de optelsom.

En dan komt de echte vraag: wat vinden we gevaarlijker? Een overheid die meer gaat modereren en daarmee het risico loopt gezien te worden als beperkend? Of een overheid die vrijwel niets doet terwijl buitenlandse kwaadwillende actoren de publieke opinie actief proberen te beïnvloeden?

Aan de ene kant willen we voorkomen dat de overheid gaat bepalen wat waar is. Aan de andere kant zien we dat georganiseerde desinformatie juist gebruikmaakt van onze terughoudendheid. Het speelt handig in op de ruimte die we bewust laten in een open samenleving. Dat maakt de onderliggende vraag steeds scherper: kan je eigenlijk wel weerbaar zijn zonder enige vorm van begrenzing, wanneer dezelfde openheid bewust wordt ingezet om verwarring en polarisatie te versterken?

Het dilemma is daarmee minder zwart-wit dan "wel of geen censuur". Niets doen betekent accepteren dat manipulatie een vaste plek krijgt in het publieke debat. Iets doen vraagt om het durven bespreken van beperkende maatregelen, een idee dat al snel botst met ons vertrouwen in vrijheid van meningsuiting. Er is geen risicoloze optie. Precies daardoor is het zinvol om deze spanning hardop te benoemen: welke vrijheid willen we beschermen en welke risico's zijn we bereid te nemen om dat te blijven doen?

7) December 2025. Beantwoording vragen over de voortgang Rijksbrede strategie voor de effectieve aanpak van desinformatie

"Gebruik AI niet als poortwachter, maar als hulpmiddel dat patronen zichtbaar maakt."

AI als patroonherkenner van desinformatie

Wat nu nodig en mogelijk is, is het vergroten van inzicht in plaats van het beperken van uitingen. Niet bepalen wat mensen mogen zeggen, maar begrijpen hoe bepaalde verhalen ontstaan en waarom ze soms razendsnel richting geven aan het publieke debat. Daar kan AI een rol in spelen. Niet als poortwachter, maar als hulpmiddel dat patronen zichtbaar maakt: herhaling in berichten, opvallende clusters van accounts, plotselinge escalaties of signalen dat dezelfde bron onder verschillende namen opereert.

In Europa wordt hier al mee geëxperimenteerd via het door de EU gefinancierde platform AI4Trust[8], dat grote hoeveelheden online content vrijwel in real time analyseert om patronen van mogelijke desinformatie en beïnvloeding zichtbaar te maken. Kenmerkend is dat het systeem geen inhoudelijke oordelen velt, maar signalen aandraagt die door journalisten en experts verder worden geduid.

Tegelijkertijd laat dit voorbeeld zien dat inzicht alleen niet voldoende is. De netwerken, technieken en infrastructuur waarmee buitenlandse actoren publieke opinie proberen te beïnvloeden blijven actief en ontwikkelen zich sneller dan de maatregelen ertegen. Desinformatie beweegt sneller en op een ander speelveld dan regelgeving.

Digitale middelen als wapen en verdediging

Desinformatie is niet nieuw, maar de snelheid, schaal en gerichtheid waarmee zij zich verspreidt wel. Digitale technologie maakt het mogelijk om misleidende informatie nauwkeurig te richten op specifieke doelgroepen. Het is daarmee geen tijdelijk probleem dat vanzelf verdwijnt of met incidentele monitoring en correcties kan worden opgelost. Ook ligt de oplossing niet in het blokkeren of verbieden van alles.

Technologie is een onvermijdelijk onderdeel van de oplossing. Dezelfde technieken die het mogelijk maken om desinformatie snel en gericht te verspreiden, kunnen ook worden ingezet om die dynamiek te begrijpen en te duiden. Niet om te bepalen wat gezegd mag worden, maar om te herkennen wanneer beïnvloeding plaatsvindt, hoe zij zich ontwikkelt en waar publieke weerbaarheid onder druk komt te staan. Dat inzicht is geen eindpunt, maar een noodzakelijke voorwaarde voor een weerbare digitale samenleving.

Waarom afwachten geen optie meer is

Desinformatie heeft aantoonbaar effect en wordt grootschalig en internationaal georganiseerd verspreid. Tegelijkertijd ontwikkelt zij zich sneller dan de maatregelen die overheden daartegen kunnen inzetten.

Afwachten betekent dat beïnvloeding structureel een voorsprong houdt. Juist daarom is handelen nu noodzakelijk. Niet door te bepalen wat gezegd mag worden, maar door beter te begrijpen hoe desinformatie werkt, waar zij ontstaat en wanneer zij het publieke debat beïnvloedt.

Ironisch genoeg ligt een deel van de oplossing in dezelfde technologie die het probleem heeft vergroot. Digitale platforms en AI-toepassingen maken desinformatie sneller, gerichter en op grotere schaal toepasbaar, maar kunnen ook worden ingezet om patronen, herhaling en coördinatie zichtbaar te maken. Technologie is daarom een onmisbaar hulpmiddel.

De vraag blijft dus: hoe bescherm je burgers tegen desinformatie zonder te vervallen in censuur en het inperken van de vrijheid van meningsuiting? Technologie is een begin, maar zeker nog niet de eindoplossing.

8) https://pilot.platform.ai4trust.eu/

Over de auteurs

Peter Kwant
Principal consultant

Peter is werkzaam bij Capgemini als Principal Consultant Public Sector. Peter (Executive Master Security & Defence) is projectmanager met achtergrond in cybersecurity bij Capgemini en Defensie en voormalig marineofficier.

peter.kwant@capgemini.com

https://www.linkedin.com/in/peter-kwant-06b5b811

Thirza van de Ven
Business Analist

Thirza is werkzaam bij Capgemini als Business Analist. Thirza is gespecialiseerd in de menselijke kant van veiligheid en handhaving: hoe mensen denken, handelen en keuzes maken. Met een achtergrond in (forensische) psychologie en een master criminologie vertaalt ze menselijk gedrag naar analyse en praktische inzichten.

thirza.van.de.ven@capgemini.com

www.linkedin.com/in/thirza-van-de-ven

Regie voeren in een weerbarstig ecosysteem

Hoe kan JenV onder politieke en juridische druk toch bouwen aan slagkracht?

Highlights

- Regie in JenV vraagt balanceren, geen hiërarchisch sturen
- Meer afstemming vergroot niet automatisch de slagkracht
- Capabilities brengen focus in overladen ecosystemen
- Het werksysteem is cruciaal voor vernieuwing
- Verandering vraagt realistische moed van de ambtelijke top

JenV en A&M opereren in complexe ketens onder permanente operationele, juridische enmaatschappelijke druk. Hoe organiseer je regie die niet verstikt, maar uitvoering daadwerkelijk vooruithelpt?

Regie voeren onder continue druk

Regie voeren binnen de domeinen van JenV en Asiel & Migratie is vandaag de dag een opgave op zichzelf. De vraagstukken zijn politiek gevoelig, juridisch complex en maatschappelijk scherp zichtbaar. Tegelijkertijd spelen ze zich af in ecosystemen van organisaties met eigen wettelijke taken, financieringslogica en verantwoordingslijnen die ieder onder hoge operationele druk werken. Regie betekent hier balanceren tussen tempo en zorgvuldigheid, tussen bestuurlijke rust en operationele urgentie. Vrijwel elke beweging van de ambtelijke top vindt plaats onder gelijktijdige politieke aandacht, juridisch afbreukrisico en mediadynamiek. Bestuurders en managers opereren daarbij vaak gelijktijdig in meerdere ketens, taskforces en programma's, terwijl de reguliere lijnverantwoordelijkheid met alle operationele aspecten onverminderd doorloopt.

Ambitie en realiteit lopen uiteen

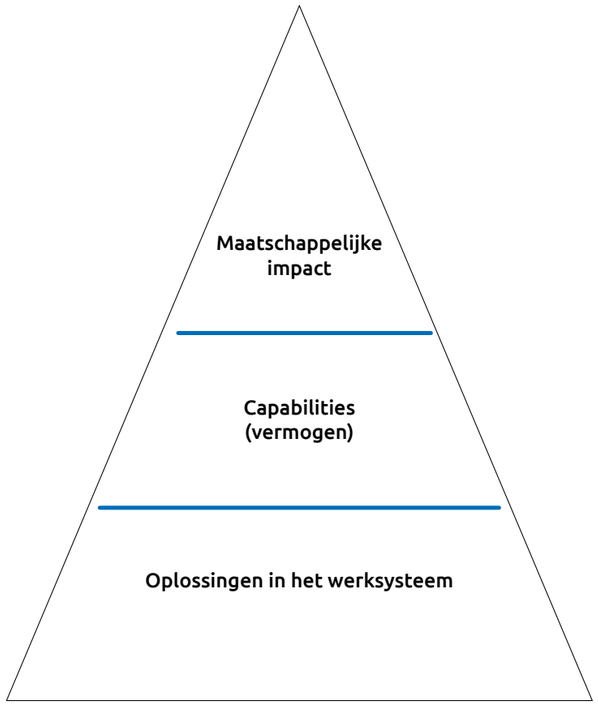
Op papier is de richting helder. In de strafrechtketen gaat het om voorspelbaarheid, kortere doorlooptijden en minder piekbelasting. In asiel en migratie om grip op instroom, opvang en doorstroom met behoud van de menselijke maat. In de praktijk trekt de dagelijkse werkelijkheid van incidenten, procedures, Kamervragen en toezicht de aandacht naar beheersing en verantwoording. De overlegdruk is zeer hoog en de verhoudingen moeten continu worden gemanaged. Het systeem functioneert, maar verandert beperkt doordat het primair is ingericht op afstemming en risicobeperking.

Waarom meer regie niet vanzelf helpt

De afgelopen jaren is veel geïnvesteerd in het versterken van regie via programma's, taskforces en coördinerende rollen. Dat heeft het systeem ook zwaarder gemaakt. Regie wordt gemakkelijk synoniem aan afstemmen en rapporteren, terwijl nieuwe interventies tijd en aandacht vragen van dezelfde schaarse groep mensen. In een context waarin management en uitvoering al onder spanning staan, leidt extra regie zelden tot versnelling.

Van structuur naar vermogen

Strategic Capability Thinking verschuift de focus van inrichting naar vermogen. Niet de vraag wie formeel verantwoordelijk is staat centraal, maar wat het systeem als geheel moet kunnen om een opgave goed uit te voeren. Capabilities beschrijven dat gezamenlijke vermogen, zoals het tijdig vertalen van instroom naar handelen of het beheersen van piekbelasting. Juist in overbelaste omgevingen helpt dit perspectief bestaande inspanning te bundelen.



Afbeelding 1 Strategic Capability Thinking

Strategic Capability Thinking visueel

De piramide hiernaast laat zien hoe maatschappelijke impact, capabilities en oplossingen in het werksysteem zich tot elkaar verhouden.

Regie als het mogelijk maken van beweging

Wanneer capabilities centraal staan, verandert de rol van regie. Het gaat minder over afdwingen via structuren en meer over het creëren van condities waaronder het systeem beter kan functioneren. Dat vraagt scherpe keuzes, waaronder het stoppen of vertragen van minder kritische initiatieven om ruimte te maken voor wat echt verschil maakt.

Stabiliteitssysteem en werksysteem

Bestuurskundige Wouter Landman onderscheidt het stabiliteitssysteem en het werksysteem. Het stabiliteitssysteem borgt rechtmatigheid en continuïteit; het werksysteem biedt ruimte voor leren en aanpassen rond concrete opgaven. Vernieuwing wordt kansrijk wanneer het werksysteem expliciet ruimte krijgt naast het formele bestel.

Toegepast in strafrecht en asiel

In de strafrechtketen verschuift het perspectief naar het vermogen om zaken ketenbreed planbaar en tijdig af te handelen. In asiel en migratie draait het om het vermogen om instroomontwikkelingen tijdig te vertalen naar voorspelbaar handelen. Dat vraagt gezamenlijke duiding, expliciete keuzes en de acceptatie dat niet elke beslissing perfect kan zijn.

Wat als? Landelijk werken aan voorspelbaarheid in de asielketen

De IND vormt een scharnierpunt in de asielketen. In de praktijk zijn instroomprognoses, beleidswijzigingen en uitvoeringsinformatie wel beschikbaar, maar worden zij niet tijdig vertaald naar gezamenlijke handelingskeuzes. Het gevolg is geen gebrek aan inzicht, maar een gebrek aan voorspelbaarheid: keuzes worden laat of impliciet gemaakt, waardoor druk zich opstapelt in uitvoering en management.

In plaats van een nieuw programma of aanvullende governance wordt een klein, integraal capabilityteam ingericht met medewerkers van IND, COA, relevante beleidsdirecties en enkele cruciale gemeenten en andere ketenpartners. Het team neemt geen lijnverantwoordelijkheid over en start geen pilots. De opdracht is scherp en begrensd: het versterken van het vermogen van de keten om landelijke instroomontwikkelingen en beleidskeuzes tijdig te vertalen naar expliciete, gedragen operationele keuzes voor de komende weken en maanden.

Het team werkt met een vaste ritmiek. Periodiek worden instroom- en voorraadontwikkelingen gezamenlijk geduid en vertaald naar concrete handelingsvragen: wat betekent dit voor prioritering, planning en uitvoerbaarheid? Deze vragen worden voorbereid als expliciete keuzepunten, inclusief effecten en afruilen, zodat bestuurlijke besluitvorming niet langer plaatsvindt onder ad-hoc tijdsdruk.

Het effect zit niet in extra capaciteit of nieuwe structuren, maar in het herstellen van voorspelbaarheid. Verrassingen in de keten nemen af, last-minute escalaties worden minder en lijnmanagers hoeven minder te improviseren. Daarmee vermindert de operationele druk op zowel uitvoering als bestuur, terwijl de formele inrichting van de keten ongewijzigd blijft.

Conclusie

Regie voeren in complexe ecosystemen vraagt meer dan beheersing. Door te sturen op capabilities ontstaat ruimte voor slagkracht zonder het systeem overhoop te halen. Klein beginnen, bewust kiezen en het werksysteem ruimte geven, juist wanneer de druk het hoogst is.

Over de auteur

Thomas Venema
Director Capgemini Invent

Thomas is werkzaam bij Capgemini Invent en gespecialiseerd in strategie en transformatie binnen het veiligheidsdomein. Thomas richt zich op vraagstukken rond regie, samenwerking en uitvoerbaarheid in complexe publieke ecosystemen.

thomas.ve nema@capgemini.com

https://www.linkedin.com/in/thomas-venema-57094576/

Hoe soeverein wil je zijn?

Is de digitale werkplek een fundament voor operationele soevereiniteit?

Highlights

- De digitale werkplek is een cruciaal en kwetsbaar fundament voor operationele soevereiniteit
- Soevereiniteit draait om controle over en continuïteit van technologie, operaties en data
- Zonder adoptie door medewerkers blijft digitale soevereiniteit slechts een papieren werkelijkheid

De digitale werkplek in het soevereiniteitsdebat

Soevereiniteit staat hoog op de agenda van overheden en publieke organisaties. De discussie gaat vaak over afhankelijkheid van niet-Europese technologieaanbieders, buitenlandse wetgeving en geopolitieke spanningen. Wat daarbij opvallend vaak ontbreekt, is aandacht voor de digitale werkplek. Juist die werkplek is het meest gebruikte, meest zichtbare én meest kwetsbare onderdeel van het digitale landschap. Wanneer daar de toegang wegvalt, staat het werk stil. Daarmee is de werkplek geen randvoorwaarde, maar een cruciale schakel in de operationele soevereiniteit van een organisatie.

Wat bedoelen we met een soevereine werkplek?

Een soevereine werkplek is geen ideologisch concept, maar een praktisch vraagstuk. Het gaat om operationele soevereiniteit: de mate waarin een organisatie kan blijven functioneren, ook als externe omstandigheden veranderen. Denk aan gewijzigde wetgeving, beperkingen vanuit leveranciers, geopolitieke druk of verstoringen bij cloudaanbieders.

De soevereine werkplek raakt drie samenhangende dimensies:

- **Operationeel**: kan het primaire werk doorgaan als voorwaarden wijzigen of diensten tijdelijk niet beschikbaar zijn?
- **Technologisch**: heeft de organisatie zeggenschap over de gebruikte software, standaarden en infrastructuur?
- **Data**: waar bevindt data zich, wie heeft toegang en onder welke jurisdictie valt deze?

De werkplek maakt deze vragen concreet. Iedere medewerker ervaart dagelijks wat afhankelijkheid of autonomie in de praktijk betekent.

Waarom is soevereiniteit nu prangender dan ooit?

Geopolitieke ontwikkelingen, afhankelijkheid van een beperkt aantal dominante aanbieders en incidenten in het publieke domein laten zien dat digitale continuïteit geen vanzelfsprekendheid is. Wanneer primaire werkplekdiensten onder druk komen te staan, heeft dat directe gevolgen voor dienstverlening, besluitvorming en publieke veiligheid. Juist daarom groeit het besef dat soevereiniteit niet alleen een infrastructuur- of cloudvraagstuk is, maar ook een werkplekvraagstuk.

Zonder begrip van het waarom en zonder goede begeleiding ontstaat weerstand, of erger: schaduw-IT. Soevereiniteit die niet wordt gebruikt, bestaat alleen op papier.

De kern: soevereiniteit vraagt méér dan technologie

Het inrichten van een soevereine werkplek begint bij technische keuzes: open standaarden, Europese of nationale oplossingen, en het beperken van lock-in. Maar technologie alleen is onvoldoende. De doorslaggevende factor is adoptie.

Een overstap naar een (gedeeltelijk) soevereine werkplek raakt het dagelijks werk van mensen. Interfaces veranderen, samenwerking verloopt anders en vertrouwde functionaliteit ziet er plots niet meer hetzelfde uit. Zonder begrip van het waarom en zonder goede begeleiding ontstaat weerstand, of erger: schaduw-IT. Soevereiniteit die niet wordt gebruikt, bestaat alleen op papier.

Voorbeeld uit de praktijk

Wanneer een publieke organisatie overstapt van een dominante commerciële suite naar een alternatief gebaseerd op open standaarden, is de technische implementatie vaak goed te organiseren. Het echte risico zit in het menselijk gedrag. Als medewerkers niet begrijpen waarom deze stap noodzakelijk is, blijven oude werkwijzen bestaan of worden informele oplossingen gezocht. Daarmee ondermijnen goedbedoelde soevereiniteitskeuzes hun eigen doel.

Weerbaarheid als strategisch resultaat

Het uiteindelijke doel van een soevereine werkplek is weerbaarheid. Niet in de zin van maximale onafhankelijkheid tegen elke prijs, maar in het vergroten van handelingsvrijheid. Dat betekent:

- Minder afhankelijkheid van één leverancier
- Meer flexibiliteit door open standaarden
- Beter kunnen inspelen op veranderingen in wetgeving en markt
- Grotere continuïteit bij verstoringen

Elke stap richting meer controle vergroot de weerbaarheid van de organisatie, ook als volledige soevereiniteit niet realistisch of wenselijk is.

De adoptie-uitdaging: mensen meenemen

Succesvolle invoering van een soevereine werkplek vraagt om bewust verandermanagement:

- Duidelijke en eerlijke communicatie over nut en noodzaak
- Gerichte training en ondersteuning
- Betrokkenheid van medewerkers als ambassadeurs
- Gefaseerde invoering met ruimte om te leren en bij te sturen

Soevereiniteit is daarmee geen IT-project, maar een organisatieverandering.

Hoe soeverein wil je zijn?

De centrale vraag is niet of soevereiniteit belangrijk is, maar hoe ver je wilt en kunt gaan. Dat is geen zwart-witte keuze, maar een spectrum. De digitale werkplek is een logisch startpunt: zichtbaar, tastbaar en direct van invloed op het functioneren van de organisatie.

Conclusie

Bestuurders en beleidsmakers: plaats de digitale werkplek expliciet in het soevereiniteitsdebat. Maak bewuste keuzes over afhankelijkheid en controle, maar investeer net zo nadrukkelijk in adoptie. Want uiteindelijk bepaalt niet de technologie, maar de mens of digitale soevereiniteit daadwerkelijk wordt gerealiseerd.

Over de auteur

Niels Lemmens
Delivery Head Public and Financial Service

Niels is werkzaam bij Cloud Infrastructure Services en is als expert op het gebied van souvereine digitale dienstverlening en infrastructuur in de publieke sector werkzaam op het snijvlak van mens en techniek.

niels.lemmens@capgemini.com
https://www.linkedin.com/in/nelemmens/

Buiten de gebaande paden is het veiliger

Waarom is het nodig dat JenV-onderdelen onderdelen over hun schaduw heen weglaten stappen en een gezamenlijk SOC weglaten beginnen?

Highlights

- Het inrichten van een SOC helpt organisaties te voldoen aan diverse wettelijke vereisten
- één ministerie – tientallen keren hetzelfde probleem
- een lokaal SOC is onbereikbaar voor de kleinere taakorganisaties
- Sui Generis is niet Sui Bedrijfsvoeris – maar in praktijk pakt het wel zo uit
- Door samenwerking zou in het ministerie van Justitie en Veiligheid een van de grootste SOC's van Nederland kunnen ontstaan

Veel taakorganisaties binnen het ministerie van Justitie en Veiligheid worstelen met dezelfde cybersecurityeisen. Een gezamenlijk SOC biedt een kans om veiliger, slimmer en betaalbaarder te werken.

Sui Generis is niet Sui Bedrijfsvoeris

Het ministerie van Justitie en Veiligheid bestaat naast het kerndepartement uit verschillende grotere taakorganisaties - bijvoorbeeld DJI, de Rechtspraak, het OM - en daarnaast ook kleinere taakorganisaties, zoals de Autoriteit Persoonsgegevens, het NFI en de Raad voor de Rechtsbijstand. Elke taakorganisatie wordt in meer of mindere mate door het ministerie van Justitie en Veiligheid aangestuurd[1]. De onafhankelijkheid van de Nederlandse rechtsketen staat hoog in het vaandel en daarvoor wordt de term Sui Generis gebruikt.

Wat is Sui Generis?

Het Latijnse "Sui Generis"[2] kan vertaald worden als "van zijn eigen soort" of "op zichzelfstaand". Binnen de context van het Nederlandse rechtsketen wordt er mee bedoeld dat de Politie, het Openbaar Ministerie, de Raad voor de Rechtspraak en de Hoge Raad onafhankelijk functioneren. Hiermee wordt een objectieve rechtsgang geborgd en kan er geen sprake zijn van politieke beinvloeding.

Alle taakorganisaties dienen taak-inhoudelijk en onafhankelijk te zijn. De toegewezen taak dient uitgevoerd te worden zonder politieke inmenging. Hoewel dit niet strikt noodzakelijk is, heeft de functionele onafhankelijkheid er ook toe geleid dat de ondersteunende bedrijfsvoering van taakorganisaties onafhankelijk en dus zelfstandig is ingericht.

Hierdoor zijn er binnen het ministerie van Justitie en Veiligheid tientallen ICT-organisaties, HR-organisaties, recruiting-organisaties en andere organisaties ontstaan, waarvan gesteld zou kunnen worden dat één organisatie net zo effectief kan zijn, maarin ieder geval schaalvoordelen zou moeten kunnen bieden. Technologische ontwikkelingen hebben het mogelijk gemaakt dat taak-inhoudelijke onafhankelijkheid van een organisatie goed geborgd zou kunnen worden in een gezamenlijke bedrijfsvoering.

Toch blijkt uit het bestaan van tientallen parallelle afdelingen, dat de beleving dat een taakorganisatie onafhankelijkheid moet inleveren in een gezamenlijke bedrijfsvoering, ertoe geleid heeft dat taakorganisaties zich zelfstandig inrichten en slechts beperkt samenwerken. Van de beleving van onafhankelijkheid kan gezegd worden dat die deels slechts schijn is; het is immers altijd dezelfde minister van Justitie en Veiligheid die naar de Tweede Kamer wordt geroepen om uitleg te geven.

Het in gezamenlijkheid, met andere taakorganisaties, zoeken naar een brede gezamenlijke bedrijfsvoering en aanpak is dus niet de standaard werkwijze van een

1) Bijlage 6: Overzicht JenV-organisaties en aan JenV-gelieerde organisaties | Ministerie van Financiën - Rijksoverheid
2) Sui generis - Wikipedia

taakorganisatie. Het is daarom ook niet verwonderlijk dat er binnen het ministerie van Justitie en Veiligheid tientallen lokale Security Operations Centers (SOC's) zijn ontstaan of worden geïnitieerd.

Verschillende taakorganisaties – Verschillende bedrijfsvoering – hetzelfde probleem

Elk van deze SOC's staat namens iedere taakorganisatie voor dezelfde vraagstukken;

- Hoe beschermen we onszelf tegen cyberaanvallen?
- Hoe kunnen we effectief en efficient aantonen dat we voldoen aan alle verschillende relevante wet- en regelgeving?

Ondanks dat het inrichten van een SOC op zichzelf niet voldoende is om aan alle verplichtingen van ondermeer de de Cyberbeveiligingswet (Cbw) en de tweede Baseline Informatiebeveiliging Overheid (BIO2) te voldoen. Blijkt in praktijk dat het wel een hele effectieve maatregel is om aantoonbaar aan een belangrijk deel van die verplichtingen te voldoen.

Wat is een SOC?

Een Security Operations Center (SOC) is een centraal team dat mensen, processen en technologie inzet om cyberdreigingen snel op te merken, te onderzoeken en aan te pakken. Zo blijven de belangrijkste bedrijfsprocessen zo goed mogelijk beschermd en worden verstoringen geminimaliseerd.

Veel gebruikte SOC-functies en bijbehorende technologieën zijn Security Incident & Event Monitoring (SIEM), Endpoint Detection & Response (EDR), Network Monitoring en Vulnerability Management. Invulling van deze functies zijn vereisten in de BIO2- en NIS2-richtlijnen. Ieder van deze technologieën genereert 24/7 meldingen van meer of minder urgente aard waar medewerkers, zogeheten security analisten, op moeten reageren.

Voor de Rijksoverheid biedt het team Versterken SOC Stelsel Rijk (VSSR) producten, diensten en samenwerkingen ten bate van het inrichten van een SOC binnen de Rijksoverheid[3].

Een SOC is een aanzienlijke investering

Het inrichten van een SOC vereist een aanzienlijke investering in zowel technologie als personeel. Een SOC dat 24/7 actief is vereist in praktijk tenminste een team van 9 security analisten en minimaal 2 security engineers capaciteit die gevonden moeten worden in een krappe arbeidsmarkt. Het beperken van actieve bewaking tot kantooruren vermindert het aantal benodigde Security Analisten, maar ook de effectiviteit. Kwaadwillenden zullen zich immers niet aan Nederlandse kantooruren houden.

Voor het ministerie van Justitie en Veiligheid is een SOC geen enkelvoudige investering, maar is de uitdaging veel groter. De gebaande paden lijken te leiden tot de inrichting van tientallen SOC's. Het is niet realistisch om te verwachten dat iedere taakorganisatie van het ministerie van Justitie en Veiligheid zelfstandig een effectief SOC inricht. Sommige taakorganisaties kunnen het budgettair niet dragen een SOC in te richten, andere taakorganisaties hebben niet de expertise om dit te doen. Daar komt bij dat alle taakorganisaties hebben te maken met krapte in arbeidsmarkt van cybersecurityspecialisten en in die markt moeten concureren met het bedrijfsleven.

3) https://www.ncsc.nl/producten-en-diensten/versterken-soc-stelsel-rijk-vssr

- Wat zou er gebeuren als dit probleem wordt omgedacht?
- Wat als er binnen het ministerie van Justitie en Veiligheid niet tientallen SOC's nodig zijn, maar slechts één gezamenlijk JenV SOC?

Bestaande samenwerkingen bieden nog geen geëffend pad naar een gezamenlijk SOC

De Justitiële ICT Organisatie (JIO) biedt gecentraliseerde ICT-diensten, waaronder SOC-dienstverlening. Een dergelijke SOC-dienstverlening is het meest effectief in combinatie met onderliggende ICT-diensten. Omdat veel organisaties ervoor kiezen om zelfstandig de ICT-voorzieningen in te richten, kan het SOC van JIO niet de brede bescherming bieden die het ministerie van Justitie en Veiligheid eigenlijk nodig heeft.

Het Nationaal Cyber Security Center (NCSC) valt weliswaar onder het Ministerie van Justitie en Veiligheid, maar is erop gericht om heel Nederland te beschermen en niet uitsluitend het ministerie van Justitie en Veiligheid.

Het Versterken SOC Stelsel Rijk (VSSR) is een programma dat sinds 2025 onder het Ministerie van Justitie en Veiligheid valt en is gericht op het verbeteren en versterken van nieuwe en bestaande SOC's, maar levert zelf geen SOC-dienstverlening.

De gebaande paden binnen het ministerie van Justitie en Veiligheid zullen haast als vanzelf leiden tot het bestaan van tientallen SOC's - voor iedere taakorganisatie één.

Buiten de gebaande paden is het veiliger

De gebaande paden binnen het ministerie van Justitie en Veiligheid zullen haast als vanzelf leiden tot het bestaan van tientallen SOC's - voor iedere taakorganisatie één. Een radicaal andere aanpak, de inrichting van één gezamelijk overkoepelend SOC, biedt een route naar een alternatieve situatie waarin meer veiligheid voor minder kosten mogelijk is;

- Zelfs als iedere organisatie binnen het ministerie van Justitie en Veiligheid slechts 1 fte zou bijdragen aan een gezamenlijk SOC, zou dit leiden tot een van de grootste Security Operations Centers van Nederland.
- Door samenwerking zouden uitdagingen met het werven, behouden en trainen van medewerkers aanzienlijk verminderen.
- Er zullen minder inkooptrajecten nodig zijn en door het grotere volume van te bewaken omgevingen zullen er gunstiger voorwaarden bedongen kunnen worden.
- Omdat organisaties elk te maken krijgen met verschillende dreigingen, ontstaat een brede variatie aan lokale maatregelen waarvan gezamenlijk geprofiteerd kan worden. De gezamenlijke optelsom daarvan is uiteindelijk groter, en vaak robuuster, dan wat één enkele taakorganisatie ooit zelfstandig zou implementeren.

Er is ook een belangrijke randvoorwaarde om tot een gezamenlijk overkoepelend SOC te komen; de inhoudelijke onafhankelijkheid van iedere taakorganisatie moet geborgd blijven. De noodzakelijke technologie voor security monitoring van de verschillende organisaties zal derhalve in silo's ingericht moeten worden. Hiermee wordt zelfs de schijn van het vermengen van informatie vermeden. Dat neemt niet weg dat op ieder van die silo's dezelfde dreigingen, detecties en responses van toepassing zijn. Eén enkele technische omgeving zal effectiever zijn, maar het opdelen van een SOC in onafhankelijke silo's heeft slechts geringe impact op alle potentiële voordelen.

Een gezamenlijk onafhankelijk J&V SOC betekent overigens niet dat organisaties binnen het ministerie van Justitie en Veiligheid geen security activiteiten meer hoeven te verrichten. Juist om taak-inhoudelijke onafhankelijkheid te borgen is lokale expertise en activiteit noodzakelijk. Met name het in stand houden van een lokale responsecapaciteit is essentieel. Het is onwenselijk en onrealistisch dat vanuit een gezamenlijk onafhankelijk SOC bepaald wordt hoe een organisatie reageert op een security incident. Er zal altijd lokale expertise benodigd zijn om te bepalen of een incident response maatregel proportioneel is in relatie tot het incident en de primaire processen van een organisatie

Hoe van het gebaande pad af te stappen

Om tot een gezamenlijk onafhankelijk J&V SOC te komen kunnen min of meer dezelfde stappen gevolgd worden die ook voor de inrichting van een lokale SOC van toepassing zijn[4], kwartier maken, doelstellingen en scope definiëren, architectuur vaststellen, inkopen en bouwen, operatien/uitbreiden/verbeteren.

Als eerste stap is daarom een grondige fase van kwartier maken essentieel. De drie belangrijkste doelen van deze fase zouden moeten zijn om:

01 Te bepalen wanneer welke taakorganisaties met welke bijdrage in een gezamenlijk overkoepelend SOC zullen stappen.

02 Te bepalen welke technische en organisatorische randvoorwaarden ingevuld moeten worden om voldoende onafhankelijkheid van taakorganisaties te kunnen garanderen.

03 Te bepalen onder welke aansturing een gezamenlijk overkoepelend SOC onder het ministerie van Justitie en Veiligheid ondergebracht moet worden.

4) NCSC - Versterken SOC Stelsel Rijk (VSSR)

Daarnaast is een eerste architectonische verkenning ook bijzonder zinvol omdat daarmee in een vroeg stadium verschillende aanvullende randvoorwaarden geïdentificeerd kunnen worden die in volgende fasen geadresseerd dienen te worden. Tenslotte zal het opstellen van een heldere financiële en functionele businesscase het voor deelnemende organisaties eenvoudiger maken ondubbelzinnig commitment af te geven.

Deze allereerste stap vereist de benoeming van een team van Kwartiermakers met aanvullende expertise;

- Een Visionair die in staat is om bruggen te bouwen tussen de verschillende belangen
- Een Architect die in staat is om een gedragen technische richting te formuleren
- Een Realist die in staat is om de, nu nog onbekende, beren op de weg te verjagen
- Een Facilitator die zorgt dat de Visionair, de Architect en de Realist effectief kunnen werken.

Met een relatief kleine investering van initieel enkele FTE's gedurende één jaar en de bereidheid om de nek uit te steken zou het ministerie van Justitie en Veiligheid buiten de gebaande paden om een sprong in het diepe kunnen wagen die over enkele jaren ontzettend veel zekerheid en daarmee veiligheid kan bieden waardoor de minister in ieder geval niet meer vanwege een cybersecurity incident naar de Tweede Kamer wordt geroepen.

Conclusie

De conventionele aanpak zal naar verwachting leiden tot de inrichting van tientallen lokale SOC's. Door intensieve samenwerking van taakorganisaties valt er veel aan effectiviteit en efficientie te winnen. Het onafhankelijk functioneren van een taakorganisatie is een randvoorwaarde die in een samenwerking gewaarborgd moet zijn. Ondanks de randvoorwaarden kan gesteld worden dat een intensievere samenwerking aanzienlijke voordelen biedt, zoals bijvoorbeeld de inrichting van een gezamenlijk overkoepelend SOC.

Om tot dat succes te komen is het essentieel dat iedere organisatie binnen het ministerie van Justitie en Veiligheid bereid is de principiële keuze te maken om een een stukje zelfstandigheid van bedrijfsvoering in te leveren in ruil voor alle voordelen die een gezamenlijk en onafhankelijk JenV SOC biedt. Zonder commitment van alle betrokken organisaties is ieder initiatief om tot een gezamenlijk en onafhankelijk JenV SOC te komen gedoemd te mislukken.

Over de auteur

Folkert Visser
Managing Consultant Cyber Defense

Folkert is een Cyber Defense enthousiasteling die uitblinkt in het overbruggen van het gat tussen theorie, policy en de weerbartsige praktijk. Hij heeft een achtergrond in de telecomsector, hij richt zich tegenwoordig vooral op het versterken van cybersecurity in het publieke domein.

https://www.linkedin.com/in/fkvisser

folkert.visser@capgemini.com

Effectieve AI voor continue weerbaarheid en compliance

Hoe versterken organisaties hun digitale weerbaarheid zó dat security, continuïteit en compliance aantoonbaar geborgd blijven in een tijd waarin dreigingen sneller evolueren dan ooit?

Highlights

- Continue digitale dreiging vraagt om realtime inzicht en sturing
- Traditionele risicobeheersing schiet tekort in een ketenafhankelijke wereld
- AI-agents maken security, continuïteit en compliance aantoonbaar en doorlopend
- Van periodieke controle naar proactieve, geïntegreerde weerbaarheid

Digitale dreiging raakt publieke veiligheid en continuïteit. Hoe behouden organisaties grip en compliance terwijl aanvallen sneller en ketenbreed toeslaan?

Digitale dreiging raakt vandaag niet alleen IT-systemen, maar de kern van publieke organisaties: veiligheid, continuïteit en bestuurbaarheid. Voor het publieke domein betekent dit dat digitale incidenten direct kunnen doorwerken in primaire processen, medewerkersveiligheid en het vertrouwen van burgers. Tegelijkertijd worden organisaties geconfronteerd met een dreigingslandschap dat sneller, gerichter en ketenbreed opereert, terwijl afhankelijkheden van externe ICT-diensten blijven toenemen.

Wetgevers en toezichthouders spelen hierop in met strengere eisen aan aantoonbare risicobeheersing, continu toezicht en bestuurlijke verantwoordelijkheid. Dat vraagt om meer dan periodieke controles of losse rapportages. De centrale vraag is daarom niet óf organisaties moeten veranderen, maar hóé zij hun digitale weerbaarheid versterken zonder hun publieke opdracht uit het oog te verliezen. Dit artikel laat zien hoe AI-agents publieke organisaties kunnen ondersteunen bij het continu monitoren, duiden en beheersen van digitale risico's, als versterking van professioneel handelen en als fundament voor aantoonbare veiligheid, continuïteit en compliance.

Wat is de aard van de digitale dreiging waar organisaties vandaag mee te maken hebben?

De digitale dreiging waarmee organisaties vandaag worden geconfronteerd is continu, doelgericht en steeds sterker verweven met de digitale ketens waarin zij opereren. Cybercriminelen, statelijke actoren en andere dreigingsgroepen maken gebruik van schaalbare technieken en generatieve AI, waardoor aanvallen sneller, geavanceerder en moeilijker te herkennen zijn. Digitale dreiging manifesteert zich daardoor niet langer incidenteel, maar structureel en vaak specifiek gericht op bepaalde organisaties, functies of processen.

Voor organisaties in het publieke domein is deze dreiging geen abstract technologisch vraagstuk. Digitale incidenten raken direct aan de continuïteit van publieke dienstverlening, de veiligheid van medewerkers en het vertrouwen van burgers. Verstoringen blijven bovendien zelden beperkt tot één organisatie: afhankelijkheden in software, cloud-diensten en leverancierssketens zorgen ervoor dat impact zich snel verspreidt over meerdere partijen en maatschappelijke processen.

Deze realiteit stelt hogere eisen aan risicobeheersing en bestuurlijke grip. Organisaties moeten digitale risico's sneller kunnen signaleren, duiden en opvolgen over de gehele keten heen, terwijl de beschikbare reactietijd steeds korter wordt. Periodieke, handmatige controles en statische risicobeelden schieten daarbij tekort. Effectieve digitale weerbaarheid vraagt om continu inzicht, samenhang en tijdige besluitvorming, juist in een dreigingslandschap dat voortdurend in beweging is.

Waarom schiet de traditionele manier van risicobeheersing tekort in het huidige dreigingslandschap?

De toenemende digitale kwetsbaarheid van organisaties komt voort uit twee structurele tekortkomingen, die in de volgende paragraaf nader worden toegelicht. Ten eerste is er de groeiende afhankelijkheid van uitbestede ICT-diensten, gecombineerd met een versnipperde manier van beheersen en monitoren over de digitale keten. Ten tweede neemt de regelgevingsdruk toe en worden organisaties steeds vaker verplicht om hun risicobeheersing aantoonbaar te maken.

De afhankelijkheid van uitbestede ICT-diensten diensten raakt direct aan ketenveiligheid en bestuurlijke grip: naarmate toezicht en regie bij externe partijen liggen, neemt het vermogen af om risico's te overzien, eisen te handhaven en tijdig bij te sturen.

Publieke organisaties vertrouwen externe leveranciers en cloudproviders voor cruciale digitale functies, terwijl de directe sturingsmogelijkheden op beveiliging, continuïteit en incidentrespons beperkt zijn. De SecurityScorecard sectoranalyse 2025 toont internationaal aan dat een aanzienlijk deel van beveiligingsincidenten zijn oorsprong vindt bij derde partijen, waarbij één kwetsbare leverancier meerdere organisaties tegelijk kan raken. Tegelijkertijd blijft een substantieel deel van de incidenten het gevolg van interne kwetsbaarheden, zoals configuratiefouten of menselijke fouten. Digitale dreiging manifesteert zich daarmee zowel binnen als buiten de eigen organisatie.

De impact van ketenafhankelijkheid beperkt zich dus niet tot individuele organisaties. Eén kwetsbare leverancier kan leiden tot verstoring van kernprocessen bij meerdere publieke en private partijen tegelijk. Het Rathenau Instituut wijst erop dat publieke sectoren zoals zorg, onderwijs en overheidssystemen in Nederland structureel afhankelijk zijn geworden van een beperkt aantal grote cloudaanbieders. Deze concentratie vergroot systeemrisico's en bemoeilijkt herstel bij grootschalige incidenten.

De toenemende afhankelijkheid van uitbestede ICT-diensten vergroot de afstand tussen uitvoering en verantwoordelijkheid. Hoewel de operationele beveiliging en incidentrespons vaak bij leveranciers zijn belegd, blijven bestuurders eindverantwoordelijk voor continuïteit, beveiliging en naleving. Effectieve regie vereist daarom samenhangend en actueel inzicht in de volledige digitale keten. In de praktijk is dat inzicht vaak versnipperd over audits, rapportages, contracten en incidentele controles. Het ontbreken van samenhang en context bemoeilijkt tijdig ingrijpen en proactieve sturing wanneer risico's zich ontwikkelen. Hierdoor komt niet alleen de weerbaarheid, maar ook de aantoonbaarheid van bestuurlijke risicobeheersing onder druk te staan.

Deze lijn is zichtbaar in meerdere Europese toezichtrapporten, waaronder het Joint Committee Report van de Europese toezichthouders (EBA, EIOPA, ESMA), dat benadrukt dat instellingen aantoonbaar en continu inzicht moeten geven in hun operationele en ICT-risico's, inclusief monitoring en toetsing hiervan. Ook het Digital Operational Resilience Act (DORA) raamwerk verplicht organisaties om risico's inzichtelijk te maken, maatregelen te documenteren en periodiek te testen op effectiviteit, inclusief rapportage aan toezichthouders. Periodieke manuele controles en losse registraties volstaan niet langer; governance moet continu, samenhangend en inzichtelijk zijn.

Daarnaast bevestigen recente analyses dat de EU regelgevende agenda steeds meer inzet op transparantie, risicobeheer en aantoonbare weerbaarheid, bijvoorbeeld via CRR III/CRD6 en de bredere operational resilience agenda voor organisaties in de publieke en private sector

Het rijksbrede onderzoek 'Van kwetsbaar naar weerbaar' concludeert bijvoorbeeld dat cruciale overheidsprocessen onvoldoende bestand zijn tegen langdurige uitval van ICT-diensten. Het rapport benadrukt dat politieke en ambtelijke top verantwoordelijk blijven voor het expliciet afwegen en vastleggen van continuïteitsrisico's en bijbehorende mitigerende maatregelen. Dit is verankerd in NIS2-richtlijnen en het rijksbrede kader BIO2. Aantoonbare risicobeheersing is daarmee geen administratieve last, maar een voorwaarde voor bestuurlijke legitimiteit en publieke verantwoording.

Hoe kunnen AI-agents bijdragen aan beveiliging, continuïteit en compliance?

In dit spanningsveld komen AI-agents in beeld. AI-agents zijn digitale assistenten die continu werken en beleid, risico's, logs en controles in samenhang kunnen interpreteren. Zij vormen geen vervanging van professionals, maar een versterking van bestaande rollen en verantwoordelijkheden binnen security, governance en risicobeheersing.

In plaats van losse beveiligingssignalen te analyseren, kan een AI-agent continu bewaken welke digitale diensten cruciaal zijn voor primaire processen en welke externe leveranciers daarbij betrokken zijn. Door beschikbaarheid, incidenthistorie, contractuele afspraken en vastgestelde risicotoleranties te combineren, signaleert de agent wanneer de continuïteit van een essentieel proces structureel onder druk komt te staan. Bestuurders krijgen daarmee een actueel en samenhangend beeld van waar risico's zich opstapelen en of bestaande maatregelen nog volstaan, waardoor tijdig kan worden bijgestuurd voordat daadwerkelijke uitval optreedt.

Wanneer een AI-agent constateert dat een kritieke leverancier structureel afwijkt van vastgelegde beveiligings- of continuïteitseisen, plaatst hij dit in bestuurlijke context. De agent maakt inzichtelijk welke normen worden geraakt, welke risico's toenemen en welke expliciete of impliciete risicoacceptatie dit betekent. Zo ontstaat geen technisch alarm, maar een onderbouwd signaal dat aantoonbaar ondersteunt bij besluitvorming, toezicht en publieke verantwoording.

Iets vergelijkbaars geldt voor continuïteit en ketenrisico's. Veel organisaties hebben (na de assessmentfase) leveranciersrisico's beschreven in documenten of contracten, maar monitoren deze niet continu. Incidenten waarbij één leverancier grote delen van de digitale keten raakt, laten zien hoe kwetsbaar deze aanpak is. Een AI-agent kan beschikbare leveranciersinformatie, kwetsbaarheidsmeldingen en interne afhankelijkheden continu volgen en vroegtijdig signaleren wanneer missie-kritieke processen risico lopen.

Ook op het gebied van compliance bieden AI-agents concrete meerwaarde. Verplichtingen onder NIS2, CER en DORA vereisen dat organisaties kunnen aantonen dat controles daadwerkelijk werken. AI-agents kunnen control-evidence continu verzamelen, configuraties vergelijken met beleidskaders en afwijkingen vastleggen met bron, tijdstempel en context. Daarmee

ontstaat een actueel, consistent en herleidbaar verantwoordingsbeeld richting toezichthouders en auditors.

Wanneer een kritieke afhankelijkheid in de digitale keten ontstaat, bijvoorbeeld door structurele prestatieproblemen bij een cloudleverancier, signaleert de AI-agent dit als indicatie dat de betrouwbaarheid van essentiële diensten onder druk staat. Door deze signalen te koppelen aan interne processen en potentiële impact, ondersteunt de AI-agent tijdige maatregelen, nog vóórdat een daadwerkelijke verstoring optreedt.

Publieke waarde en professionele verantwoordelijkheid

Voor professionals in het publieke domein raakt deze ontwikkeling aan meer dan efficiëntie of compliance alleen. Digitale weerbaarheid is onlosmakelijk verbonden met publieke waarde: het vermogen van organisaties om hun maatschappelijke opdracht betrouwbaar, veilig en voorspelbaar uit te voeren. Burgers verwachten dat essentiële diensten beschikbaar blijven, dat gevoelige informatie wordt beschermd en dat de overheid aantoonbaar grip heeft op digitale risico's, juist wanneer uitvoering deels is uitbesteed.

AI-agents ondersteunen professionals in die verantwoordelijkheid door continu inzicht te bieden in risico's die anders versnipperd of onzichtbaar blijven. Zij versterken niet alleen snelheid, maar ook de kwaliteit van besluitvorming doordat risico-informatie contextueel, actueel en uitlegbaar wordt gepresenteerd. Daarmee dragen AI-agents bij aan transparantie, verantwoording en bestuurlijke legitimiteit. Niet als technologische 'shortcut', maar als instrument dat vakmanschap, toezicht en governance ondersteunt.

AI-agents als sleutel tot aantoonbare en continue digitale weerbaarheid

De digitale dreiging ontwikkelt zich sneller dan organisaties kunnen bijbenen, terwijl de afhankelijkheid van uitbestede ICT-diensten de afstand tussen risico en regie vergroot. Wetgeving vraagt daarom om aantoonbare, doorlopende beheersing. AI-agents bieden een manier om deze kloof te verkleinen door continu digitaal inzicht, samenhang en auditbewijs te leveren.

Voor professionals in het publieke domein is dit geen technologische hype, maar een strategische keuze. Wie nu investeert in intelligente en aantoonbare risicobeheersing, vergroot digitale weerbaarheid, bestuurlijke grip en het vertrouwen van burgers. Dat vraagt om een samenhangende aanpak waarin mensen, governance en technologie elkaar versterken. Interne professionals blijven daarbij cruciaal; AI-agents functioneren als versterkend instrument in een steeds complexer digitaal landschap.

Tot slot vergt deze ontwikkeling ook een culturele verschuiving: van periodieke controles naar continu inzicht, van reactief naar proactief risicobeheer. Organisaties die deze omslag tijdig maken, zetten AI-agents in als strategische bouwsteen voor blijvende digitale weerbaarheid en publieke veiligheid.

Over de auteurs

Marieke van de Putte
Principal consultant - Go-to-Market Lead, Enterprise Resilience

Marieke is verantwoordelijk voor de Go-to-Market-strategie binnen Enterprise Resilience. Zij focust op het vergroten van bewustzijn rondom digitale weerbaarheid en het versnellen van de adoptie van compliance-automatisering binnen publieke en private sectoren. Met haar strategische blik en expertise van 25+ jaar helpt zij organisaties de stap te maken van traditionele risicobeheersing naar geïntegreerde, schaalbare en aantoonbare resilience-oplossingen.

marieke.vande.putte@capgemini.com
https://www.linkedin.com/in/marieke-van-de-putte-43120a4/

Rahul Rauniyar
Senior Manager - Delivery Lead, Enterprise Resilience

Rahul begeleidt organisaties bij de implementatie van moderne, data-en AI-gedreven risk & compliance-oplossingen. Hij richt zich op de praktische industrialisatie van automated controls, continuous monitoring en het ontwerpen van schaalbare GRC-architecturen. Met zijn ervaring in cybersecurity, Risk & Compliance helpt hij organisaties om complexe risicobeheersing efficiënt én aantoonbaar te operationaliseren.

rahul.rauniyar@capgemini.com
https://www.linkedin.com/in/rahul-rauniyar/

Olaf Kurpershoek
Consultant - Enterprise Resilience (Capgemini)

Olaf specialiseert zich in operationele beveiliging, ketenrisico's en de bescherming van vitale processen. Hij ondersteunt organisaties bij het doorlichten van hun digitale afhankelijkheden, het verbeteren van detectie- en responsprocessen, en het toepassen van security-best practices binnen zowel IT- als OT-omgevingen.

olaf.kurpershoek@capgemini.com
https://www.linkedin.com/in/olafkurpershoek/?locale=en

Colofon

Deze editie van Trends in Veiligheid is tot stand gekomen met medewerking van:

Aydan Gunduz
Martijn van de Ridder
Natasja Pieterman
Erik Staffeleu
Gerard Pieter Borren
Katya Smit
Roeland de Koning
Joris Commissaris
Merve Gurbuzcan
Dennis Paardekoper
Bart van Riel

Advies, ontwerp en productie:

Marketing & Communicatie, Capgemini Nederland B.V.

Ernes Mahmutovic
Thomas de Klerk
Arundhati Bhattacharya
Ashim Karmakar

Over Capgemini

Capgemini is een wereldwijd opererende partner voor bedrijfs- en technologische transformatie, gedreven door AI, die aantoonbare bedrijfswaarde levert. Wij verbeelden de toekomst van organisaties en maken die werkelijkheid met AI, technologie en mensen. Met een sterke historie van bijna 60 jaar zijn wij een verantwoordelijke en diverse organisatie met meer dan 420.000 medewerkers in ruim 50 landen. Wij leveren end-to-end diensten en oplossingen, ondersteund door diepgaande sectorkennis en een sterk partner-ecosysteem. Hierbij benutten wij onze capaciteiten op het gebied van strategie, technologie, design, engineering en bedrijfsvoering. Capgemini Group rapporteerde in 2025 een wereldwijde omzet van €22,5 miljard.

Make it real.

Capgemini Nederland B.V.
Postbus 2575 – 3500 GN Utrecht
+31 30 689 00 00
www.capgemini.nl

2C-006.26

Copyright © 2026 Capgemini. All rights reserved.