# Trends in Veiligheid 2025

*Digitale Veiligheid* als Fundament voor een Weerbare Samenleving

Capgemini

# Trends in Veiligheid 2025

*Digitale Veiligheid* als Fundament voor een Weerbare Samenleving

# Inhoudsopgave

# Digitale veiligheid: fundament voor publieke veerkracht

## Een strategische visie op zes maatschappelijke kernvragen

**Nu onze samenleving in hoog tempo digitaliseert, is veiligheid een systeemvoorwaarde geworden. Zonder digitale veiligheid geen betrouwbare dienstverlening, geen weerbare instituties en geen toekomstbestendige samenleving. Welke implicaties heeft dat voor de publieke sector anno 2025?**

We lijken het stadium van voorspellen echt voorbij: wat ooit (misschien wel hoogst onwaarschijnlijke) toekomstmuziek was, speelt nu keihard op onze radio. De trends in veiligheid bonzen hard op de voordeur van onze publieke sector. Die staat voor ingrijpende keuzes die ook nog eens snel en adequaat handelen vereisen. Niet alleen door de toegenomen complexiteit van digitale technologie, maar zeker ook door alle mondiale ontwikkelingen die het speelveld fundamenteel, en bijna dagelijks, veranderen. Het politieke landschap, de blijvende en toegenomen (digitale)dreigingen en het vervagen van internationale afspraken stellen allerlei overheden en overheidsinstanties voor nieuwe dilemma's. Tegelijkertijd neemt de druk van binnenuit toe: burgers verwachten snelheid, bescherming, transparantie, controle over hun gegevens en regie van de overheid op het van gebied digitale transformatie en veiligheid. Juist nu technologie diffuse risico's introduceert.

Het rapport verkent deze nieuwe realiteit binnen onze publieke sector.

**De samenleving wordt slimmer. De risico's ook.**

Digitale transformatie is inmiddels geen beleidsambitie meer maar dagelijkse praktijk. AI wordt geïntegreerd in processen, data is leidend voor besluitvorming, en digitale dienstverlening is de standaard. Maar elke stap vooruit brengt ook nieuwe afhankelijkheden, verantwoordelijkheden en kwetsbaarheden met zich mee. In een wereld waarin Amerikaanse big tech-partijen alles domineren, groeit het digitale ongemak. Autonomie is een strategisch doel geworden. Maar hoe bouw je als overheid aan onafhankelijkheid als je techstack uit Silicon Valley komt?

De kwetsbaarheid van onze samenleving zien we ook terug bij het groeiende fenomeen van impersonatie: burgers die slachtoffer worden van oplichters die zich voordoen als agent, gemeenteambtenaar of zorgverlener. De technologische grens tussen echt en nep vervaagt snel, en met die vervaging neemt het risico op ondermijning van vertrouwen in publieke instellingen toe. Een aanpak die de burger centraal stelt, bijvoorbeeld in de ontwikkeling van identiteitsverificatie-oplossingen, wordt daarmee geen luxe, maar noodzaak.

Publieke organisaties moeten dus niet alleen technologische keuzes maken, maar ook maatschappelijke: hoe waarborgen ze transparantie? En hoe zorgen ze dat digitale oplossingen bijdragen aan rechtvaardigheid en vertrouwen? Hoe houden ze de digitale systemen en algoritmen inclusief?

**Zes thema's, één rode draad**

Binnen het publieke domein zien we zes thema's die het hart raken van de veiligheidsopgave: Burger Centraal, Toekomst van Werk, Duurzaamheid, Weerbaarheid, Wendbaarheid en Data. Ieder thema kent zijn eigen dynamiek, maar samen vertellen ze één verhaal: technologie, maatschappij en veiligheid zijn onafscheidelijk met elkaar verbonden.

Zo raakt het thema Toekomst van Werk twee pijnpunten tegelijk: het personeelstekort én de opkomst van GenAI. In veel veiligheidsorganisaties wordt gezocht naar manieren om mensen slimmer en flexibeler te laten werken. Een volwassen digitale werkomgeving kan werkdruk verlagen en bureaucratie reduceren. Tegelijk vraagt het om scherp toezicht op hoe GenAI wordt ingezet in HR-processen, van werving tot personeelsplanning. Want hoewel AI strategisch voordeel kan bieden, vereist het ook bewustwording, training en grenzen. Technologie en talent moeten samen optrekken.

Duurzaamheid lijkt op het eerste gezicht een domein van energie en klimaat, maar raakt ook direct aan veiligheid. Denk aan extreme weersomstandigheden die leiden tot overstromingen of bosbranden, of de maatschappelijke onrust die ontstaat bij ecologische verstoringen. In een tijd waarin de legitimiteit van de overheid onder druk staat, wordt duurzaamheid ook een maatstaf voor maatschappelijke betrouwbaarheid. Organisaties die duurzaamheid als kernwaarde integreren, blijken beter bestand tegen schokken, zowel ecologisch als sociaal.

Ook op geopolitiek niveau worden keuzes steeds ingewikkelder. Wendbaarheid blijkt geen innovatiejargon, maar een overlevingsstrategie. De afhankelijkheid van Amerikaanse techbedrijven maakt onze digitale wendbaarheid impliciet ook tot een veiligheidsvraagstuk. Moet je als publieke organisatie zelf blijven bouwen om grip en autonomie te behouden? Of

kies je voor snelheid en schaalbaarheid met alle afhankelijkheden van dien?

En hoe staat het met onze weerbaarheid? Cybersecurity alleen lijkt niet meer te volstaan als defensiemechanisme. Organisaties moeten zich ook voorbereiden op scenario's waarin bestaande ketens onder druk komen te staan. De blauwdrukken voor cyberweerbaarheid zijn er. Nu moeten ze nog integraal onderdeel worden van de veiligheidsstrategie.

En tot slot is er data. Zonder goede data geen zicht, geen actie, geen besluit. Maar met verkeerde of onbetrouwbare data ontstaan juist nieuwe risico's. Defensie experimenteert inmiddels met datagedreven informatiedominantie, waarbij governance en techniek samen zorgen voor snelheid én controle. Ook andere delen van de overheid kunnen daarvan leren: grip op data is de voorwaarde voor publieke regie in een versneld technologisch tijdperk.

### Van incidentgericht naar strategisch adaptief

Wat al deze bewegingen vragen van de publieke sector is niet alleen technische competentie, maar strategische keuzes. De reflex om te reageren op incidenten is begrijpelijk, maar onvoldoende. Veiligheid is een voortdurend veranderende grootheid geworden. Bestendigheid is niet langer wat ons staande houdt; het is ons aanpassingsvermogen dat bepalend zal zijn in de komende jaren.

Dit vraagt om anders kijken. Om het durven combineren van technologische innovatie met publieke waarden. Om samenwerking over domeinen en bestuurslagen heen. En om het lef om niet alleen risico's te beheersen, maar ook actief te sturen op de keuzes die vandaag nodig zijn voor een veilige toekomst.

### Niet alles hoeft tegelijk. Maar niets kan meer wachten.

De boodschap van Trends in Veiligheid 2025 is helder: het publieke domein hoeft niet alles morgen op orde te hebben. Maar moet wel vandaag beginnen. Met heldere keuzes. Met realistische scenario's. En met het inzicht dat digitale veiligheid niet één van de opgaven is, maar de voorwaarde waaronder alle andere kunnen slagen.

Veiligheid is immers de kern van onze democratische veerkracht.

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


Burger
centraal

Interview:

# Veiligheid hand in hand met innovatie bij de Raad voor de Kinderbescherming

Bij de Raad voor de Kinderbescherming (‘de Raad’) is geen casus hetzelfde. Voor het uitbrengen van een zorgvuldig en objectief advies is betrouwbare, volledige informatie cruciaal. Volgens Erwin Bremer, directeur bedrijfsvoering en Chief Information Officer, staan in de bedrijfsvoering daarom drie zaken centraal; het kind, de medewerkers, en veiligheid.

**Erwin Bremer**

Directeur Bedrijfsvoering
bij de Raad voor de
Kinderbescherming (RvdK).

Kinderen hebben recht op een gezonde en stabiele ontwikkeling. In Nederland beschermt de Raad dat recht voor kinderen die in hun ontwikkeling worden bedreigd tijdens dwangtrajecten. Dat kunnen ondertoezichtstellingen, uithuisplaatsingen of taakstraffen zijn. Daarnaast coördineert de Raad taakstraffen en geven ze advies bij adoptie, pleegzorg en complexe scheidingen. Vanuit het kinderperspectief kijken raadsonderzoekers of casusregisseurs naar de omgeving van het kind en naar het verloop van het traject. Vervolgens levert de Raad een advies aan een rechter. Bremer: “We komen bij mensen achter de voordeur. Onze raadsonderzoekers staan naast het kind en kijken naar de omgeving. De adviezen van de Raad raken het gezin in het hart, dus er moet altijd een objectief en onderbouwd advies zijn. Het doel van onze bedrijfsvoering is het ondersteunen van de complexe taken van onze - raadsonderzoekers.

### De juiste informatie, op het juiste moment, bij de juiste persoon

Informatievoorziening is cruciaal voor het primaire proces van de Raad, zegt Bremer. “Het kind staat daarin altijd centraal. Daarvoor moeten we als bedrijfsvoering in twee belangrijke zaken voorzien: ons werk ondersteunt allereerst de rechtsgelijkheid, van Leeuwarden tot Limburg. We volgen daarom procedures. We ondersteunen waar het gaat om het verkrijgen, opslaan en beveiligen van de informatie die de raadsonderzoekers en andere medewerkers nodig hebben bij het uitvoeren van het werk. Ten tweede: elke situatie is anders. Wij ondersteunen in het verkrijgen, opslaan en beveiligen van de informatie die raadsonderzoekers - en andere medewerkers – nodig hebben bij het uitvoeren van hun werk. De juiste informatie, op het juiste moment, bij de juiste persoon. Zonder die combinatie kan een raadsonderzoeker nooit een juist advies geven.”

### Digitalisering ondersteunt de bedrijfsvoering

Digitalisering van de informatievoorziening is daarbij essentieel. Sinds 2018 is het digitale archief van de Raad leidend in de bedrijfsvoering. In dat archief worden alle onderzoeksgegevens van een kind vastgelegd in een digitaal dossier. Dat gebeurt om achteraf een heldere verantwoording te leveren, maar ook opdat raadsonderzoekers toegang hebben tot de juiste dossiers, bijvoorbeeld wanneer er werk van een zieke collega moet worden overgedragen. Bremer: “Digitalisering ondersteunt de betrouwbaarheid, actualiteit en beschikbaarheid van onze informatievoorziening. Het stelt onze mensen in staat om snel, accuraat en direct over verschillende bronnen te beschikken. Met de ontwikkelingen in digitalisering wordt de informatievoorziening daardoor steeds sneller en betrouwbaarder.”

### Razendsnelle verandering brengt uitdagingen en kansen

Tijdig kunnen inspelen op die ontwikkelingen is essentieel. Bremer: “Het tempo van wijzigingen ligt hoog, gestuurd vanuit wet- en regelgeving, technische of maatschappelijke ontwikkelingen, of ontwikkelingen binnen onze samenwerkingsverbanden. Dat brengt uitdagingen met zich mee.

Ons absorptievermogen om nieuwe technologieën te omarmen moet permanent groot zijn, en de mens kan daarin een kwetsbare factor zijn. We moeten daarom zorgen dat de 'AI en datageletterdheid' van medewerkers op orde is en blijft. Datageletterdheid betekent dat zij op de hoogte zijn van de laatste ontwikkelingen op het gebied van data en digitalisering, maar ook dat ze in staat worden gesteld om zich op nieuwe veranderingen voor te bereiden. Vijf jaar geleden, toen de Coronapandemie uitbrak, wist bijvoorbeeld niet iedereen hoe je moest videobellen. Binnen een week was dat gemeengoed. Dit tempo biedt ook kansen. Met de juiste innovatie kunnen we sneller informatie ontsluiten. AI-tools zouden bijvoorbeeld kunnen zorgen dat inzageverzoeken minder beslag leggen op het primaire proces en onze medewerkers."

**Veiligheid voorop**

Innovatie biedt veel nieuwe mogelijkheden, maar voor Bremer staat veiligheid daarbij altijd voorop. Hij pleit voor zorgvuldige afwegingen: "Ik vind dat we in de bedrijfsvoering soms saai moeten zijn. Onze taak is het gestructureerd op orde brengen van een veilige basisorganisatie. Ontwikkelingen zoals AI zijn allemaal volgend. Innovatie is noodzakelijk, maar veiligheid en betrouwbaarheid staan bovenaan. Daarom leggen wij de komende jaren de focus op een data-en beveiligingslab en niet op een innovatielab. Tuurlijk heeft innovatie een functie maar het is niet onze drijfveer. Innovatie heeft in zo'n lab uiteraard wel een functie. Als we met bijvoorbeeld AI op een veilige en transparante manier makkelijker informatie kunnen ontsluiten en actief kunnen aanbieden, dan kan dat veel bijdragen aan onze hoofddoelstellingen. Het moet echter altijd heel duidelijk zijn waar onze focus ligt. Dat is misschien niet heel hip, maar veiligheid is het allerbelangrijkst. Zeker binnen een organisatie als de Raad."

**Op de achtergrond**

Voor Bremer draait zijn team dan ook niet om het verwezenlijken van IT-ambities an sich. "Bedrijfsvoering hoort op de achtergrond te functioneren. Je moet ons niet zien of merken. Het gaat uiteindelijk allemaal om het kind; dat staat centraal. Om dat uitgangspunt in onze informatievoorziening te borgen, betrekken wij altijd mensen uit het primaire proces bij onze IT-teams. Zij weten wat er nodig is, wat er nog ontbreekt. Dat is onze werkwijze: we moeten vanuit het primaire doel verbeteringen aanbrengen, niet vanuit een IT-ambitie. Je zal mij geen presentatie zien geven waarbij het kind secundair is, of waarbij niet een individuele casus of een praktijkervaring van een collega centraal staat. Onze primaire taak is de basis. Altijd."

**Wanneer een laptop hapert**

Dat illustreert Bremer met een pakkend voorbeeld: "Stel, de moeder van een kind wil vanwege een nieuwe partner verhuizen en dat zou betekenen dat de vader zijn kind niet meer kan zien tijdens zijn middagpauze. Tijdens het gesprek daarover wordt de vader – precies als hij zijn emotionele betoog doet – tot twee keer toe onderbroken door een haperende internetverbinding van de verslagleggende raadsonderzoeker. Het gesprek leidt uiteindelijk tot een goede regeling. Maar de vader werd door die verstoring diep geraakt. Hij benoemt dat, en hij heeft groot gelijk. Een werkende bedrijfsvoering is een wezenlijk onderdeel van ons proces. De les is: ons werk als bedrijfsvoering gaat niet over een laptop of de verbinding. Dat zijn slechts de middelen. Doen die het niet, dan doet dat in ons werk enorm veel afbreuk aan de mens. De beste ondersteuning die wij vanuit de bedrijfsvoering kunnen leveren, is dat alles werkt."

**Een duidelijke focus**

Digitalisering vereist echter ook verregaande automatisering en standaardisatie. Daarbij kan de menselijke maat in de knel komen. Om te voorkomen dat het kind ondersneeuwt in het toekomstige IT-landschap, is volgens Bremer een duidelijke focus cruciaal: "Informatievoorziening is primair gericht op het ondersteunen van onze raadsonderzoekers. Informatie is daarbij een middel, niet het doel op zich. We zorgen daarom dat het systeem nooit bepaalt, en dat er nooit een stap wordt overgeslagen wanneer er een afweging moet worden gemaakt. Informatievoorziening is belangrijk, maar het mag nooit leidend zijn. Het menselijk contact staat voorop, informatie ondersteunt de casus – de mens."

**Trends voor overheden**

Met het menselijke contact in het achterhoofd ziet Bremer ook een aantal ontwikkelingen in de informatievoorziening richting burgers. "Allereerst moet informatie beter aansluiten bij de belevingswereld van onze doelgroepen. Als wij een brief sturen naar een zestienjarige om zich te melden voor een taakstraf, wordt die wellicht niet gelezen. Stuur je een appje, dan leest die zestienjarige het waarschijnlijk wel. Daarnaast kan de overheid transparanter en voor burgers beter benaderbaar worden door een betere toegang tot informatie. Alleen al de toegang tot betrouwbare informatie geschreven op het juiste taalniveau maakt voor een burger een groot verschil. Moeten alle medewerkers dan geschoold worden om op dit niveau te kunnen schrijven of zetten we hier AI voor in? Bovendien is het voor overheden belangrijk om proactief met feiten en informatie te komen, want het contact met burgers verloopt niet automatisch vanuit een vertrouwensbasis. Tot slot willen we alle informatie direct beschikbaar hebben in het contact met de burgers. Het is niet meer acceptabel om te zeggen 'ik heb het antwoord nu even niet'. Dat wordt niet meer gepikt. Snel beschikken over informatie is de norm geworden. Voor al die ontwikkelingen geldt dat we niet meer alleen vanuit ons eigen perspectief naar informatievoorziening kunnen kijken. Het perspectief van de andere betrokkenen is minstens zo belangrijk, als niet belangrijker. We moeten ons kunnen verplaatsen in de burger en hun verwachtingen."

**Overheid hoeft niet voorop te lopen**

Bremer concludeert dat zijn werk altijd ondergeschikt zal zijn aan de mensen in het veld. "Onze 'business' is leidend. Digitalisering en technologische ontwikkelingen blijven uiteraard onmiskenbaar belangrijk voor de Raad voor de Kinderbescherming. Onze systemen moeten altijd werken zodat onze raadsonderzoekers het kind en het gezin op ieder moment kunnen bijstaan. Wij kunnen als overheidsorganisatie nooit harder lopen dan de rest. Dat hoeft ook niet, zolang we onze focus maar scherp houden: de mens staat in ons werk centraal."

01

# Zet uw gebruiker op nummer 1

Hoe verandert u de focus van product naar gebruiker?

**Het succes van een applicatie, website of app wordt voor een belangrijk deel bepaald door de mate van adoptie door de gebruiker. Oftewel: wordt het product naar volle tevredenheid gebruikt en omarmd. Design thinking is een bewezen ontwerpmethodiek waarbij de gebruiker en zijn behoeften centraal staan. Alles draait daarbij om het zo goed mogelijk begrijpen van die gebruiker en de context waarin hij zich bevindt.**

## Highlights

- Design thinking biedt een gestructureerde aanpak om de gebruiker of burger centraal te stellen bij de ontwikkeling van digitale producten en diensten
- Met onderzoek leert u de gebruiker en zijn context kennen. Dit geeft inzicht in de echte gebruikersproblematiek en voorkomt symptoombestrijding
- Voor het oplossen van knelpunten of het maken van keuzes is een ‘gezonde’ afweging nodig tussen de gebruikers- en organisatiebelangen

U zou denken dat design thinking bovenaan het wensenlijst staat van iedere manager die verantwoordelijk is voor een website, applicatie of app. Zeker in overheidsland bij de ontwikkeling van digitale producten en diensten liggen er mogelijkheden om de burger een centrale plek te geven in het ontwerpproces. Ik zie het zelf als een uitgelezen kans om iets te doen aan het verkleinen van de kloof tussen overheid en burger. Gelukkig merk ik dat het gedachtengoed steeds vaker wordt toegepast, al is het nog niet een vanzelfsprekendheid. Zeker bij manier waar de doorlooptijd of het budget in het gedrang is, ziet u helaas te vaak dat de opdrachtgevers in hun oude reflexen schieten en kiezen voor de ‘oude manier’ van werken. In plaats van de kans te pakken, is de beweging vaak terugtrekkend en wordt er een streep door design thinking gezet. Al die mooie beloftes over ‘de gebruiker of de burger centraal stellen’ worden rücksichtslos opzijgeschoven. Vaak ook nog met de opmerking dat het team en de opdrachtgever de gebruiker goed kennen omdat ze al jarenlang aan het product werken. U zou dan toch aannemen dat de gebruikerservaring van het product goed is en dat de gebruiker zich volledig (h)erkent in het product. Het tegendeel is vaak waar.

**Wat is design thinking?**

Design thinking is een ontwerpmethodiek bestaande uit vijf fases waarbij de nadruk ligt op het iteratief en multidisciplinair samenwerken. De fases worden in de meeste situaties stap voor stap doorlopen, maar het is mogelijk om af te wijken. De vijf fases zijn: inleven, definiëren, ideeën genereren, prototype maken en testen. Het eindresultaat is een gevalideerd prototype dat eruitziet en functioneert als het te realiseren product. Oftewel: echte gebruikers hebben in een gebruikerstest, aan de hand van opdracht- en succesvol hun belangrijkste taken in het prototype kunnen uitvoeren.

De activiteiten binnen de vijf fases verschillen sterk per situatie, net als de doorlooptijd en het benodigde budget. U kan dus stellen dat ieder design thinking traject uniek is. Een omschrijving per stap is als bijlage opgenomen. In dit artikel richt ik me op de eerste twee fases: 'Inleven' en 'Definiëren'. Deze twee fases hebben namelijk de grootste impact op het uiteindelijke succes van het product, omdat dit precies de stappen zijn waar de gebruikers- en organisatieperspectieven elkaar overlappen én soms conflicteren. Er moeten dus duidelijke keuzes worden gemaakt.

**Design thinking bij het Centraal Orgaan opvang Asielzoekers (COA)**

Met dit praktijkvoorbeeld laat ik zien hoe design thinking in de praktijk leidt tot betere oplossingen, waarmee u zowel het gebruikersgemak verbetert als de organisatiedoelen verwezenlijkt. Het voorbeeld betreft het herontwerp van de incidentregistratie bij het COA.

Net als bij een gezin thuis, vinden er bij de opvang van asielzoekers op een AZC gebeurtenissen plaats die ingaan tegen de huisregels. Zo is het niet toegestaan om op de kamer te roken en u mag ook niet moedwillig een bord of ander voorwerp kapot maken. Ook kan er sprake zijn van een vechtpartij tussen twee of meerdere asielzoekers. Al deze gebeurtenissen worden vastgelegd in een informatiesysteem.

Het COA streeft ernaar om de vastlegging van incidenten landelijk meer te standaardiseren en om een kwaliteitsimpuls te geven aan de onderbouwing. Dit moet het slagingspercentage van zaken die bij de rechter voorkomen verhogen. Daarnaast moet onderzocht worden of de kwaliteit van de rapportages aan het ministerie

verder aangescherpt kan worden. Deze twee punten waren de directe aanleiding voor het herontwerp. Dit keer echter met design thinking als ontwerpmethodiek. De keuze voor design thinking sloot hierbij mooi aan bij de behoefte van het COA om haar medewerkers een belangrijkere rol in het proces van de totstandkoming van een ICT-product te laten spelen.

Met de doelen vanuit de organisatie in ons achterhoofd ging ik samen met een collega aan de slag met de eerste fase: het 'inleven'. Wat is het probleem achter het probleem? Welke behoeften leven er bij de medewerkers en waar lopen ze zoal tegenaan. We startten met een bezoek aan drie verschillende opvanglocaties. Waarbij we veel tijd inruimden voor het afnemen van interviews en het doen van observaties. We keken over de schouder mee hoe medewerkers een tweetal voorbeeld incidenten in het informatiesysteem vastlegden. Dit veldwerk leverden ons veel inzichten op voor de tweede fase: het 'definiëren'. In die fase identificeerden wij vier belangrijke knelpunten. Per knelpunt geef ik hieronder aan hoe deze later in het ontwerptraject is opgelost. Tot slot ga ik ook in op het resultaat van de verandering voor de gebruiker én de organisatie:

1. **Alle type incidenten worden in het huidige informatiesysteem op eenzelfde manier afgehandeld ongeacht complexiteit of impact. Daarbij blijkt dat er voor bepaalde kleine veelvoorkomende type incidenten met een vaste afhandeling veel tijd nodig is, tot wel 15 minuten per gebeurtenis. Voorbeelden hiervan zijn: roken op de kamer en het afplakken van de brandmelder.**
   De voorgedragen oplossing: het maken van een onderscheid tussen incidenten en generieke gebeurtenissen. Hierdoor wordt het mogelijk om de generieke gebeurtenissen te voorzien van vooraf ingevulde teksten. De medewerker moet aan het begin van het registratieproces allereerst de keuze maken tussen een incident of een generieke gebeurtenis, daarna hoeft hij bij de generieke gebeurtenissen alleen de informatie te controleren en eventuele bijzonderheden toe te voegen. De tijdbesparing voor de medewerker is ruim 10 minuten per incident. Omdat de teksten centraal worden beheerd, ontstaat er ook meer uniformiteit in de verslaglegging. De medewerker is minder tijd kwijt, terwijl de vastlegging meer gestandaardiseerd is.
2. **De registratie van het incident gebeurt in de huidige applicatie over meerdere tabbladen. Op het eerste tabblad worden de betrokkenen vastgelegd en op het tweede tabblad wordt het incident feitelijk beschreven. Het nadeel van deze opzet is dat bij het controleren van de namen de medewerker steeds tussen de twee tabbladen heen-en-weer moet springen. Omdat dit niet handig werkt maken de medewerkers bovenaan het verslag eerst een eigen legenda aan met de namen van alle betrokkenen. De keerzijde is dat dit dubbelwerk is en fouten in de hand werkt. Daarnaast wil het COA in verband met de AVG-richtlijnen geen namen van betrokkenen in het verslag hebben staan. De richtlijn is om aliasnamen te gebruiken.**
   De voorgedragen oplossing: in de nieuwe opzet is het vastleggen van de betrokkenen verhuisd naar het tweede tabblad bij het verslag. De medewerker heeft nu in één oogopslag zowel het verslag als alle betrokkenen inclusief hun aliasnaam in beeld. Het zelf opmaken van een legenda is daardoor niet meer nodig. Ook vindt er tijdens het opslaan van het incident een extra AVG-controle plaats.
   Met deze eenvoudige aanpassing wordt een frustratie bij de medewerkers weggenomen en een belangrijke organisatiedoelstelling met betrekking tot het naleven van de AVG-richtlijnen behaald.
3. **Het is soms een uitdaging om een goed en feitelijk verslag te schrijven. Uit de interviews bleek dat medewerkers het vaak lastig vinden om een begin te maken met het schrijven van het verslag.**
   De voorgedragen oplossing: in de nieuwe opzet wordt onder het verslag een lijst met hulpzinnen getoond. De medewerker kan deze hulpzinnen met één muisklik in het verslag plaatsen. De hulpzinnen bieden de medewerker een handvat en het bespaart ze ook tijd. De hulpzinnen verschillen per type incident en worden centraal beheerd. De hulpzinnen ondersteunen de medewerker met de aanzet van het schrijven van het verslag waarbij tegelijkertijd de vastlegging van een incident meer gestandaardiseerd wordt.
4. **Bij het opvoeren van een incident is het in het huidige informatiesysteem mogelijk om een vinkje te zetten bij het selectievak met het label 'Aangifte'. Uit de gesprekken met de medewerkers bleek als snel dat dit heel verschillend geïnterpreteerd werd. De één ging ervanuit dat de aangifte daadwerkelijk was gedaan, terwijl een ander aangaf dat de betrokkene van plan was om aangifte te gaan doen.**
   Het vinkje heeft invloed op de rapportage over het aantal aangiftes dat per tijdvak is gedaan. De voorgedragen oplossing: door het label 'Aangifte' simpel te hernoemen naar 'Aangifte gedaan' is het voor alle medewerkers meteen helder wanneer het vinkje gezet moeten worden. Dit werd bevestigd in de gebruikerstest met een 100% score.
   Met deze op het oog simpele aanpassing wordt een onduidelijkheid weggenomen en gaat de betrouwbaarheid van de rapportage omhoog.

Met het voorbeeld van het COA wil ik aantonen, dat door u te verdiepen in de gebruiker en zijn context, u het probleem achter het probleem beter kunt duiden. Dit voorkomt een ad hoc oplossing en symptoombestrijding. Omdat design thinking uitgaat van het actief betrekken van de gebruiker in het ontwerpproces, resulteert dit in betere ontwerpbesluiten die organisaties aantoonbaar verder helpen. Zelfs een ogenschijnlijk kleine aanpassing kan een positieve impact hebben op de organisatiedoelstelling(en).

Design thinking is zeker geen wondermiddel, maar de ontwerpmethode geeft organisaties wel beter inzicht in de op te lossen uitdaging(en) met de daarbij behorende belangen. Maakt u zich daarbij geen zorgen dat de focus te veel neigt naar de gebruiker, want als u het makkelijk maakt voor de gebruiker dan maakt u het uiteindelijk ook makkelijk voor uzelf als organisatie.

De design thinking fases op een rij:

- In fase 1 wordt er ingezoomd op het probleem en gekeken voor wie de oplossing bedoeld is. Wat zijn hun behoeftes, verwachtingen en wat is de impact van de context op het product? Daarnaast is het belangrijk om de vraag van de opdrachtgever goed te duiden. Wat wil de organisatie bereiken en waarom?
- In fase 2 stelt u aan de hand van de bevindingen uit fase 1 de werkelijke probleemstelling vast. Dit zorgt ervoor dat er niet aan symptoombestrijding wordt gedaan en dat het echte gebruikersprobleem voorop komt te staan. Tot slot moet er een balans worden gevonden tussen de gebruikers- en organisatiebehoeftes en dat alles binnen het technisch kader en met inachtneming van alle geformuleerde kwaliteitseisen.
- Fase 3 richt zich op het bedenken van ideeën voor de verschillende problemen.
- In fase 4 wordt uit de verzameling van ideeën één totaaloplossing gecreëerd en wordt deze verder uitgewerkt tot een prototype dat geschikt is voor de gebruikerstest in fase 5.
- In fase 5 wordt het prototype voorgelegd aan minimaal zes gebruikers van het te ontwikkelen product. Het doel is om te valideren of het prototype voldoet en te ontdekken waar nog aanpassingen nodig zijn.

## Over de auteur

**Arno van der Hulst**
Design Director en
gamification specialist

Arno van der Hulst is met name werkzaam binnen het overheidsdomein. De focus van zijn werkzaamheden ligt bij het betrekken van de gebruiker in het ontwikkelingsproces van diensten en producten.

arno.vander.hulst@capgemini.com

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

02

# Ben jij het wel EGGIE? Oplossingen zijn nodig om nep van echt te onderscheiden

## Welke rol speelt een burgergerichte aanpak in het bestrijden van impersonatie?

**Impersonatie is een groeiend probleem. Een aanpak waarin de burger centraal staat is nodig om effectieve oplossingen te ontwikkelen.**

## Highlights

- Oplichting door impersonatie is een groeiend probleem
- Explosieve toename van nepagenten heeft grote impact op slachtoffers en de maatschappij
- De burger centraal stellen in oplossingen tegen impersonatie en oplichting



"Papa, ik ben mijn telefoon kwijt, dit is mijn nieuwe nummer." "Goedemiddag, met de Rabobank. Ik bel over een verdachte transactie op uw rekening." Deze scripts zijn bekend van WhatsApp- en bankhelpdeskfraude. Ondanks waarschuwingen via verschillende voorlichtingscampagnes van de overheid neemt fraude toe. In 2024 werden 1,4 miljoen personen slachtoffer van online oplichting en fraude[1]. Criminelen gebruiken steeds slimmere social engineering technieken, versterkt door de nieuwste technologieën zoals Generatieve Artificiële Intelligentie (GenAI). Deze criminaliteit gaat verder dan het online domein. Stelt u voor: u wordt gebeld door iemand die zich voordoet als uw wijkagent en zegt dat uw huis doelwit is van een inbraak. Voordat u het gesprek beëindigt staat er al een 'collega', in iets dat lijkt op een uniform, aan de deur. Hoe weet u zeker dat deze persoon echt een politieagent is? Dit blijkt lastig, vooral voor kwetsbare ouderen als meest voorkomende doelwit. In 2024 registreerde de politie 8329 incidenten met nepagenten, vijftien keer zoveel als in 2023[2]. Van 1600 burgers is bekend dat zij in 2024 slachtoffer waren en dit aantal neemt verder toe[3].

Nepagenten hebben een aanzienlijke impact op zowel de burger als de politie. Ze ondermijnen het vertrouwen van burgers in instanties en diensten en veroorzaken een gevoel van onveiligheid. Oplichting door nepagenten heeft niet alleen financiële, maar ook emotionele en psychische gevolgen voor slachtoffers. Daarnaast legt de toename van incidenten met nepagenten extra druk op de politie. Dit leidt ertoe dat de politie meer tijd en middelen moet besteden aan onderzoeken en de verwerking van aangiftes. Bovendien lijdt het imago van en het vertrouwen in de politie eronder, wat het contact met burgers verstoort en de effectiviteit van het politiewerk raakt. Volgens het Openbaar Ministerie heeft deze vorm van criminaliteit een 'maatschappij-ontwrichtend karakter'[4]. Vanwege deze gevolgen wordt het dan ook onder 'high impact crimes' geschaard[5].

Om oplichting en de gevolgen daarvan aan te pakken zet de politie zich al in op het weerbaarder maken van de samenleving. Dit gebeurt met initiatieven waarbij de burger centraal wordt gesteld bij het ontwikkelen van een oplossing, zoals de nepwebshop (pakjedeals.nu). Hierbij werden gebruikers met scherpe prijzen gelokt om artikelen te kopen, om vervolgens de gebruiker te wijzen op het feit dat de webshop niet legitiem is. Om de gebruiker weerbaarder te maken wordt uitgelegd hoe zij in het vervolg een nepwebshop kan herkennen. Een ander initiatief van de politie is "Check je hack", waarbij de politie burgers helpt om te controleren of hun e-mailadres en daaraan gekoppelde data voorkomt in datasets die door criminelen worden verhandeld.

Bovenstaande initiatieven zijn voorbeelden die geïnitieerd zijn om burgers meer bewust te maken van oplichting en zich weerbaarder te maken voor de wereld van vandaag. In de wereld van morgen wordt impersonatie, waarbij criminelen zich voordoen als iemand anders, steeds makkelijker door imitatie van gezichten en stemmen via GenAI. Kan de burger dan nog nep van echt onderscheiden en is bewustwording dan voldoende? Het is essentieel om meer te doen vanuit het perspectief van de burger om dit toenemende probleem aan te pakken en zo de burger beter te kunnen ondersteunen.

Om het probleem van impersonatie te benaderen en de druk bij de politie te verminderen, moet de overheid meer doen dan bewustwording creëren. Het is essentieel om hulpmiddelen te ontwikkelen die burgers in staat stellen zelf impersonatie te herkennen en direct zelf actie te ondernemen. Burgers zouden onomstotelijk moeten kunnen verifiëren of iemand is wie hij zegt dat hij is. Als voorbeeld hiervan hebben wij een oplossing bedacht die we EGGIE noemen. Een oplossing die verschilt van de eerdergenoemde initiatieven doordat het de burger (nog) meer centraal zet en een praktisch hulpmiddel biedt om oplichting te voorkomen. Om te komen tot een dergelijke oplossing is een burgergerichte aanpak van groot belang.

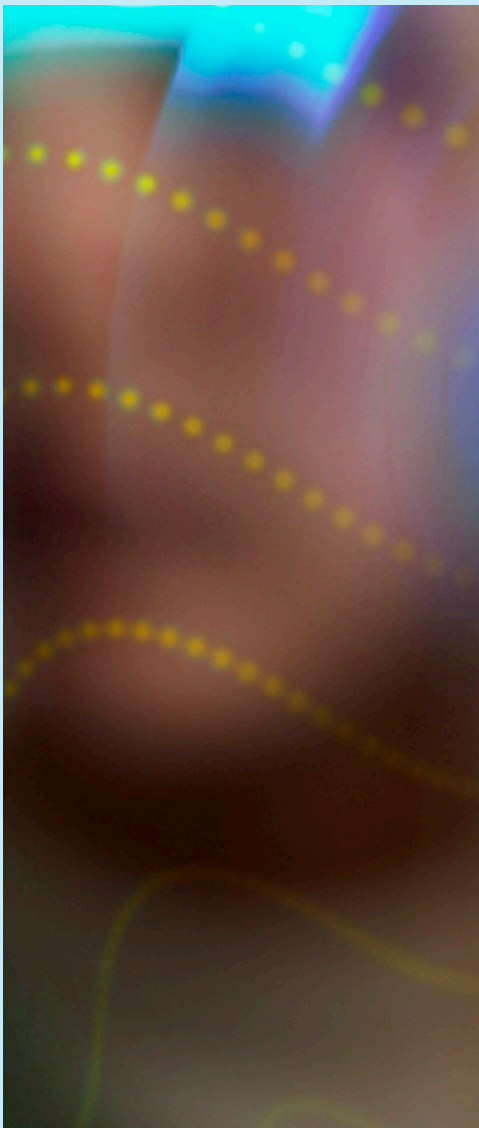
Maar eerst leggen wij de werking van het voorbeeld EGGIE uit: een te verifiëren persoon, bijvoorbeeld een politieagent, geeft een code met een beperkte geldigheidsduur aan de burger. Deze code kan door de burger digitaal worden gecontroleerd om na te gaan of er inderdaad op dat tijdstip een code is gegenereerd door de betreffende persoon.

Mocht dit niet het geval zijn en er is sprake van een verdachte situatie dan kan de burger direct melding hiervan maken en daarnaast zelf actie ondernemen door bijvoorbeeld het gesprek te beëindigen. Data van deze door burgers uitgevoerde controles en meldingen kunnen door de politie worden geanalyseerd met hulp van GenAI. Dit geeft een meer compleet beeld over waar, wanneer en hoe criminelen handelen. De politie kan hierop acteren wat bijdraagt aan een grotere pakkans, preventie en een daling van oplichtingsgevallen. Naast visuele controles, zoals het uniform en de politiepas in het geval van een agent, helpt de verificatie met EGGIE om echte agenten van nepagenten te onderscheiden. Met EGGIE heeft de burger hierdoor een extra hulpmiddel, initiatief en controle, wat hen vertrouwen en houvast geeft in situaties die als onveilig worden ervaren.

Nu u weet hoe onze concept-oplossing EGGIE werkt, nemen we u mee in een drietal principes die zijn gehanteerd om de burger centraal te stellen. Deze principes vormen altijd de basis voor het ontwikkelen van effectieve oplossingen om vanuit het perspectief van de burger te denken en beredeneren. Ze zijn dus ook essentieel voor oplossingen tegen oplichting, zoals het toenemende probleem van impersonatie.

**Om effectieve oplossingen te ontwikkelen, moet de overheid burgers centraal stellen bij het vaststellen van problemen en het ontwerpen van oplossingen.** Dit vereist een outside-in benadering, waarbij niet wordt gedacht vanuit regels en interne processen, maar vanuit de actuele behoeften en ervaringen van burgers. Publieke organisaties zoals de politie spelen een cruciale rol in het versterken van het vertrouwen van burgers door betrouwbare dienstverlening aan te bieden. Een aanpak waarbij de burger op de eerste plaats wordt gezet, zorgt voor werkbare oplossingen die passen bij de behoeften van burgers en, waar mogelijk, aansluiten op wat zij al kennen en vertrouwen. Gebruik bijvoorbeeld bestaande en bewezen technieken die burgers herkennen om acceptatie en gebruik te vergemakkelijken. Zo is de verificatiemethode van EGGIE vergelijkbaar met two-factor authentication (2FA), een veelvoorkomende en dus herkenbare methode.

**Het betrekken van burgers bij de ontwikkeling en implementatie van oplossingen is cruciaal.** Door samen te werken kan een oplossing worden afgestemd op de werkelijke behoeften van de gebruikers, wat de adoptie en effectiviteit van een oplossing vergroot. Samenwerking met de burger levert waardevolle input op. Het is bijvoorbeeld belangrijk om te begrijpen hoe burgers technologie willen gebruiken en hoe het voor hen kan werken. In het geval van EGGIE kan bijvoorbeeld het automatisch activeren van de camera om beeldopnamen te maken ongetwijfeld realiseerbaar en interessant zijn voor de politie, maar is de burger er ook mee geholpen? In interviews en testscenario's rondom EGGIE geven burgers aan dat ze zich hierdoor juist onveilig zouden voelen. Oplossingen moeten niet alleen technisch goed functioneren, maar ze moeten vooral ook praktisch en bruikbaar zijn voor burgers in het dagelijks leven. Dit benadrukt het belang van het vinden van de juiste balans tussen veiligheid, privacy en gebruiksvriendelijkheid. Een onveilige oplossing leidt tot een vertrouwensbreuk, terwijl een niet gebruiksvriendelijke oplossing tot gefaalde adoptie leidt. Deze balans kan alleen samen met de burger worden gevonden.



## Bronen

1. Online oplichting en fraude | CBS
2. Forse stijging incidenten met nepagenten in 2024 | politie.nl
3. Oplichting van ouderen door nepagenten explosief toegenomen: 'Ze zijn nietsontziend'
4. OM eist gevangenisstraffen tegen verdachten die nepagenten aanstuurden: 'Dit raakt de kern van ons rechtssysteem' | Nieuwsbericht | Openbaar Ministerie
5. Kamervragen (Aanhangsel) 2024-2025, nr. 786 | Overheid.nl > Officiële bekendmakingen

Burger centraal

**Ontwikkel oplossingen die eenvoudig te begrijpen en gebruiken zijn, en die herbruikbaar zijn in verschillende contexten.** Dit vermindert complexiteit en verhoogt de efficiëntie. Het uitgangspunt van EGGIE is om een veelzijdige totaaloplossing te bieden tegen alle soorten babbeltrucs en situaties, zowel fysiek, telefonisch als digitaal. De oplossing moet breed inzetbaar zijn voor verschillende gebruikers, zoals agenten, bankmedewerkers, monteurs en collectanten. Door een herbruikbare en schaalbare oplossing in te zetten wordt voorkomen dat burgers met verschillende werkwijzen worden geconfronteerd. Herkenning en eenvoud vergroten het gebruiksgemak, wat bijdraagt aan een succesvolle oplossing. Daarnaast zijn eenvoudige en herbruikbare oplossingen cruciaal voor een efficiënte overheid. Hergebruik van oplossingen verkort de ontwikkeltijd en stelt de overheid in staat sneller in te spelen op de actualiteit en behoeften van de samenleving.

Uit het voorbeeld van EGGIE blijkt hoe het centraal stellen van en samenwerken met de burger kan leiden tot een effectieve oplossing tegen impersonatie. In een wereld waarin technologie ervoor zorgt dat de grens tussen nep en echt steeds minder duidelijk wordt, zijn nu oplossingen nodig waarin identiteit en authenticiteit onomstotelijk kan worden vastgesteld. Met initiatieven die gericht zijn op de burger, kunnen we een toekomst creëren waarin burgers beter beschermd zijn tegen oplichting, en waarin het vertrouwen in instanties en diensten wordt hersteld. Het is een gezamenlijke inspanning die vraagt om innovatie, samenwerking en een voortdurende focus op de behoeften van de samenleving.

## Over de auteurs

**Casper Lubbers**
**Senior Consultant / Business Analist**

Als Business Analist binnen het veiligheidsdomein, waaronder OM en Politie, zorgt Casper ervoor dat oplossingen effectief en efficiënt worden ontwikkeld en positief impact maken op complexe bedrijfsprocessen. Mede-initiatiefnemer van het concept EGGIE als potentiële oplossing voor het probleem van impersonatie.

casper.lubbers@capgemini.com
https://www.linkedin.com/in/casper-lubbers-73a272159/

**Eefje van Tongeren**
**Managing Consultant / Business Analist**

Eefje is een ervaren consultant.
De afgelopen jaren werkte zij voor overheidsorganisaties. Zij legt de aandacht op burgergerichte dienstverlening. Zij is mede-initiatiefnemer van het concept EGGIE als potentiële oplossing voor het probleem van impersonatie.

eefje.van.tongeren@capgemini.com
https://www.linkedin.com/in/eefje-van-tongeren-7a8a7692/

# Toekomst van werk

Interview:

# De toekomst van werk: wendbaar blauw

De toekomst van werk binnen de politie vraagt om fundamentele veranderingen, zowel in het operationele veld, als in de manier waarop mensen worden ondersteund vanuit de bedrijfsvoering. Flexibiliteit, eenvoud en datagedreven sturing zijn dé voorwaarden om medewerkers optimaal te faciliteren. “Onze bedrijfsvoering zal steeds meer bepalen hoe wendbaar en toekomstgericht we kunnen opereren.”

## Janet de Vries

Programma Directeur Vernieuwing ICT bedrijfsvoering bij de Politie.

“We leven echt in een andere context dan voorheen,” stelt Janet de Vries, Programmadirecteur Modernisering Informatievoorziening Bedrijfsvoering (MIB) bij de Politie. “Of het nu klimaatdemonstraties zijn of supportersrellen, de grilligheid neemt toe. We moeten ons voortdurend opnieuw verhouden tot de wereld om ons heen. Die onzekerheid heeft directe gevolgen voor de manier waarop ons werk wordt georganiseerd. Dit vraagt wendbaarheid, maar ook nieuwe keuzes.”

### Driehoek van mens, omgeving en technologie

Het programma MIB moderniseert de bedrijfsvoeringsystemen en optimaliseert de integraties en verbindingen tussen deze systemen. De Vries: “Onze taak is om de bedrijfsvoeringsprocessen maximaal te faciliteren zodat onze mensen hun werk sneller, efficiënter en effectiever kunnen uitvoeren.”

Bedrijfsvoering moet volgens De Vries dan ook gericht zijn op het faciliteren van continue verandering in de organisatie. “Als we nadenken over de politie van de toekomst, dan kijk ik naar een goede balans tussen collega, omgeving en de invloed van technologie. Deze zijn altijd met elkaar verweven. Het implementeren van nieuwe informatiesystemen is geen doel op zich. Technologie speelt een sleutelrol, maar moet altijd bekeken worden in relatie tot de impact op mens, organisatie en omgeving.
Een van de manieren waarop we wendbaarder worden, is door processen te standaardiseren, automatiseren en/of te robotiseren. Dit bespaart direct tijd, waardoor medewerkers zich kunnen richten op betekenisvoller werk. We zetten hier goede stappen in, maar de uitdaging ligt in het duurzaam integreren van deze digitalisering in onze bedrijfsvoering.”

### Naar structurele implementatie

Die stap naar duurzame integratie is complex, merkt ze. “Het is veel makkelijker om een instrumentele verandering door te voeren dan een structurele cultuurverandering. Het automatiseren en robotiseren kan bijvoorbeeld uren vrijspelen, maar hoe we die uren vervolgens efficiënt inzetten, is een organisatievraagstuk. Dit raakt direct aan de kern van onze toekomstbestendige bedrijfsvoering. We moeten niet alleen nieuwe technologieën adopteren, maar ook nadenken over hoe ze invloed hebben op processen en mensen. En hiervoor nieuwe (werk)concepten introduceren. De impact op ons gedrag en de manier waarop wij werken, wordt nog wel eens onderschat. Het vervangen van de bedrijfsvoeringssystemen is een grote en complexe operatie. Alles hangt met elkaar samen en is afhankelijk van elkaar. Daardoor kan het langer duren voordat de collega’s iets van de verbeteringen gaan merken. En het vernieuwen gebeurt allemaal terwijl de winkel openblijft.”

### De grote transitie

Een van de grootste transities voor de bedrijfsvoering binnen de Politie ligt in de modernisering van informatietechnologie, zegt De Vries. “We hebben grote ambities: we willen als organisatie wendbaarder zijn, slimmer werken en sneller handelen. Dat raakt essentiële processen zoals capaciteitsmanagement, HR, financieel, logistiek en inkoop. Als programma MIB moeten we daarvoor een

stevig, toekomstbestendig fundament leggen, en dat fundament betekent: vernieuwing en vervanging van onze informatiesystemen."

Om de volledige potentie van nieuwe technologieën te benutten, moeten onderliggende processen worden gestandaardiseerd en geharmoniseerd. "Dat betekent ook minder maatwerk en meer gebruik van bestaande oplossingen uit de markt. Dat zal eerst wellicht wat pijn doen, omdat het een forse investering vraagt voordat we er de vruchten van plukken: het betekent een andere manier van werken. Dat kan uiteraard even wennen zijn voor onze collega's: ze zullen oude patronen moeten loslaten. De nieuwe informatiesystemen werken echter slimmer, makkelijker en sneller. Andere voordelen zijn dat we toegang hebben tot de laatste state-of-the-art-technieken, de gebruikerservaring van andere organisaties beter kunnen benutten waarmee we onze informatiesystemen continu kunnen optimaliseren, en uiteraard minder zorgen zullen hebben over het onderhoud en toekomstbestendigheid van het systeem."

**Veranderingen die de operatie ondersteunen**

Processen zullen ook sterk vereenvoudigen en begrijpelijker worden voor de gebruiker. De Vries geeft een voorbeeld: "Op dit moment kennen we circa honderd verschillende aanvraagprocessen, die inhoudelijk vaak slechts minimaal van elkaar verschillen. Elk type aanvraag, van een uniform tot een bos bloemen, kent verschillende variaties en moet je met behulp van verschillende systemen indienen. Dit versnipperde landschap zorgt voor onnodige complexiteit en beperkt onze wendbaarheid. Door deze processen te standaardiseren tot een uniforme aanvraagstructuur, waarbij de uitkomst kan verschillen maar het basisproces gelijk blijft, vergroten we het gebruikersgemak aanzienlijk. Medewerkers hoeven niet langer te navigeren tussen verschillende loketten, maar kunnen via een eenduidige bestelprocedure hun aanvraag indienen. Deze loketfunctie-gedachte maakt het bestelproces simpeler, efficiënter en legt de nadruk waar die hoort: op het faciliteren van onze medewerkers."

**Ze vervolgt:** "We willen onze administratieve processen ook vereenvoudigen: ziekmelden, declaraties, reserveringen, contracten, kledingpakketten - alles moet sneller en makkelijker geregeld kunnen worden. Onze capaciteitsplanning is een ander voorbeeld. Inmiddels zijn we bezig met het implementeren van een nieuw capaciteitsmanagementsysteem. Met deze vernieuwing kunnen eenheden beter onderling afstemmen, plannen en personeel efficiënter inzetten. Dat geeft inzicht, overzicht en maakt flexibeler plannen mogelijk. En door 'samenroosteren' via nieuwe tools krijgen collega's ook nog eens meer invloed op hun werk/privébalans. Samenroosteren houdt in dat collega's zelf intekenen op de diensten die ze willen draaien. Die stemmen ze samen af zodat alle diensten eerlijk gevuld worden. Zo hebben ze zelf meer invloed op wanneer ze werken en wanneer ze vrij zijn. Dit biedt meer flexibiliteit en het ruilen van diensten wordt makkelijker. De techniek maakt het mogelijk dat medewerkers dit straks dus zelf kunnen, heel eenvoudig met een app op hun telefoon."

**Meer regie en juiste tooling**

Daarnaast ziet ze, mede door een veranderende samenstelling van het personeelsbestand, minder functievastheid. "We zullen toegroeien naar een organisatie waarin de opgaven centraal komen te staan, niet zozeer de functies. Dat vraagt vanuit bedrijfsvoering ook om een andere ondersteuning van onze organisatie. Onze medewerkers worden steeds meer ingezet op basis van hun ambities en expertises, en moeten in staat worden gesteld om nieuwe rollen op te pakken. Dan is een continu inzicht in hun competenties, wensen en ambities onmisbaar. Met die informatie kunnen we onze mensen beter begeleiden bij hun ontwikkeling. Dat vraagt om nieuwe informatiesystemen die dit inzicht bieden en de ontwikkelingen van onze mensen in de volle breedte kunnen ondersteunen."

Zover is het op dit moment nog niet, zegt De Vries. "Ons huidige ICT-landschap ondersteunt nu nog onvoldoende dat mensen zelf de regie kunnen nemen over hun inzet en loopbaan: informatiesystemen zijn niet flexibel en nog niet ingericht als logische flows. De toekomst van werk vereist dat medewerkers hun eigen keuzes kunnen maken, dat die keuzes transparant zijn en ze de benodigde administratie eenvoudig kunnen bijhouden. Ons MIB-programma ondersteunt deze transitie: zo dragen we bij aan de bredere medewerkerstevredenheid."

**Datagedreven organisatie**

De harde scheiding tussen operationele en ondersteunende processen zal bovendien steeds meer vervagen door slim gebruik van data en technologie, meent De Vries. "Technologie helpt ons om een toekomstbestendige organisatie neer te zetten die onze operatie zo goed mogelijk ondersteunt. Data is daarvoor van onschatbare waarde. Als we onze processen en informatiesystemen goed inrichten, kunnen we optimaal datagedreven werken en betere strategische beslissingen nemen. Onze bedrijfsvoering is ons fundament. Geen politieagent kan de straat op zonder een goed functionerende bedrijfsvoeringsorganisatie."

Ze licht toe: "Kijk bijvoorbeeld naar de manier van opsporen en handhaven: die verandert in rap tempo door de enorme hoeveelheid informatie en data. Op basis van data ter plaatse moeten onze mensen een vertaling kunnen maken naar de juiste interventies. Datzelfde geldt ook voor de bedrijfsvoeringsdata die beter ingezet kan worden in besluitvormingsprocessen of in het maken van de juiste beleidskeuzes."

**De bedrijfsvoering van de toekomst**

Door te investeren in die toekomstgerichte, datagedreven en flexibelere bedrijfsvoering kan de politie zich krachtiger voorbereiden op de uitdagingen van morgen, concludeert De Vries. "Politie blijft mensenwerk, maar de manier waarop we het werk organiseren en ondersteunen, verandert fundamenteel. Ik zie bedrijfsvoering dan ook als een dynamisch systeem dat niet alleen processen ondersteunt, maar actief meebeweegt met de ontwikkeling van onze mensen en de eisen van de samenleving. Dat vraagt om nieuwe technologie, maar vooral om een andere mindset: flexibeler, wendbaarder, en veel meer gericht op het faciliteren van continue verandering. Dat is onze taak."

03

# GenAI in HR: Optimalisatie of ontwrichting in de veiligheidssector?

## Is de impact van GenAI op HR een kans of bedreiging voor veiligheidsorganisaties?

**GenAI verandert de toekomst van werk razendsnel. Maar hoe? Ontdek de kansen van GenAI in HR, en hoe u technologie slim inzet voor succes.**

### Highlights

- Toekomst van werk verandert in een razend tempo
- GenAI biedt hierbij kansen, maar ook uitdagingen
- HR-proces moet proactief inspelen op ontwikkelingen
- GenAI krijgt een rol in personeelsplanning en talentmanagement
- Technologie en talent gaan hand in hand

De mogelijkheden van generatieve AI (GenAI) blijven zich razendsnel ontwikkelen. Voor veiligheidsorganisaties betekent dit enerzijds een kans om processen te optimaliseren en strategischer te werken, en anderzijds een uitdaging: medewerkers moeten veilig, vaardig en bewust leren omgaan met deze technologie. Gezien de grote hoeveelheid vertrouwelijke gegevens waar veiligheidsorganisaties dagelijks mee werken, is het essentieel dat gebruikers van GenAI geen onnodige risico's nemen. Dit vraagt dan ook om een strategische aanpak die verder gaat dan traditioneel HR, met een visie waarin technologie en talent naadloos op elkaar aansluiten.

**De dubbelrol van GenAI: een onmisbare kans en onzichtbare uitdaging**

Volgens het "Future of Jobs Report" van het World Economic Forum (2025) moeten medewerkers als gevolg van technologische ontwikkelingen gemiddeld 39% van hun huidige vaardigheden vervangen of uitbreiden in de komende vijf jaar. GenAI staat samen met big data bovenaan de lijst van snelgroeiende vaardigheden, gevolgd door netwerk- en cybersecurity. Het is dan ook evident dat GenAI niet langer een optie is, maar de realiteit. Door de impact van deze ontwikkelingen op het dagelijkse werk is up- en reskilling van medewerkers cruciaal om enerzijds GenAI als kans te benutten, maar ook de uitdagingen en mogelijke risico's van het gebruik van GenAI te mitigeren. Een voorbeeld van een risico is dat medewerkers de GenAI-tool (onopzettelijk) toegang geven tot gevoelige informatie van slachtoffers, getuigen en verdachten. De gevolgen hiervan kunnen verstrekkend zijn: criminelen kunnen deze data gebruiken om waardevolle slachtofferprofielen op te stellen die kunnen worden ingezet voor verschillende vormen van criminaliteit (Openbaar Ministerie & Politie, 2024).

Voor HR-teams zijn de kansen en uitdagingen die GenAI biedt niet anders. In Trends in Veiligheid: Society 5.0 (Capgemini, 2024) wordt een situatie in het veiligheidsdomein beschreven met HR-implicaties: de toenemende interesse in het Dienjaar Defensie. Dit vraagt van Defensie dat zij zich voorbereiden op een groot aantal militairen die een relatief korte opleiding krijgen en mogelijk maar een jaar in actieve dienst blijven. GenAI kan bijdragen aan het sneller en effectiever ontwikkelen van nieuwe medewerkers door gebruik te maken van algoritmen die patronen herkennen in vaardigheden, prestaties en groeipotentieel. Dit vertaalt zich in gepersonaliseerde trainingsprogramma's die inspelen op de specifieke behoeften van medewerkers, evenals een integratie

in wervingsprocessen die sneller en efficiënter verlopen door AI-gestuurde analyses van kandidaatprofielen. Het optimaliseren van deze processen met behulp van GenAI stelt HR-teams binnen Defensie in staat om hun tijd en middelen effectiever in te zetten en biedt ruimte om strategisch vooruit te kijken.

Wat daar dus wel tegenover staat is dat er op verantwoorde wijze om wordt gegaan met deze GenAI tools. Hiervoor moeten dan ook de volgende vragen beantwoord worden: hoe werft u medewerkers met kennis of affiniteit met GenAI die een rol kunnen spelen in de (door)ontwikkeling van deze tools? En hoe zorgt u ervoor dat zittende medewerkers op een verantwoorde manier met deze technologie omgaan? Het is van groot belang dat organisaties niet alleen focussen op het aanleren van technische vaardigheden, maar ook op het creëren van een cultuur waarin medewerkers zich bewust zijn van de ethische en veiligheidsaspecten van GenAI. Trainingen en workshops kunnen helpen om medewerkers te informeren over de risico's en verantwoordelijkheden die gepaard gaan met het gebruik van deze technologie. Dit versterkt niet alleen de competenties van het personeel, maar bevordert ook een proactieve benadering van de uitdagingen die GenAI met zich meebrengt.

### Strategische personeelsplanning 2.0 met behulp van GenAI

Strategische Personeelsplanning (SPP) is het proces waarmee organisaties anticiperen op toekomstige personeelsbehoeften en -uitdagingen om hun strategische doelen te kunnen bereiken. Door toekomstige personeelsbehoeften te voorspellen en hierop te anticiperen, zorgt SPP ervoor dat de juiste mensen met de juiste vaardigheden op het juiste moment op de juiste plek aanwezig zijn. GenAI biedt krachtige kansen om het SPP-proces sneller en nauwkeuriger te doorlopen door processen te automatiseren en voorspellende analyses uit te voeren.

Een voorbeeld hiervan is het gebruik van GenAI in fase 0 van het SPP-proces, waarin een taxonomie wordt opgesteld op basis van bestaande functieprofielen. Door deze profielen direct in te laden in een GenAI-tool kan in korte tijd een uitgebreide taxonomie worden gegenereerd. Dit versnelt niet alleen het proces, maar zorgt ook voor een hogere nauwkeurigheid en consistentie. Bovendien biedt deze aanpak organisaties de mogelijkheid om snel inzicht te krijgen in de vaardigheden en competenties die beschikbaar zijn binnen het personeelsbestand, wat onderdeel is van fase 2 van het SPP-proces (analyse huidige formatie en bezetting).

Een ander voorbeeld komt kijken bij fase 1 van het SPP-proces, waarin de toekomstige personeelssamenstelling wordt bepaald. Door historische gegevens, huidige omgevingsfactoren en ontwikkelingen op gebied van bijvoorbeeld technologie en demografie te analyseren over personeelsverloop, wervingsprocessen en prestatiebeoordelingen, kan GenAI voorspellende scenario's ontwikkelen die de toekomstige situatie schetsen. Deze scenario's kunnen onder andere de impact van seizoensgebonden fluctuaties in de vraag naar personeel op kaart brengen, evenals veranderingen in de arbeidsmarkt die van invloed kunnen zijn op de beschikbaarheid van talent.

Organisaties dienen zich binnen het SPP-proces bewust te zijn van de mogelijke risico's die gepaard kunnen gaan met het verzamelen en analyseren van gegevens ten behoeve van voorspellende analyses. Cyberaanvallen en ongeautoriseerde toegang zijn reële bedreigingen, en als vertrouwelijke informatie -zoals historische gegevens en interne visiestukken- in verkeerde handen vallen, kan dit ernstige gevolgen hebben. Deze risico's dienen dan ook te worden gemitigeerd door


Afbeelding 1. Proces strategische personeelsplanning

gevoelige gegevens uit de gebruikte data te onttrekken, in combinatie met de implementatie van robuuste gegevensbeschermingsmaatregelen zoals encryptie en toegangscontrole.

**Succes in werving, ontwikkeling en behoud van medewerkers**

Met de resultaten voortkomend uit het GenAI gestuurde SPP-proces beschikt u over de juiste informatie ten behoeve van strategische doorontwikkeling van de talentmanagementstrategie. Strategisch talentmanagement (STM) is het proces waarbij organisaties gericht inzetten op het aantrekken, ontwikkelen en behouden van medewerkers om zo hun strategische doelstellingen te behalen.

GenAI brengt ook hier kansen voor optimalisatie en automatisering in de uitvoering van het STM-proces. Zoals eerder genoemd bij het voorbeeld van Defensie is een waardevolle toepassing van GenAI de optimalisatie van wervingsprocessen. GenAI kan met geavanceerde algoritmen en natuurlijke taalverwerking snel en nauwkeurig Cv's analyseren en kandidaten identificeren die voldoen aan specifieke functie-eisen. Dit versnelt het selectieproces en zorgt ervoor dat recruiters zich kunnen richten op de meer strategische aspecten van hun werk. Bovendien kan GenAI helpen bij het verminderen van bias, wat bijdraagt aan een inclusiever wervingsproces. Het is hierbij wel essentieel zorgvuldig om te gaan met trainingsdata en het modelontwerp om bias binnen de tool zelf te voorkomen. Dit kan door gebruik te maken van een transparante dataset waarop het model wordt getraind, zodat bias zichtbaar wordt. Daarnaast is het van belang om een divers en interdisciplinair team te betrekken, dat verschillende perspectieven inbrengt.

GenAI biedt ook waardevolle kansen bij de ontwikkeling van medewerkers. Door gepersonaliseerde leermodules aan te bieden, kunnen trainingen worden afgestemd op de unieke behoeften en leerstijlen van medewerkers. Dit verhoogt de effectiviteit van trainingsprogramma's en helpt medewerkers sneller in te spelen op veranderende eisen binnen hun functie, waaronder het omgaan met nieuwe technologieën. GenAI past leermodules flexibel aan op basis van realtime prestaties en voortgang, waardoor voortdurende ondersteuning mogelijk is in de vorm van microlearning of on-demand feedback. Organisaties moeten echter de balans vinden tussen geautomatiseerd leren met GenAI en leren met trainer of mentor. Hoewel GenAI gepersonaliseerde leermodules kan creëren en onmiddellijke feedback geeft, kunnen medewerkers het gevoel hebben dat deze digitale interacties niet dezelfde diepgang en empathie bieden als menselijke trainers of mentoren. GenAI kan de nuances van interpersoonlijke communicatie niet begrijpen en overbrengen, wat essentieel is voor het ontwikkelen van soft skills. Door een combinatie van leren met GenAI en menselijke begeleiding, kunt u een cultuur creëren waarin medewerkers zich continu kunnen doorontwikkelen.

Tot slot kan GenAI trends identificeren door gegevens over vertrekkende medewerkers te analyseren. Dit onthult patronen in verloopgedrag, veelvoorkomende redenen voor vertrek en de effectiviteit van retentieprogramma's. Deze inzichten stellen organisaties in staat om gerichte maatregelen te nemen, wat de betrokkenheid en tevredenheid van medewerkers verhoogt en het verloop vermindert. Het is echter cruciaal dat de aangeleverde data compleet en nauwkeurig is. Onjuiste data-invoer kan leiden tot onnauwkeurige conclusies en ineffectieve of zelfs contraproductieve maatregelen.

Bronnen

Capgemini. (2024). Trends in Veiligheid 2024-2025: Veiligheid in Society 5.0. https://www.capgemini.com/nl-nl/wp-content/uploads/sites/19/2024/06/TiV-web.pdf

Openbaar Ministerie, & Politie. (2024). Cybercrimebeeld Nederland 2024. https://fts.politie.nl/cybercrimebeeld/

World Economic Forum. (2025). The future of jobs report 2025. World Economic Forum. https://www.weforum.org/publications/the-future-of-jobs-report-2025/

**Synergie: waar procesoptimalisatie en mensontwikkeling samenkomen**

De ware kracht van GenAI schuilt niet in de technologie zelf, maar in de synergie die ontstaat wanneer organisaties technologie en menselijk talent naadloos met elkaar verbinden. Zoals we eerder zagen bij de voorbeelden van SPP en STM, kan GenAI processen optimaliseren en nieuwe mogelijkheden creëren, maar het is de mens die de technologie stuurt, de ethische grenzen bewaakt en de uiteindelijke beslissingen neemt. De verbinding tussen technologie en talent is cruciaal voor alle organisaties, maar in het bijzonder voor veiligheidsorganisaties, waar de beslissingen vaak verstrekkende gevolgen hebben en ethische overwegingen van het grootste belang zijn.

De toekomst van technologie is niet iets van morgen; het is er al, hier en nu, en het is aan ons om deze kansen te grijpen. Alleen dan kunnen we de volledige potentie van GenAI benutten en een veiligere en rechtvaardigere samenleving creëren.

## Over de auteurs

**Jim Wouters**
Senior Consultant Workforce Transformation

Gespecialiseerd in de ontwikkeling van toekomstbestendige personeels- en organisatiestructuren binnen het veiligheidsdomein, met een sterke focus op de optimalisatie en integratie van GenAI.

jim.wouters@capgemini.com
https://www.linkedin.com/in/JimWouters

**Megan Tolner**
Managing Consultant Workforce Transformation

Gespecialiseerd in de menselijke factor van transformaties binnen het publieke veiligheidsdomein en richt zich op strategische personeelsplanning, strategisch talent management, en organisatie inrichting.

megan.tolner@capgemini.com
www.linkedin.com/in/megantolner

**Marjolein Wenderich**
VP / Global Head of Workforce & Organization / Advisory Client Partner Ministerie van Defensie.

Gespecialiseerd in HR (IT) transformaties, organisatiekunde en strategische personeelsplanning. Marjolein is met 25+ jaar ervaring in consulting een ervaren gesprekspartner voor CHRO's in het (semi) publieke domein en begeleidt organisaties in hun (digitale) transformaties.

marjolein.wenderich@capgemini.com
https://www.linkedin.com/in/marjolein-wenderich-66865a1/

04

# Een volwassen digitale werkomgeving: Sleutel tot efficiëntie en behoud van personeel

## Waarom is de digitale werkomgeving een essentieel onderdeel van het thema Toekomst van Werk?

**In Nederland heerst er momenteel een krapte op de arbeidsmarkt en naar verwachting houdt dit de komende jaren aan, zo blijkt uit het rapport van de Staatscommissie Demografische Ontwikkeling 2050[1]. Deze krapte wordt ook gevoeld in de publieke sector. Daarbovenop komen de recent aangekondigde bezuinigingen door het kabinet, wat maakt dat publieke organisaties voor een grote uitdaging staan[2]. Hoe verzet je meer werk met hetzelfde aantal mensen en maak je het werk efficiënter en effectiever binnen hetzelfde of een lager budget?**

## Highlights

- Om de uitdagingen effectief aan te pakken, is het essentieel om een strategisch traject in te richten voor de digitale werkomgeving
- Digital Employee Experience (DEX) zorgt ervoor dat technologie de werknemerservaring verbetert, wat essentieel is voor behoud en tevredenheid van personeel
- Gartner's Digital Workplace Maturity Model biedt een gestructureerd raamwerk voor het bepalen van het volwassenheidsniveau
- Zonder nu stappen te zetten binnen het volwassenheidsmodel, verliezen organisaties de wendbaarheid om in te spelen op innovaties

In deze uitdagende context speelt een volwassen digitale werkomgeving een cruciale rol. Door werkprocessen te optimaliseren, administratieve lasten te verlichten en medewerkers flexibeler te laten werken, kunnen organisaties efficiënter opereren. Daarnaast draagt het op de juiste manier inzetten van moderne technologie bij aan een betere werknemerstevredenheid, wat er weer voor zorgt dat medewerkers worden behouden. In dit artikel verkennen we hoe een volwassen digitale werkomgeving een antwoord kan bieden op deze uitdagingen.

Om die volwassen omgeving te realiseren is het ten eerste belangrijk om het huidige volwassenheidsniveau in kaart te brengen om vervolgens te kijken welke technologische trends hierbij van toepassing zijn om de stap naar een hoger niveau te zetten. Gartner biedt voor beide onderwerpen nuttige handvatten middels het 'Digital Workplace Maturity Model' en de 'Hype Cycle for Digital Workplace Applications'. Het Digital Workplace Maturity Model beschrijft een raamwerk waarin de volwassenheid van de werkomgeving ingedeeld kan worden op vijf niveaus[3]. In de Hype Cycle worden een aantal belangrijke trends geïdentificeerd, zoals Everyday AI, Workplace Experience Apps, Superapps, Citizen Developers, Workstyle Analytics en Digital Employee Experience (DEX)[4]. Deze trends bieden concrete mogelijkheden om processen te verbeteren, de productiviteit te verhogen en de werknemerstevredenheid te optimaliseren.

### Het belang van een volwassenheidsanalyse op de digitale werkomgeving

Om de uiteindelijke voordelen te kunnen behalen, moet er eerst inzicht komen in de huidige situatie van de werkomgeving om zo een passende ambitie te kunnen formuleren. Het volwassenheidsmodel evalueert de digitale werkomgeving van organisaties op basis van zeven thema's: strategische waarde, metriek en metingen, toewijding, rapportage, functies en rollen, beheertools en resultaten. Door deze thema's één voor één te analyseren en te beoordelen ontstaat er een compleet beeld van het huidige volwassenheidsniveau. De beoordeling wordt, zoals eerder genoemd, gedaan op een schaal van één tot vijf: van reactief (niveau 1) tot transformerend (niveau 5) Zie afbeelding 1..

Momenteel zit de meerderheid van onze publieke organisaties binnen het veiligheidsdomein op niveau 1 (reactief) of niveau 2 (ondersteunend) wat wordt geclassificeerd als laag. Organisaties op deze niveaus hebben moeite met het implementeren, beheren en bijbenen van (nieuwe) werkplek technologie. Een stap naar minimaal niveau 3 (activerend) zou daarom gewenst zijn. Op dit niveau wordt de medewerker meer centraal gesteld en betrokken in de ontwikkeling van de digitale werkomgeving. Daarnaast wordt


**Afbeelding 1: Volwassenheidsscan van de digitale werkomgeving**

er gestreefd naar operational excellence.

**Trends in de digitale werkomgeving**

Na het verkregen inzicht over het huidige volwassenheidsniveau, kan er een ambitieniveau worden vastgesteld. Om vervolgens concreet te kunnen maken op welke manier het ambitieniveau kan worden bereikt, komen de trends weer om de hoek kijken. De eerdergenoemde zes trends zien we als meest interessant voor het veiligheidsdomein en worden daarom kort uitgelicht.

Everyday AI integreert kunstmatige intelligentie in dagelijkse werkprocessen, waardoor medewerkers efficiënter kunnen werken en administratieve lasten verminderen. Workplace Experience Apps verbeteren de interactie tussen medewerkers en digitale systemen, terwijl Superapps verschillende functies en tools combineren in een enkele applicatie, wat de gebruikerservaring en efficiëntie ten goede komt. Daarnaast stelt de opkomst van Citizen Developers medewerkers zonder diepgaande IT-kennis in staat om zelf oplossingen te bouwen, wat innovatie versnelt en de afhankelijkheid van IT-teams vermindert. Workstyle Analytics helpt organisaties inzicht te krijgen in werkpatronen en knelpunten van medewerkers, zodat werkomgevingen geoptimaliseerd kunnen worden. Tot slot zorgt Digital Employee Experience (DEX) ervoor dat de algehele ervaring (perceptie en interactie) van werknemers met technologie binnen de werkomgeving verbetert, wat essentieel is voor behoud en tevredenheid van personeel.

### Trends in de digitale werkomgeving

Na het verkregen inzicht over het huidige volwassenheidsniveau, kan er een ambitieniveau worden vastgesteld. Om vervolgens concreet te kunnen maken op welke manier het ambitieniveau kan worden bereikt, komen de trends weer om de hoek kijken. De eerdergenoemde zes trends zien we als meest interessant voor het veiligheidsdomein en worden daarom kort uitgelicht.

Everyday AI integreert kunstmatige intelligentie in dagelijkse werkprocessen, waardoor medewerkers efficiënter kunnen werken en administratieve lasten verminderen. Workplace Experience Apps verbeteren de interactie tussen medewerkers en digitale systemen, terwijl Superapps verschillende functies en tools combineren in een enkele applicatie, wat de gebruikerservaring en efficiëntie ten goede komt. Daarnaast stelt de opkomst van Citizen Developers medewerkers zonder diepgaande IT-kennis in staat om zelf oplossingen te bouwen, wat innovatie versnelt en de afhankelijkheid van IT-teams vermindert. Workstyle Analytics helpt organisaties inzicht te krijgen in werkpatronen en knelpunten van medewerkers, zodat werkomgevingen geoptimaliseerd kunnen worden. Tot slot zorgt Digital Employee Experience (DEX) ervoor dat de algehele ervaring (perceptie en interactie) van werknemers met technologie binnen de werkomgeving verbetert, wat essentieel is voor behoud en tevredenheid van personeel.

## Over de auteur

**Emily van der Haagen**
**Manager Enterprise Model & Strategy**

Waardemanagement consultant met ervaring in strategische consultancy binnen het Justitie en Veiligheid-domein, met name op het ontwikkelen van businesscases en programmaplannen voor innovatie, scenarioanalyses voor opvang en huisvesting, het implementeren van batenmanagement en het formuleren van een visie op digitale werkomgevingen.

emily.vanderhaagen@capgemini.com
https://www.linkedin.com/in/emilyvanderhaagen/

Bronnen

1. Staatscommissie Demografische Ontwikkelingen 2050. (2024, 12 maart). Rapport Staatscommissie Demografische Ontwikkelingen 2050 – Tweede druk. https://www.staatscommissie2050.nl/documenten/rapporten/2024/03/12/rapport-staatscommissie-demografische-ontwikkelingen-2050-tweede-druk
2. Rijksoverheid. (2025, 14 maart). Kabinet aan de slag met 22% structurele bezuiniging bij rijksoverheid. https://www.rijksoverheid.nl/actueel/nieuws/2025/03/14/kabinet-aan-de-slag-met-22-procent-structurele-bezuiniging-bij-rijksoverheid
3. Gartner. (2025). Digital Workplace Maturity Assessment. Geraadpleegd op 21 mei 2025, van https://www.gartner.com/en/conferences/emea/digital-workplace-uk/conference-resources/digital-maturity-assessment
4. Cain, M., & Murphy, J. (2024, 10 juli). Hype Cycle for Digital Workplace Applications, 2024 (ID G00811075). Gartner, Inc.

# Duurzaamheid

## Wim Saris

Directeur-generaal Dienst Justitiële Inrichtingen bij het Ministerie van Justitie en Veiligheid

Interview:

# Duurzaamheid bij DJI: veiliger en mensgerichter detentiesysteem

De Dienst Justitiële Inrichtingen (DJI) staat de komende jaren voor complexe uitdagingen, onder andere op het gebied van personeel en capaciteit. In een wereld waar duurzaamheid, wendbaarheid en het centraal stellen van de burger steeds belangrijker worden deelt Wim Saris, DG van DJI, zijn visie over hoe deze thema's de lange termijnstrategie van DJI beïnvloeden: "We hebben te maken met een veranderende maatschappij, waarin we slimmer moeten werken, duurzamer moeten opereren en tegelijk veilige en humane detentie moeten blijven garanderen."

**Van bewustwording naar actie**

Duurzaamheid binnen DJI betekent veel meer dan het doorvoeren van enkele energiezuinige maatregelen. De organisatie staat voor een flinke transformatie om milieuvriendelijker en efficiënter te werken. Het duurzaamheidsrapport dat DJI in 2023 voor het eerst heeft uitgebracht, was dan ook kritisch. DJI streeft ernaar in 2030 klimaatneutraal te zijn, en de CO2-uitstoot tot nul te reduceren. Maar dat blijkt lastig. "Onze gevangenissen zijn verouderd en verre van energiezuinig. Als het buiten warm is, is het binnen warm en als het buiten koud is, is het binnen koud. Dit aanpakken vraagt om forse investeringen," zegt Saris. "Maar de financiële middelen zijn helaas beperkt. En we hebben te maken met dure gebouwen die complex in elkaar zitten. Wil je dat volledig isoleren, ben je heel wat investeringen verder. Als de keuze gaat tussen verduurzamen of het updaten van essentiële beveiligingssystemen om veiligheid te garanderen, is een beslissing snel genomen."

**Verduurzamingsslag**

Belangrijke onderdelen van de verduurzamingsslag zijn de elektrificatie van het wagenpark en de inkoop van groene energie. "We halen nu al grotendeels onze stroom van een windpark op de Maasvlakte. Daardoor wordt ongeveer 94% van onze verbruikte elektriciteit duurzaam opgewekt. Dit betekende een CO2-reductie van 34%. En een deel van ons wagenpark rijdt elektrisch. Niet alles, want voor sommige taken kunnen we ons het risico niet veroorloven om ergens stil te staan om op te laden. Maar we maken stappen in de goede richting." Een ander voorbeeld van de verduurzamingsslag is de inzet op een circulaire economie, zoals een afvalhub binnen een van de gevangenissen waar gedetineerden afval sorteren zodat het kan worden gerecycled. Het begon bij één gevangenis in Dordrecht waar werknemers samen met gedetineerden een afvalsorteerhub opzetten. Saris: "Dit soort initiatieven zijn heel welkom. Het draagt bij aan het milieu en creëert werkgelegenheid binnen detentie. Werk is natuurlijk een belangrijk onderdeel van re-integratie. Als we dat kunnen koppelen aan actuele thema's als duurzaamheid slaan we twee vliegen in één klap." De afvalhub is zo succesvol gebleken dat DJI het de komende maanden uitrolt naar andere inrichtingen.

### Wendbaarheid in een veranderende samenleving

"Een gedetineerde is op een bepaald moment weer iemands buurman. Het is onze taak om hen op een verantwoorde manier terug te laten keren in de maatschappij," stelt Saris. Dat vraagt om een continue balans tussen beveiliging en ruimte voor re-integratie, waarbij het dagprogramma voor justitiabelen goed aan moet sluiten bij de realiteit buiten de muren van de inrichtingen van DJI. Een belangrijke ontwikkeling is dan ook de herziening van dat dagprogramma. Saris: "In een aantal landen is gebleken dat een uitgebreid dagprogramma met veel activiteit juist bijdraagt aan veiligheid en gedragsverbetering. Veel meer dan door alleen beperkingen op te leggen. We kampen bij DJI al een aantal jaar met personeelstekorten. De neiging is om programma's juist in te korten als we met minder personeel moeten werken. Maar misschien moeten we het juist omdraaien en naar effectievere methoden kijken. Momenteel zijn we bezig te onderzoeken hoe we deze dagprogramma's effectiever in kunnen steken."

Dat blijkt een flinke uitdaging door constant gebrek aan personeel. "De krimpende arbeidspopulatie dwingt ons om met minder mensen hetzelfde werk te doen, zonder in te leveren op onze kernwaarden. Dat kan alleen door slimmer te organiseren en technologie beter in te zetten," legt Saris uit. Dit betekent bijvoorbeeld dat taken efficiënter moeten worden uitgevoerd met behulp van automatisering en digitale hulpmiddelen. Zoals de implementatie van slimme camera's die afwijkend gedrag kunnen detecteren. Dit maakt dat toezicht efficiënter kan worden uitgevoerd en minder bewakers nodig zijn. "Waarom zou je altijd twee mensen fysiek laten surveilleren, als technologie kan helpen bij detectie en signalering? Het past echt binnen de bredere trend van nu waarin DJI digitalisering inzet om veiligheid en efficiëntie te vergroten."

### Nieuwe technologie en cyberveiligheid

Waar technologie uitkomsten biedt, brengt het ook uitdagingen met zich mee. Naast fysieke veiligheid wordt ook digitale veiligheid een steeds grotere zorg binnen DJI. De opkomst van cybercriminaliteit en technologische dreigingen zoals drones maken extra beveiligingsmaatregelen noodzakelijk. "We moeten voorbereid zijn op een toekomst waarin digitale aanvallen net zo'n grote dreiging vormen als fysieke uitbraken," waarschuwt Saris. "Neem nou de drones. Onze gebouwen zijn bestand tegen de traditionele aanvallen, maar drones kunnen makkelijk op locaties komen waar dat voor buitenstaanders voorheen onmogelijk was. Hier moeten we dan ook op anticiperen." DJI investeert daarom in IT-infrastructuur en cyberweerbaarheid om te garanderen dat systemen veilig blijven en gevoelige informatie beschermd is.

### Reorganisatie voor een wendbaarder DJI

Om al deze veranderingen effectief door te voeren, wordt DJI intern gereorganiseerd. "We gaan van een model met één plaatsvervangend DG naar een vierkoppige dienstleiding, waarin verantwoordelijkheden beter verdeeld worden," licht Saris toe. Dit moet zorgen voor snellere besluitvorming en een meer samenhangende strategie. Daarnaast worden de budgetten anders verdeeld om innovatie en modernisering te stimuleren. "Op dit moment geven we 90% van ons budget uit aan personeel en 10% aan technologie en gebouwen. Dat moet naar 70-30, zodat we toekomstbestendig blijven." En dat is hard nodig om het tekort aan cellen en personeel het hoofd te kunnen bieden. "We hebben al een tekort aan detentiecapaciteit en tegelijkertijd moeten we verduurzamen en moderniseren. Dat is een lastige spagaat," geeft Saris toe. Dit betekent dat prioriteiten zorgvuldig worden gewogen, waarbij zowel humane detentie als veiligheid vooropstaan. Saris: "Een mogelijke oplossing is om bestaande cellencomplexen efficiënter te benutten door betere planning en het inzetten van technologie. Ook zijn we continu aan het kijken naar de mogelijkheden voor samenwerking met andere landen om tijdelijke capaciteitstekorten op te vangen."

### De toekomst van DJI

DJI gaat zich dus nog meer richten op interne verbeteringen en samenwerking met ketenpartners en maatschappelijke organisaties. "Veiligheid is een gezamenlijke verantwoordelijkheid. Door nauwer samen te werken met gemeenten, zorginstellingen en bedrijven kunnen we justitiabelen beter begeleiden naar een succesvolle terugkeer in de maatschappij", zegt Saris. "Innovatie speelt een belangrijke rol om capaciteitsproblemen het hoofd te bieden, en tegelijkertijd ook verduurzaming door te kunnen voeren. We experimenteren met nieuwe vormen van detentie. We moeten de juiste balans vinden tussen beveiliging en voorbereiding op het leven buiten. Re-integratie begint ten slotte al binnen de gevangenismuren. Ik geloof er heilig in dat dat de toekomst is van veilige en humane detentie."

05

# Van nature duurzaam

## Duurzaamheid als kernwaarde omarmen in het Justitie & Veiligheid (J&V) domein?

**De noodzaak voor duurzaamheid in het J&V-domein is urgenter dan ooit. Dit artikel verkent hoe en waarom J&V-organisaties het concept 'Van Nature Duurzaam' moeten omarmen om zowel bij te dragen aan een veilige en duurzame samenleving als ook om wendbaar en weerbaar te blijven.**

### Highlights

- Duurzaamheid raakt zowel de legitimiteit als ook de weerbaarheid van J&V-organisaties
- Van nature duurzaam betekent duurzaamheid als kernwaarde te omarmen
- Van nature duurzaam biedt J&V-organisaties een kans om zowel maatschappelijke als organisatorische uitdagingen effectief aan te pakken

**Van nature duurzaam: duurzaamheid als kernwaarde omarmen in het J&V-domein**

Klimaatverandering, milieuvervuiling en het verlies van biodiversiteit vormen aanzienlijke veiligheidsrisico's voor Nederland. Deze ecologische uitdagingen leiden tot bredere maatschappelijke problemen, zoals toenemende maatschappelijke onrust , die op hun beurt weer zorgen voor uitdagingen op het gebied van veiligheid en publieke orde. Extreme weersomstandigheden, zoals zware regen of droogte, kunnen leiden tot overstromingen of bosbranden, waardoor extra inzet van organisaties zoals de politie benodigd is. Daarnaast is steeds warmer wordend weer gelinkt aan een toename van bepaalde criminaliteitsvormen, wat druk legt op de gehele justitie-en veiligheidsketen.

Omdat het Justitie en Veiligheid (J&V)-domein verantwoordelijk is voor de veiligheid van de samenleving, is er een intrinsieke noodzaak voor deze organisaties om via hun bedrijfsvoering bij te dragen aan een duurzamere samenleving. Het raakt immers de legitimiteit en het bestaansrecht van deze organisaties. Bovendien zetten de maatschappelijke uitdagingen rondom ecologische en sociale duurzaamheid extra druk op de verschillende organisaties binnen het J&V-domein. Denk aan de toenemende druk op de al schaarse capaciteit op bijvoorbeeld de migratieketen of de financiële impact op organisaties met een grote huisvestingsportefeuille (zoals het COA, DJI of Politie) als gevolg van stijgende energiekosten. Deze uitdagingen hebben een directe relatie met sociale en ecologische duurzaamheid en raken de weerbaarheid van J&V-organisaties. Kortom, duurzaamheid is om twee redenen urgent voor J&V-organisaties: ten eerste omdat het de geloofwaardigheid en legitimiteit van deze organisaties raakt, en ten tweede omdat duurzaamheid ook gelinkt is aan andere grote uitdagingen (zoals schaarste in capaciteit en middelen) waar deze organisaties mee te maken hebben, wat extra druk zet op hun wendbaarheid en weerbaarheid.

Veel uitvoeringsorganisaties in het J&V-domein zijn al actief bezig met duurzaamheid. In lijn met de Sustainable Development Goals en het Nederlandse klimaatakkoord hebben veel uitvoeringsorganisaties in het J&V-domein duurzaamheidsdoelen voor hun interne bedrijfsvoering opgesteld. Echter, deze worden vaak opgepakt in de vorm van een apart en (vaak) tijdelijk duurzaamheidsprogramma of team, en dit maakt het realiseren van deze doelen een uitdaging, omdat de duurzaamheidsdoelen niet goed afgestemd zijn op de overige strategische ambities en doelen, en daardoor ook niet kunnen inspelen op de andere kernuitdagingen waar deze organisatie mee te maken hebben.

Onze stelling in dit artikel is dat J&V-organisaties een stap verder moeten gaan en duurzaamheid niet als een los project of programma georganiseerd moet worden. In plaats daarvan moet duurzaamheid als kernwaarde in de strategie van de organisaties worden omarmd. Met andere woorden: J&V-organisaties moeten van nature duurzaam zijn. Deze benadering van duurzaamheid biedt de mogelijkheid om zowel vooruitgang te boeken op morele duurzaamheidsdoelen als bij te dragen aan het aanpakken van bredere uitdagingen waarmee deze organisaties te maken hebben.

In dit artikel zullen we verder ingaan op het concept “van nature duurzaam” en zullen we aan de hand van voorbeelden laten zien waarom het juist voor de organisaties in het J&V-domein van belang is.

**Wat betekent het om “van nature duurzaam” te zijn?**

Het houdt in dat duurzaamheid een fundamenteel onderdeel is van elke beslissing en actie binnen de organisatie. Duurzaamheid is niet iets wat apart wordt behandeld, maar is een kernwaarde die in alle lagen van de organisatie is ingebed. Dit betekent dat bij elke keuze die wordt gemaakt, duurzaamheid een prioritaire waarde is. Het is essentieel om helder te definiëren wat de prioritaire duurzame waarden zijn en ervoor te zorgen dat geen enkele actie een negatief effect heeft op deze waarden. Om dit te bereiken, moeten organisaties op verschillende niveaus het gesprek aangaan over duurzaamheid. Dit begint bij het opnemen van duurzaamheid in de kernwaarden, missie en visie van de organisatie. Vervolgens moet dit worden vertaald naar elk onderdeel van de organisatie, ingebed in de primaire processen, in de structuur en het besturingsmodel van de organisatie. Medewerkers moeten worden opgeleid en meegenomen in deze duurzame visie, zodat zij begrijpen wat duurzaamheid betekent voor hun dagelijkse werkzaamheden en hoe zij hieraan kunnen bijdragen.

Een uitstekend voorbeeld van een organisatie die het concept “van nature duurzaam” heeft omarmd is Lego. Lego stelt hele hoge eisen aan de kwaliteit en prestaties van hun producten. De belangrijkste eis is dat Lego stenen perfect op elkaar moeten passen zonder hun vermogen om samen te klikken te verliezen, iets wat ze ‘clutch power’ noemen, waardoor ze langdurig meegaan. Tegelijkertijd heeft Lego duidelijke ambities op gebied van duurzaamheid en hebben ze duurzaamheid ook als kernwaarde opgenomen in de ontwerpeisen voor hun producten . Dit betekent dat ze rigoureus op zoek zijn naar hernieuwbare en duurzame materialen die gebruikt kunnen worden voor productie van hun Lego stenen die ook altijd voldoen aan hun strenge veiligheids- en kwaliteitsnormen. Ze gebruiken bijvoorbeeld suikerriet voor flexibele onderdelen zoals bloemen en minifiguuraccessoires, en gerecyclede materialen zoals oude visnetten en motorolie voor banden. Dit laat zien hoe duurzaamheid kan worden geïntegreerd in het innovatieproces en productontwerp, en hoe Lego “van nature duurzaam” is door duurzaamheid als een fundamenteel onderdeel van hun bedrijfsvoering te beschouwen.

We kennen ook inspirerende voorbeelden van organisaties die het concept “van nature duurzaam” weten te omarmen in het J&V-domein. Zo heeft de Dienst Justiële Inrichtingen (DJI) onlangs de Afvalhub  in een van hun penitentiaire inrichtingen gelanceerd (zie ook interview met Wim Saris). De Afvalhub is een werkzaal, waar gedetineerden al het afval van de inrichting nascheiden. Met de Afvalhub werkt DJI niet alleen aan hun duurzaamheidsdoelen, zoals afvalreductie, maar krijgt de organisatie ook beter inzicht in hun afvalstromen. Dit leidt ertoe dat bepaalde afvalstromen vermeden of verminderd kunnen worden. Bijvoorbeeld, medicijnen die onnodig worden weggegooid kunnen minder besteld worden, en textiel dat in het afval belandt kan gerecycled of hergebruikt worden, wat aanzienlijke kostenbesparingen kan opleveren. Daarnaast draagt de Afvalhub bij aan de veiligheid in de penitentiaire inrichting en biedt gedetineerden een waardevolle dagbesteding. Gedetineerden leren waardevolle vaardigheden die ze kunnen gebruiken bij hun re-integratie in de samenleving, zoals het vinden van een baan bij een milieudienst. Door duurzaamheid als kernwaarde te omarmen en te linken aan andere doelen en uitdagingen, zoals veiligheid, kostenbesparing en dagbesteding voor gedetineerden,

maakt DJI impact op meerdere vlakken. Dit voorbeeld illustreert hoe duurzaamheid geïntegreerd kan worden in de bedrijfsvoering en hoe het concept "van nature duurzaam" in de praktijk kan worden gebracht.

Er zijn nog veel andere thema's en uitdagingen waar het omarmen van het concept "van nature duurzaam" een kans biedt om niet alleen duurzaamheidsdoelen te bereiken, maar ook kan bijdragen aan andere doelstellingen binnen het J&V-domein. Een actueel bedrijfsvoeringsthema is de kosten van huisvesting, naast de verduurzaming van de huisvestingsportefeuille. Organisaties zoals de Politie, COA en DJI hebben grote huisvestingsportefeuilles die ze willen of moeten verduurzamen. Tegelijkertijd staan deze organisaties onder druk vanwege bezuinigingen. Hier ligt een kans: door goed inzicht te krijgen in de energie-efficiëntie, bijvoorbeeld via een energy command center, en te investeren in de verduurzaming van panden, kunnen aanzienlijke besparingen op energiekosten worden gerealiseerd. Daarnaast zijn J&V-organisaties bezig met digitale transformaties, maar de ambities op het gebied van digitalisering houden vaak geen rekening met verduurzamingsambities. Ook hier bestaan oplossingen om op een zo duurzaam mogelijke manier te digitaliseren. Door duurzaamheid te integreren in digitale transformaties, kunnen J&V-organisaties niet alleen hun ecologische voetafdruk verkleinen, maar ook efficiënter en kosteneffectiever opereren. Dit kan bijvoorbeeld door het gebruik van energiezuinige datacenters, het implementeren van groene IT-oplossingen en het bevorderen van digitale werkprocessen die minder afhankelijk zijn van papier en fysieke middelen.

**Van nature duurzaam biedt J&V-organisaties een kans om zowel maatschappelijke als organisatorische uitdagingen effectief aan te pakken**

De noodzaak voor duurzaamheid in het J&V-domein is urgenter dan ooit. Klimaatverandering, milieuvervuiling en het verlies van biodiversiteit vormen aanzienlijke veiligheidsrisico's voor Nederland. Deze ecologische en sociale uitdagingen vereisen een proactieve aanpak in de bedrijfsvoering van J&V-organisaties. Maar, door aan te slag te gaan met duurzaamheid, nemen J&V-organisaties niet alleen hun voorbeeldrol serieus om bij te dragen aan een veilige en toekomstbestendige samenleving. Van nature duurzaam zijn als organisatie biedt juist ook kansen voor J&V-organisaties om bij te dragen aan het oplossen van belangrijke operationele- en bedrijfsvoering uitdagingen waar ze momenteel mee te maken hebben. Door duurzaamheid als kernwaarde te omarmen kunnen J&V-organisaties een leidende rol nemen in het publieke domein om zowel maatschappelijke als organisatorische uitdagingen effectief aan te pakken.

## Over de auteurs

**Tom van den Nieuwenhuijzen**
**Director Sustainability, Strategy and Innovation Public Sector**

Tom is werkzaam als Director Sustainability, Strategy en Innovation bij Capgemini Invent en werkt als Global Lead Sustainability Public Sector voor de Capgemini Group. Tom adviseert en ondersteunt publieke organisaties op het gebied van duurzaamheid, (bestuurlijke-, proces- en democratische-) innovatievraagstukken en complexe politiek-maatschappelijke opgaven.

tom.vanden.nieuwenhuijzen@capgemini.com

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

**Nadja Zeiske**
**Managing Consultant Organization, Purpose & Strategy**

Nadja adviseert en ondersteunt organisaties op het gebied van duurzaamheidstransformaties met een focus op visie- en strategievorming en het borgen van duurzaamheid in de organisatiestructuur en cultuur.

nadja.zeiske@capgemini.com

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

**Francijna van Alphen**
**Client manager Justitie & Veiligheid domein**

Francijna is Client Manager binnen het Justitie & Veiligheid domein. Ze plaatst klanten centraal bij het adviseren over innovatieve en duurzame mogelijkheden, en biedt hen de kracht van het Capgemini portfolio.

francijna.van.alphen@capgemini.com

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

Bronnen
https://www.lego.com/en-us/sustainability/sustainable-materials
https://www.linkedin.com/posts/woltervandervlist_afvalhub-in-pi-dordrecht-openden-karin-activity-7286026917554601985-KGAf/?originalSubdomain=nl

06

# To Build or To Buy - That is the question

## Hoe te navigeren tussen de keuze voor het bouwen of kopen van IT-oplossingen in het nieuwe geopolitieke klimaat

**Bij het kiezen tussen het kopen (buy) of bouwen (build) van een IT-oplossing staan organisaties voor een cruciale beslissing die hun toekomst kan bepalen. Wanneer is het juiste moment om die keuze te maken? In dit artikel gaan we in op de strategische keuze tussen build en buy, en hoe deze beslissing invloed heeft op je risicobereidheid en de algehele bedrijfsvoering. Ontdek waarom een weloverwogen keuze voor build of buy essentieel is voor succes**

**Over de schrijvers:**
Niels is een fervent voorstander van het bouwen van IT-oplossingen. Met zijn achtergrond in softwareontwikkeling en zijn passie voor maatwerkoplossingen, gelooft hij sterk in de voordelen van zelf bouwen.

Folkert daarentegen is een groot voorstander van het kopen van kant-en-klare IT-oplossingen. Met jarenlange ervaring in IT-management en een focus op efficiëntie en betrouwbaarheid, ziet hij de voordelen van snel inzetbare en goed ondersteunde systemen.

Niels en Folkert brengen hun unieke perspectieven en ervaringen naar voren in deze discussie over build versus buy. Ontdek waarom een weloverwogen keuze voor build of buy essentieel is voor succes.

## Highlights

- Zelf een IT-oplossing bouwen vereist een investering vooraf, biedt een kans op besparing op termijn en geeft volledige controle over functionaliteit
- Gekochte IT-oplossingen ontzorgen organisaties, bieden voorspelbaarheid, maar minder controle over innovatie
- Het is onverstandig om een keuze tussen build vs. buy uitsluitend te baseren op economische overwegingen
- Recente geopolitieke ontwikkelingen zijn meer dan ooit van invloed op een build vs. buy overweging
- Een goede build vs. buy afweging vereist overwegingen over Beschikbaarheid, Integriteit en Vertrouwelijkheid

**Build**

Het bouwen van je eigen IT-oplossing biedt tal van voordelen, vooral als je specifieke behoeften hebt die niet door standaardoplossingen kunnen worden vervuld. Door zelf de IT-oplossing te bouwen, heb je volledige controle over het systeem of de leveringsketen. De voordelen en nadelen zijn bekend. The sky is the limit, maar tegen welke prijs? Tegelijkertijd biedt build wel de mogelijkheid om op een lager niveau in de waardeketen keuzes te maken over afhankelijkheden. De keuze voor een hyperscaler die al je data beheert is anders dan de keuze voor een opensource software library.

Hoewel de initiële kosten voor het bouwen van je eigen IT-oplossing hoger kunnen zijn dan het kopen van een oplossing, kunnen de kosten op lange termijn lager uitvallen. De use cases zijn specifiek, maar er is een markt voor partijen die eigen oplossingen bouwen, vooral in het veiligheidsdomein, omdat er naast economische overwegingen ook andere belangen meegewogen worden. Op de lange termijn kan een organisatie zelfs geld besparen met build, mits de technische kennis in huis is om het IT-platform te beheren en te exploiteren.

Het bouwen van je eigen IT-oplossing biedt aanzienlijke voordelen op het gebied van controle, heeft de potentie om een kostenbesparing te realiseren en geeft mogelijkheden tot unieke innovatie en maatwerk. Het stelt je in staat om oplossingen te creëren die perfect aansluiten bij je specifieke behoeften en je een concurrentievoordeel geven.

**Buy**

Het kopen van een kant-en-klare IT-oplossing biedt hele andere voordelen. Voor generieke bedrijfsprocessen zijn er generieke oplossingen te verkrijgen in de markt.  Kant-en-klare cloudoplossingen nemen op dit vlak veel werk uit handen.

De initiële kosten voor het kopen van een IT-oplossing zijn in de regel lager, Pay as You Go, een reserved instance of een licentie bieden vaak voorspelbaarder kostenstructuren. Je betaalt een vaste prijs voor de software en eventuele abonnementskosten voor updates en ondersteuning. Het grote voordeel: de kosten zijn voorspelbaar, budgetten zijn consistent. Risico's die samenhangen met het onderhouden van de software worden belegd bij de leverancier als onderdeel van de abonnementsprijs. What more can one wish for? De keerzijde is dat we ons overleveren aan de financiële grillen van leveranciers.

Een ander voordeel van het kopen van een IT-oplossing is dat het uitrollen van functionele - en security-updates geen inspanning vereist. Echter, in een buy-scenario heb je veel minder controle op de roadmap van een IT-oplossing. De leverancier beslist welke feature wanneer ontwikkeld wordt.

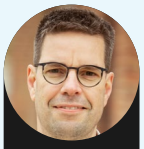
Kortom, het kopen van een kant-en-klare IT-oplossing biedt aanzienlijke voordelen op het gebied van snelle implementatie, kostenbeheersing, ondersteuning en updates. Het stelt je in staat om snel en efficiënt de IT-infrastructuur in te zetten zonder de complexiteit en risico's van het zelf bouwen.

# Een Gezamenlijke Beschouwing

Niels

"De functionele en economische afwegingen tussen build en buy zijn van toepassing voor iedere organisatie. Wat het veiligheidsdomein bijzonder maakt is een aanvullende overweging; het IT-platform van organisaties in het veiligheidsdomein is extra interessant voor statelijke actoren met belangen die haaks staan op die van de eigenaar van de data. Wanneer organisaties ervoor kiezen om eigen IT-oplossingen te bouwen, hebben zij de volledige controle over de beveiliging en compliance van het systeem. Dit betekent dat je specifieke beveiligingsmaatregelen kunt implementeren die aansluiten bij de unieke behoeften van je organisatie. Zelf bouwen kent ook aanzienlijke risico's: het ontwikkelen van een maatwerksysteem vereist diepgaande kennis van beveiligingsprotocollen en compliance-eisen. Kennis en kunde die schaars is op de markt. Waar bedrijven risico's uitdrukken in termen van economische schade gaat het in het veiligheidsdomein over een andere grootheid: onze veiligheid."

"Aan de andere kant biedt het kopen van een kant-en-klare IT-oplossing ingebouwde beveiligings- en compliance-functies die door de leverancier worden onderhouden en regelmatig worden bijgewerkt. Dit vermindert het risico op beveiligingslekken en zorgt ervoor dat je altijd voldoet aan de nieuwste regelgeving. Echter, je bent afhankelijk van de leverancier voor updates en ondersteuning. Je introduceert een aanvullende aanvalsvector: de leverancier. Daar waar de leverancier een commerciële partij is, kunnen economische belangen van bedrijven en de belangen in het veiligheidsdomein haaks op elkaar komen te staan. Ook introduceert dit geopolitieke afhankelijkheden die niet altijd wenselijk zijn. Denk aan Amerikaanse cloud-providers; een worsteling voor veel ketenpartners in het Europese veiligheidsdomein."

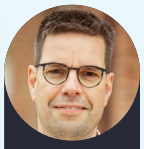


Folkert

Niels

"Nog een belangrijk aspect is de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van gegevens. Bij een zelfgebouwd systeem kun je specifieke maatregelen nemen om de BIV-principes te waarborgen. Je kunt bijvoorbeeld redundante systemen en back-ups implementeren om de beschikbaarheid te garanderen en geavanceerde encryptiemethoden gebruiken om de vertrouwelijkheid te beschermen. Dit niveau van maatwerk kan moeilijk te bereiken zijn met een standaardoplossing."

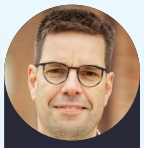
"Hoewel dat waar is, bieden veel kant-en-klare oplossingen tegenwoordig robuuste BIV-functies die zijn ontworpen om te voldoen aan de hoogste beveiligingsstandaarden. Leveranciers investeren vaak aanzienlijk in het ontwikkelen en onderhouden van deze functies, wat betekent dat je profiteert van de nieuwste technologieën zonder zelf te hoeven investeren in onderzoek en ontwikkeling. Bovendien bieden leveranciers vaak garanties en certificeringen die aantonen dat hun systemen voldoen aan de relevante regelgeving en beveiligingsstandaarden."


Folkert


Niels

"Uiteindelijk komt het neer op een afweging tussen controle en gemak. Het bouwen van je eigen IT-oplossing biedt maximale controle en maatwerk, maar brengt hogere risico's en complexiteit met zich mee. Het kopen van een kant-en-klare oplossing biedt gemak en ingebouwde beveiliging, maar je bent afhankelijk van de leverancier voor updates en compliance."

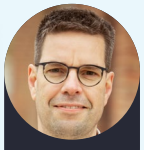
"Precies. Het is essentieel dat organisaties hun risicobereidheid en specifieke behoeften zorgvuldig evalueren voordat ze een beslissing nemen. Beide benaderingen hebben voor- en nadelen, en de beste keuze hangt af van de unieke omstandigheden van de organisatie."


Folkert


Niels

"Een aanvullende dimensie gaat over de vraag van soevereiniteit. Het Europese veiligheidsdomein is in hoge mate afhankelijk van strategische partners die in toenemende mate niet geworteld zijn in Europa. Echter, de garanties die je kunt ontlenen aan het "soeverein zijn", zijn in sterke mate afhankelijk van de controle over de leveringsketen. Anders gezegd: wie garandeert mij dat er geen achterdeur zit in de server die ik koop?"

"Absoluut. Tegelijkertijd is het end-to-end in beheer hebben van alle componenten die nodig zijn voor IT en IT-beveiliging een illusie. Om te beginnen heeft Nederland geen eigen kopermijn. Globalisering heeft ervoor gezorgd dat we dus altijd afhankelijk zijn van partijen die buiten onze directe invloedssfeer zitten."


Folkert

**Dit concluderen wij**

"To Build or to Buy. That's the question" zou Shakespeare in deze tijd gezegd kunnen hebben. Geopolitieke spanningen en onzekere leveringsketens zorgen ervoor dat veiligheidsinstanties in hogere mate zijn aangewezen op het zelf ophouden van de technologische veiligheidsbroek. Tegelijkertijd is het volledig in controle zijn een illusie. Soevereiniteit is een groot goed, maar de marktdominantie van Amerikaanse hyperscalers maakt dat het risico van schijnveiligheid op de loer ligt, zowel voor build als voor buy.

**Onze Aanbeveling**

Overheidsinstanties die opereren in het veiligheidsdomein doen er verstandig aan hun ketenpartners zorgvuldig en voor de lange termijn te kiezen. Op deze manier worden continuïteit, betrouwbaarheid en innovatie gecombineerd met een gebalanceerde mix van risico's en resultaten. ITIL leert ons al decennia om informatiesystemen zowel "fit for use" als "fit for purpose" te ontwerpen en exploiteren. Recente geopolitieke ontwikkelingen voegen een nieuwe overweging toe die tot voor kort als vanzelfsprekend "veilig" konden worden beschouwd. In het veiligheidsdomein komt nog meer nadruk te liggen op vertrouwelijkheid, integriteit en beschikbaarheid. Veiligheidsorganisaties kunnen dit niet alleen. Middels onderlinge samenwerking, kennisdeling en publiek-private samenwerking zijn er voldoende opties om een weloverwogen keuze tussen build, buy of een mengvorm te maken.

## Over de auteur

**Niels Lemmens**
**Principal Consultant Cloud Infrastructure Services**

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

niels.lemmens@capgemini.com

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

**Folkert Visser**
**Managing Consultant Cloud Infrastructure Services – Cybersecurity**

Folkert is een Cyber Defense nerd en weet als geen ander de brug te slaan tussen theorie, beleid en de weerbarstige praktijk. Hij heeft een achtergrond in de Telecom-sector en hij is momenteel vooral actief in het publieke domein.

folkert.visser@capgemini.com

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

# Weerbaarheid

**Matthijs van Amelsfort**

Directeur Nationaal Cyber Security Centrum bij het ministerie van Justitie en Veiligheid

Interview:

# Digitale weerbaarheid in een veranderend tijdperk

Wanneer een muisklik voldoende is om een bedrijf lam te leggen of een overheid te ontwrichten, wordt duidelijk hoe kwetsbaar onze digitale wereld werkelijk is. Cyberaanvallen zijn dagelijkse realiteit: van datalekken en ransomware tot geopolitiek gemotiveerde digitale sabotage. Matthijs van Amelsfort, directeur van het Nationaal Cyber Security Centrum (NCSC), deelt zijn visie op de huidige trends, uitdagingen en toekomstperspectieven binnen het cybersecurity-domein. Hoe bereidt het NCSC zich voor op de komende jaren waarin digitale weerbaarheid een absolute voorwaarde is voor maatschappelijke stabiliteit?

**Het NCSC heeft vier rollen**

De Nederlandse Cybersecuritystrategie stelt een duidelijke koers: er is een centrale organisatie nodig die de digitale weerbaarheid van Nederland versterkt. Het NCSC is daarom aan het samenvoegen met het Digital Trust Center en het CSIRT-DSP (het Computer Security Incident Response Team voor digitale dienstverleners) om die rol te kunnen vervullen. Van Amelsfort: “Dat betekent dat we niet alleen informatie en kennis uitwisselen, maar ook écht regie voeren en coördineren, in samenwerking met onze publieke en private partners. Daarnaast zijn we het Computer Security Incident Response Team (CSIRT) voor incident response en coördinatie.”
Het NCSC speelt een sleutelrol in het verhogen van de cyberweerbaarheid van organisaties en bedrijven in Nederland door hen te voorzien van actuele informatie en het delen van kennis. Het zijn spannende tijden, want de organisatie bevindt zich momenteel in een fase van grote veranderingen. Dit begint met het samenvoegen van het DTC, CSIRT-DSP en het NCSC- een flinke organisatieverandering. Maar ook het aantal organisaties dat onder de doelgroep van het NCSC valt gaat aanzienlijk groeien met de aanstaande implementatie van de EU-netwerk- en informatiebeveiligingsrichtlijn (NIS2), een richtlijn die in Nederland in 2025 wordt ingevoerd als de Cyberbeveiligingswet (Cwb).

**Lessons learned**

Een van de meest beruchte cyberincidenten van 2024 was de storing veroorzaakt door de CrowdStrike-software-update. Systemen kwamen terecht in een eindeloze herstart-lus, wat leidde tot grote ontwrichtingen in essentiële bedrijfsprocessen. Een unieke situatie, want de oorzaak lag niet in een bewuste aanval maar bij een fout in de software. Van Amelsfort: “CrowdStrike was voor veel mensen een wake-up call. Het liet wederom zien hoe afhankelijk we zijn van digitale systemen en hoe belangrijk het is om voorbereid te zijn op onverwachte verstoringen. Bijvoorbeeld door je bedrijfsvoering honderd procent op orde te hebben met solide business continuity-plannen. Zelfs onbedoelde fouten kunnen grote gevolgen hebben voor onze infrastructuur, terwijl voorheen veel meer onze focus lag op eventuele bewuste aanvallen.”

### Snel schakelen

Het NCSC speelde in de nasleep van CrowdStrike een grote rol bij het bieden van handelingsperspectief aan getroffen organisaties, zoals luchtvaartmaatschappijen en logistieke bedrijven. “Door snel te schakelen konden we verdere schade beperken en anderen waarschuwen voor soortgelijke kwetsbaarheden,” voegt van Amelsfort toe. “De CrowdStrike-kwestie toonde wederom aan hoe afhankelijk organisaties binnen het digitale ecosysteem van elkaar zijn. Om risico’s in te perken moeten we zo snel mogelijk reageren op onverwachte risico’s. CrowdStrike had daarom ook een positieve uitkomst: het leidde tot een extra evaluatie binnen het NCSC om zo processen te verbeteren en adviezen op te stellen die organisaties beter voorbereiden op dergelijke scenario’s.”

### Toename van geopolitieke dreigingen

Van Amelsfort benadrukt dat geopolitieke dreigingen in toenemende mate invloed hebben op de digitale veiligheid. “De wereld is onrustig. We zien een toename van DDoS-aanvallen en hacktivistische activiteiten, evenals verstoringen in fysieke infrastructuren zoals internetkabels. Deze gebeurtenissen hebben een directe impact op de digitale wereld, en onze fysieke wereld. Ze vragen om verhoogde paraatheid,” legt hij uit. “Relatief nieuwe technieken zoals AI voor data-analyse kunnen ons helpen om afwijkend netwerkgedrag sneller te detecteren en bedreigingen vroegtijdig aan te pakken. Maar aan de andere kant geeft AI ook nieuwe mogelijkheden om bestaande dreigingen te versterken. Denk aan een toename van spearfishing-aanvallen. Het vraagt veel van je medewerkers en de bewustwording binnen je organisatie, zeker in de bestuurskamer, nu er straks ook een meld- en zorgplicht is voor ondernemingen onder de cyberbeveiligingswet,” aldus Van Amelsfort.

### Reorganisatie

Het NCSC is volop in beweging. Momenteel vindt een samenvoeging plaats van het NCSC met het Digital Trust Center (DTC), een onderdeel van het ministerie van EZ. Deze moet rond zijn op 1 januari 2026. Dit betekent een enorme stap naar een meer gecentraliseerde en effectieve aanpak van cybersecurity in Nederland. Daarnaast zal ook het Ministerie van Economische Zaken (waar het DTC was ondergebracht) een aanvullende opdrachtgever voor het NCSC zijn. Van Amelsfort: “De handelsgeest en ondernemingsgeest die het DTC meebrengt willen we incorporeren in onze vernieuwde organisatie. Afstappen van een traditionele lijnstructuur en sturen op resultaten en vakinhoudelijke aansturingslijnen. Zo willen we onze specialisten nog meer in staat stellen hun werk te doen.”

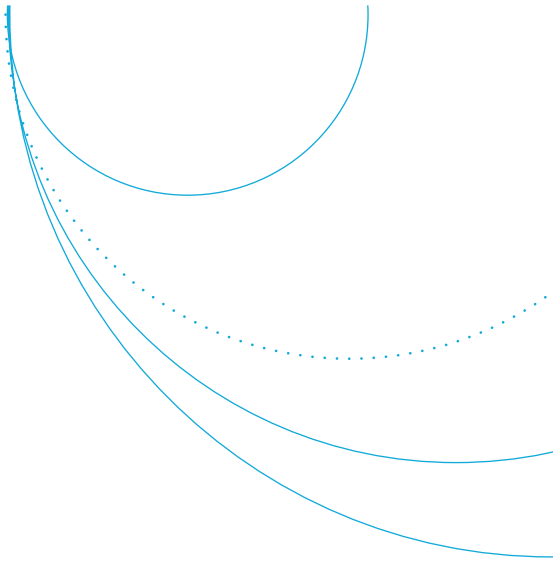
Het Digital Trust Center, voornamelijk gericht op het mkb, had de verantwoordelijkheid voor alle niet-vitale doelgroepen. Het NCSC bedient momenteel ruim 300 entiteiten maar na deze samenvoeging zal het daardoor ruim 2,4 miljoen organisaties van kennis- en advies voorzien. “De vergroting van onze organisatie maakt het mogelijk om niet alleen grote, vitale organisaties te ondersteunen, maar ook kleinere bedrijven in de keten, die vaak als stepping stones worden gebruikt in cyberaanvallen”, aldus van Amelsfort. Het DTC brengt waardevolle kennis en methodieken in voor het betrekken en ondersteunen van deze alles behalve vitaal aangemerkte organisaties bij het versterken van hun weerbaarheid. De samenvoeging versterkt zo de positie van het NCSC als centraal aanspreekpunt voor cyberveiligheid in Nederland. Maar de fusie brengt ook uitdagingen met zich mee. Denk aan het harmoniseren van werkwijzen van de drie verschillende organisaties en het creëren van een uniforme cultuur binnen de nieuwe organisatie. Deze nieuwe organisatie moet een datagedreven aanpak hanteren waarbij inzichten uit meldingen en incidenten sneller vertaald kunnen worden naar concrete actiepunten. Van Amelsfort: “Het doel is om trends en patronen te identificeren die ons in staat stellen om proactief dreigingen aan te pakken. Dit vereist technologische innovatie en nauwe samenwerking tussen publieke en private partijen.”

### Toekomstperspectieven

De toekomst van cyberveiligheid wordt mede bepaald door technologische ontwikkelingen zoals AI en post-quantum cryptografie. Van Amelsfort: “Generatieve AI biedt veel kansen maar vereist tegelijkertijd dat we de ethische implicaties en veiligheidsrisico’s goed begrijpen. Dat betekent risico’s mitigeren voor onze digitale infrastructuur, maar ook onze fysieke. Denk aan stroomuitval. Nederland is verwend met een stabiele infrastructuur, maar we moeten voorbereid zijn op disruptieve scenario’s. Het gaat erom dat we zowel als individu als samenleving veerkrachtiger worden.”

### Persoonlijke ambitie: een robuuste organisatie bouwen

Als directeur wil Van Amelsfort zijn stempel drukken door het NCSC om te vormen tot een flexibele, toekomstgerichte organisatie. Dit omvat technologische innovatie en een focus op een meer agile werkstructuur. “Het bouwen van een nieuwe, datagedreven organisatie met een cultuur waarin iedereen zich thuis voelt, is mijn belangrijkste missie,” aldus Van Amelsfort. “De samenvoeging met het DTC zal een organisatie brengen die schaalgrootte benut en expertise samenbrengt. Als ik dit kan gebruiken om een fundament te bouwen voor innovatie en weerbaarheid, ben ik tevreden.”



07

# Autonomie is dé cloud-trend; kunnen kiezen de oplossing!

**De roep om de afhankelijkheid van Amerikaanse Big Tech te doorbreken is ineens een megatrend. Ondanks het feit dat de Amerikaanse presidentsverkiezingen al lang gepland waren, zijn we toch verrast. Het is duidelijk dat we veel afhankelijker zijn van Amerikaanse bedrijven en technologie dan we in de gaten hadden. Het is ook duidelijk dat dit allerlei nadelen heeft die we in de "business case om naar de hypercloud te gaan" nooit meegewogen hebben. Leidt deze trend naar een catastrofe? Of is het een kans en zijn positieve oplossingen voor handen?**

Wat is er nieuw aan de autonomie-trend? Het issue is niet meer de vraag of Amerikaanse (of andere) diensten bij gegevens van de Nederlandse overheid kunnen. Dat is vergeleken met andere risico's nog altijd een klein probleem. Het issue is of een Amerikaanse president diensten waarvan wij afhankelijk zijn kan uitschakelen. Het Internationale Strafhof in Den Haag heeft inmiddels direct met die vraag te maken. Het vraagt zich af wat er gebeurt als Microsoft verboden wordt om diensten te blijven leveren en of het gerechtshof dan zijn dagelijkse werk kan blijven doen.

Cloudtechnologie heeft zich in de afgelopen 10 jaar ontwikkeld tot een essentiële bouwsteen van onze digitale economie en samenleving. Het is moeilijk geworden om zonder cloudtechnologie snel en goed digitale diensten te leveren. Dat de overheid sterk achterloopt op het bedrijfsleven en consumenten in cloudgebruik hangt dan ook sterk samen met het feit dat overheidsorganisaties zeer veel moeite hebben om snel genoeg moderne wendbare digitale diensten te realiseren. Deze achterstand versterkt de afhankelijkheid; te vaak ziet men geen alternatief voor cloudgebruik waar geen goede voorwaarden aan gesteld kunnen worden. Dat ligt meer aan de overheid dan aan de cloudproviders.

Hoe willen wij als Nederland op deze situatie reageren? Wat zijn de mogelijkheden die een overheidsorganisatie heeft; en wat zou iedere producteigenaar, developmentteam en managementteam zelf moeten doen?

## Highlights

- Cloud is onvermijdelijk
- Ken je echte afhankelijkheden
- Investeren in Europese alternatieven vraagt tijd
- We worden er beter van als er keuze is: maak van de cloudnood dus een deugd

**Geen besluiten nemen = besluiten nog afhankelijker te worden**

De huidige situatie is een gevolg van snelle technologie ontwikkeling die partijen met schaalgrootte een voorsprong heeft gegeven. Dit is geen eerlijke voorsprong. Microsoft kon investeren in hyperscale datacenters omdat wij windows en office licenties betaalden, Google omdat wij "googelen" en Amazon omdat wij online shoppen. De Amerikaanse overheid zou nooit op het idee komen een Europees bedrijf zo'n positie te geven, ook lang voordat MAGA de toon zette (de Buy American Act dateert van 1983).

Het boek "De vloek van Big Tech" geschreven door prof. Reijer Passchier benadrukt dat deze situatie niet eenvoudig te voorkomen was. Hyperscalers hebben met hun ongekende schaal en innovatiekracht een marktdominantie opgebouwd die moeilijk te evenaren is door Europese (laat staan Nederlandse) spelers. Het stelt de terechte vraag of je eigenaar bent als je een dienst afneemt die alleen blijft werken als deze online is en die door de aanbieder kan worden uitgezet. Ben ik eigenaar van mijn smartphone of huurder? Is de overheid eigenaar van haar voorzieningen of huurder?

Tegelijk is de scheefgroei in afhankelijkheid ook een gevolg van onze eigen besluiten over ICT. Jarenlang hebben we losse diensten aanbesteed met focus op "economisch meest voordelige keuze". Opgeteld betalen we de risico's daarvan samen. ICT-infrastructuur hebben we gezien als onbelangrijk, makkelijk vervangbaar en vrij verkrijgbaar in een open wereldmarkt. Dat hebben we ons wijs laten maken, want het is nooit het geval geweest. Het feit dat migraties van de ene naar de andere infrastructuur overheidsorganisaties regelmatig nachtmerries geeft, had ons alerter kunnen maken op de prijs van afhankelijkheid.

De grootste kosten zitten niet in migraties en een paar procent goedkopere infrastructuur contracten vormen maar een klein deel van ons budget. Het feit dat nieuwe ontwikkelingen vertragen en dat we legacy niet tijdig vervangen is veel kostbaarder. Dat betekent ook dat een overheid die nu concludeert dat ze gelukkig nog maar weinig (public) cloud gebruikt en voorlopig verder gaat met weinig cloudtechnologie besluit tot dure stilstand. Afgelopen jaren heeft deze stilstand ertoe geleid dat op allerlei plekken in organisaties in de praktijk toch de VS-hyperscale proposities gebruikt worden. Via allerlei SaaS diensten en recent op gebied van AI. Blijven zitten waar je zit is dus duur en leidt niet tot echte autonomie.

**Verwacht niks van één overheidscloud of Europa**

ICT infrastructuur is voor menigeen een saai en technisch onderwerp. Daarom is het aanlokkelijk de oplossing van buiten te verwachten. We hebben er niet genoeg verstand van, dus we besteden het uit. Inbesteden binnen de overheid bij een overheidsbrede eigen cloud is echter een nog slechter idee dan alles bij een Amerikaanse hyperscaler laten. De overheid is niet goed in het op grote schaal runnen van hoogwaardige technologie. Hoogwaardige dienstverlening door overheidsbrede shared servicecentra is buitengewoon weerbarstig. Dat neemt niet weg dat bestaande Overheidsdatacenters mee zullen moeten in de verandering; en daar zijn ze ook mee bezig. Het neemt ook niet weg dat we voor specifieke oplossingen in het veiligheidsdomein altijd oplossingen in eigen beheer willen. Die oplossingen zijn er en sommigen daarvan zijn gelukkig echt hoogwaardig genoeg. Dat wil echter niet zeggen dat één interne overheidscloud dé oplossing zou zijn. Te megalomaan, te moeilijk te organiseren in ons decentrale overheidsland. En vooral: de psychologie van het afschuiven van verantwoordelijkheid. Gelukkig vaart de staatssecretaris van BZK een meer op samenwerking met markt gerichte koers. Ook Europese oplossingen zijn geen vanzelfsprekende supertruc. Het is goed dat er EU-breed allerlei cloudinnovaties worden afgestemd en uitgedacht. Werkende oplossingen zullen we echter zelf moeten maken. Dit vereist een open samenwerking van overheid en marktpartijen gericht op maatschappelijke meerwaarde.

**Is soevereine cloud de oplossing? Slechts een beetje!**

Afgelopen jaar hebben de drie grote hyperscalers, hun opkomende concurrenten als Oracle en EU spelers hun public cloud diensten aangevuld met “soevereine” opties. Heel veel daarvan loopt stuk op de juridische kant. Als een buitenlands bedrijf verboden wordt deze diensten te leveren, dan blijft er een probleem. Veel grondigere scheiding van diensten is nodig om dit een echte oplossing te maken. Diverse Amerikaanse aanbieders zijn zich daarvan bewust en bewegen in die richting. De recente aankondiging van Microsoft dat ze Europese diensten verder gaat scheiden van de VS is veelzeggend. Microsoft gaat zo ver dat ze een kopie van haar software in Zwitserland stalt voor het geval dat en contractuele schadevergoeding belooft voor het delen van data tegen EU regels in. Dat zijn forse beloftes. In zekere zin kun je dat verstaan als bewijs dat de zorgen terecht zijn.  Wij zullen dat moeten gebruiken, simpelweg omdat alternatieven over de volle breedte niet snel genoeg voorhanden zijn en massaal overstappen geen kwestie van maanden, maar van jaren is. Met name op gebied van de werkplek geldt dat de Europese partij die M365 geheel autonoom – zo dat Microsoft het niet vanuit de VS uit kan zetten en geen data ziet – kan aanbieden snel een grote markt voor zich kan winnen; idemdito voor de partij die een andere werkplek aanbiedt die wij met nog meer werkplezier willen gebruiken.

**Je afhankelijkheid in kaart hebben en testen is een must**

Als wachten met besluiten geen optie is en soeverein aanbod slechts een beetje helpt, wat kan een overheidsorganisatie dan wel doen? Zorg dat je je eigen afhankelijkheden veel beter in kaart brengt! Vanuit risicomanagement en allerlei certificeringen zou iedere organisatie dat hoe dan ook moeten hebben; maar het kost moeite en gaat

niet vanzelf. Het gesprek hierover op ieder niveau van de organisatie, van developerteam, tot productteam tot directie is hoe dan ook een goed idee. Valkuil daarbij is om teveel energie te steken in minder belangrijke afhankelijkheden. Andere valkuil is dat we psychologisch allemaal dromen van autarkie, maar de werkelijkheid is dat supply chains ondanks de geo-politieke verschuivingen wereldwijd zijn en blijven. Voor de bewustwording zou je de volgende calamiteitenoefening zo kunnen opzetten dat geen enkel Microsoft product gebruikt kan worden en whatsapp uit staat. Het beeld zal zijn dat er nog veel meer afhankelijkheden zijn dan enkel die van VS-hyperscalers. VMware in het on premise datacenter kan bijvoorbeeld een dringender issue zijn. Als je de afhankelijkheden kent, kun je sturen.

**Keuzevrijheid is de koninklijke weg**

Afhankelijkheid is geen probleem als er alternatieven beschikbaar zijn. Dat moeten dan wel alternatieven zijn die in de praktijk snel voorhanden zijn. Zo niet dan kun je commercieel of omwille van politiek gegijzeld worden. Voor overheden dient dat onacceptabel te zijn. Keuzevrijheid kun je opbouwen door voor iedere belangrijke afhankelijkheid de vraag te stellen welk alternatief er is. Er zijn meestal meer alternatieven dan we op het eerste gezicht denken. Nederlandse en Europese bedrijven zijn veel beter in staat alternatieven te leveren dan op het eerste gezicht lijkt. Het moet hen wel gevraagd worden! En omdat zij geen hyperscale hebben om wispelturigheid mee op te vangen, vraagt het van overheden dat ze niet te vaak van gedachte veranderen en betrouwbare contractpartij zijn. Het zal een aantal jaren werk zijn, maar “never waste a good crisis”. Het bepalen van alternatieven leidt tot creativiteit en zou wel eens allerlei onverwachte baten boven tafel kunnen krijgen. Maak van de nood een deugd!

## Over de auteurs

**Nieradj Gopal**
**Digitale strategie**

Nieradj is ervaren in het leiden en ondersteunen van digitale transformaties binnen zowel publieke als private organisaties. Hij begeleidt initiatieven van concept tot realisatie, met oog voor samenhang tussen strategische, tactische en operationele niveaus.

nieradj.gopal@capgemini.com

https://www.linkedin.com/in/nieradj-gopal-4ba53687/

**Michael Stoelinga**
**Chief Architect Public Sector**

Sinds zijn eerste e-mail in 1990 houdt de impact van internet op de maatschappij Michael bezig. Zijn 30 jaar ervaring met digitalisering van de overheid benut hij om richting te geven vanuit visie, de volgende stap concreet te maken en waar nodig de status quo in vraag te stellen.

michael.stoelinga@capgemini.com

linkedin.com/in/mstoelinga

08

# Van duizend bloemen bloeien naar planten met voorbedachten rade: hoe schaalbare en wendbare innovaties het veiligheidsdomein verder helpen

## Hoe dragen schaalbare en wendbare innovaties bij aan een toekomstbestendig veiligheidsdomein?

**De wereld waarin het veiligheidsdomein opereert, is snel veranderend en turbulent. Externe factoren zoals geopolitieke spanningen en de dreiging van cyberaanvallen, terrorisme en georganiseerde misdaad vergroten de veiligheidsrisico's voor Nederland . Interne factoren zoals een tekort aan personeel bij bijvoorbeeld Defensie belemmeren snelle reacties op dreigingen . Dit vraagt om wendbare en effectieve innovaties. Echter, ongeveer 70% van de innovaties faalt.  Dit benadrukt de noodzaak voor een gedegen innovatie aanpak des te meer. Om innovatie in een turbulente omgeving te doen slagen, is wendbaarheid en opschaling als vaardigheid cruciaal.**

Een manier om te innoveren, is het bieden van ruimte aan de diversiteit aan initiatieven, geïnspireerd op het "duizend bloemen bloeien"-concept. Deze benadering stimuleert creativiteit en experimenteren om innovaties te laten opbloeien. Dit concept wordt bijvoorbeeld ook bij de Q-teams van de Politie toegepast. Echter, de veranderende maatschappelijke behoeften, verhogen de noodzaak om effectief te innoveren binnen veiligheidsorganisaties zoals Defensie en de Politie. Dit vraagt om een vervolg op het "duizend bloemen bloeien"-concept: het opschalen van geselecteerde innovatietrajecten, in lijn met de doelstellingen van de organisatie.

Het veiligheidsdomein is breed en kent uiteenlopende organisaties, van de Raad voor de Rechtspraak tot Defensie, met ieder met haar eigen uitdagingen. Dit artikel is met name relevant voor organisaties uit het veiligheidsdomein die worstelen met gedegen opschaling van innovaties, ongeacht het doel van deze organisatie. Uit onderzoek van het Capgemini Research Institute blijkt dat veel organisaties het succesvol opschalen van innovaties een uitdaging vinden. In dit artikel staan we kort stil bij de oorzaak hiervan, hoe wendbaarheid zich hiertoe verhoudt, en wordt 'outside-in' denken gestimuleerd door stil te staan bij relevante praktijkvoorbeelden uit andere domeinen.

Het omarmen van 'outside-in' denken helpt bij het vergroten van wendbaarheid en schaalbaarheid van innovaties . Dit betekent dat organisaties niet alleen interne processen en technologieën

## Highlights

- Toekomstbestendige innovatie in het veiligheidsdomein vraagt om een strategische aanpak waarin creativiteit, wendbaarheid en doelgerichte opschaling samenkomen om echte impact te realiseren
- Het “duizend bloemen bloeien”-concept stimuleert creativiteit, maar effectieve innovatie vereist ook gerichte selectie en strategische opschaling van kansrijke initiatieven
- Opschaling moet al in de beginfase van innovatie worden meegenomen als aparte discipline, niet pas aan het eind van het proces
- Organisatorische wendbaarheid helpt bij het succes van innovatie, doordat het organisaties in staat stelt om snel te reageren, effectief bij te sturen en continu te leren in een steeds veranderende omgeving
- ‘Outside-in’ denken en het toepassen van best practices uit andere sectoren kan innovatiekracht en veerkracht versterken

verbeteren, maar ook leren van externe belanghebbenden. Door inzichten van burgers, bedrijven en andere overheidsorganisaties in te winnen, kunnen veiligheidsinstanties hun strategieën en werkwijzen afstemmen op de daadwerkelijke behoeften van de samenleving. Dit creëert niet alleen een effectieve respons op actuele dreigingen, maar bevordert ook een cultuur van samenwerking en continue verbetering. Zo kunnen organisaties met een outside-in aanpak sneller inspelen op externe risico’s en beter anticiperen op nieuwe ontwikkelingen in de samenleving.

### Het ‘Duizend Bloemen Bloeien’-concept en de trend naar wendbare en schaalbare innovatieprojecten

Het “duizend bloemen bloeien” concept houdt in dat er diverse innovatieve ideeën en projecten worden gestart zonder een vooraf doordachte, overkoepelende strategie. In de natuur werkt dit concept goed. Onze ecosystemen zijn op deze manier groot en zelfvoorzienend geworden doordat er natuurlijke selectie plaatsvindt. Echter, in geval van talloze innovatieprojecten, gaat deze natuurlijke selectie niet vanzelf. Hier zijn selectie en opschaling van de juiste projecten, sterke strategische kaders, een visie en duidelijke operationalisering van het beleid voor nodig. Juist in dynamische tijden is naast schaalbaarheid ook wendbaarheid van innovaties cruciaal om in te kunnen blijven spelen op de veranderende omgeving.

De behoefte naar een gedegen proces voor schaalbare en wendbare innovatie initiatieven is dus groot. Een succesvol innovatieproces begint al voor de start van een project, met het creëren van een stevig en gedragen fundament samen met de belangrijkste belanghebbenden. Dit kan bijvoorbeeld door het organiseren van een kick-off sessie voorafgaand aan de start van het project met deze belanghebbenden in één ruimte. Hier wordt besloten over de te bereiken doelen, richtinggevende pijlers zoals wendbaarheid, schaalbaarheid en haalbaarheid, de verwachtingen, mogelijke risico’s etc. Het innovatieproces start dus al voorafgaand aan de start van een project en itereert door totdat succesvolle borging in de organisatie is bewerkstelligd of besloten wordt het initiatief te stoppen. Dit kan bijvoorbeeld omdat het iniatief niet meer voldoet aan de vereisten om door te mogen naar een vervolgfase in het innovatieproces.

Uit onderzoek van Capgemini research Institute, blijkt dat organisatiecultuur een van de grootste uitdagingen is om innovatie op te schalen. De capaciteit om barrières en problemen aan te pakken, moet vanuit bestuur en topmanagement naar de hele organisatie doorstromen en dit ontbreekt vaak. Het rapport ontdekte dat, onder de organisaties die succesvol hun innovaties opschalen, er bereidheid is om de experimenten en innovaties waar nodig te beëindigen, om ruimte te maken voor opschaling en het proberen van nieuwe dingen. Dit betreft dus de volgende stap in het proces, die zich afspeelt na de ‘Duizend bloemen bloeien’-aanpak. Een sprekend praktijkvoorbeeld uit de publieke sector, is er een waar snelle, wendbare besluitvorming mogelijk gemaakt wordt door het organiseren van wekelijkse (digitale) inloopspreekuren. Tijdens deze spreekuren kunnen bestuursleden suggesties ontvangen voor procesverbeteringen en innovatiekansen van iedereen in de organisatie. Ook kunnen snel knopen worden doorgehakt door het bestuur wanneer men vastloopt op bepaalde innovatietrajecten. Deze manier van besluitvorming vergroot wendbaarheid van de organisatie. Enerzijds doordat er snelle stappen in het innovatieproces gemaakt kunnen worden, anderzijds door het wekelijks signaleren van innovatiekansen vanuit de organisatie.

Opschaling creëert niet alleen meer waarde, maar zorgt ook voor efficiënter gebruik van middelen. Waar veel organisaties het opschalen en inbedden van innovaties als uitdaging zien, is dit juist het moment waarop de echte impact ontstaat. Ditzelfde geldt voor Defensie. Defensie wil groeien van 75.000 naar 200.000 medewerkers in 2030, ondanks beperkte opleidingscapaciteit. Deze ambitie weerspiegelt een bredere uitdaging: ook innovatieve ideeën moeten snel en effectief opgeschaald worden om bij te dragen de benodigde operationele slagkracht. Het heikel punt rond opschalen zit vaak in het feit dat er niet aan schaalvergroting als op zichzelf staande discipline wordt gedacht. Uit onderzoek van het Capgemini Research Institute blijkt dat veel organisaties geen onderscheid maken tussen het genereren van innovaties en het opschalen ervan.

Hoewel opschalen later in het innovatieproces plaatsvindt, moet de

beoordeling en planning ervan veel eerder in het proces beginnen. Een interessant voorbeeld uit de praktijk van sterk zijn in opschalen van innovaties, komt vanuit een totaal ander speelveld dan het veiligheidsdomein: succesvolle platform scale-up bedrijven, zoals Just Eat Takeaway. Uit onderzoek blijkt dat managers in deze type organisaties succesvol opschalen door het gebruiken en actualiseren van een gedefinieerde set van eenvoudige beslissingsregels. Deze regels stellen de organisatie in staat om kansen te selecteren en vast te leggen die helpen om naar opschaling over te gaan.

De dynamiek waarin het veiligheids-domein zich momenteel bevindt, maakt het vermogen om effectief en wendbaar te innoveren essentieel voor het waarborgen van de veiligheid in Nederland. Het “duizend bloemen bloeien”-concept biedt een vruchtbare bodem voor creativiteit en experimenten, maar de echte uitdaging ligt in het gericht opschalen van succesvolle innovaties met voorbedachten rade planten in plaats van toevallig laten groeien. Dit vereist een stevig fundament waarmee innovatie structureel wordt verankerd in de organisatie. Een strategische innovatieagenda helpt met richting geven aan innovatie-inspanningen en verbindt ze met de langetermijnvisie. Daarnaast kan een innovatieboard helpen om ideeën systematisch te beoordelen en prioriteren, op basis van vooraf vastgestelde criteria die passen bij de missie en ambities van de organisatie.

Een gefaseerde aanpak, zoals een stage-gate model, maakt het mogelijk om innovaties in verschillende stadia te toetsen op haalbaarheid, impact en strategische relevantie. Tegelijkertijd vraagt deze aanpak om een cultuur van samenwerking, leren en externe oriëntatie. Door actief te leren van andere organisaties, ook buiten de eigen sector, vergroten veiligheidsorganisaties hun wendbaarheid en innovatiekracht. Dit stelt hen in staat om snel te reageren op acute uitdagingen, experimenten bij te sturen of stop te zetten, en succesvolle initiatieven op te schalen — ondanks beperkte middelen.

Het is deze combinatie van strategische verankering, schaalbaarheid, wendbaarheid en een open blik naar buiten die de sleutel vormt tot veerkrachtige en toekomstbestendige innovatie. Alleen zo blijven we voorbereid op de complexe en snel veranderende uitdagingen van morgen.

## Over de auteurs

**Rosanne Holtendorp**
Consultant

Rosanne is gespecialiseerd in strategich innovatie management in de (semi)-publieke sector waarbij maatschappelijke waarde creëren centraal staat.

rosanne.holtendorp@frog.co

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

**Karlijn Meijer**
Senior Consultant

Karlijn is gespecialiseerd in schaalbare strategisch innovaties, vanuit o.a. haar ervaring met start-ups.

karlijn.meijer@capgemini.com

https://www.linkedin.com/in/karlijn-meijer/

**Teddy van Eijk**
Senior Consultant

Teddy is gespecialiseerd in het snijvlak van strategie en innovatiemanagement waarbij in gezamenlijkheid doelgericht innoveren centraal staat.

teddy.van.eijk@frog.co

https://www.linkedin.com/in/teddy-van-eijk/

Bronnen

[1] https://www.nctv.nl/actueel/nieuws/2024/06/25/trendanalyse-nationale-veiligheid-2024-stapeling-van-dreigingen-in-onzekere-tijden?

[2] https://www.nu.nl/economie/6314743/defensie-strijdt-verder-tegen-personeelstekort-met-7-procent-extra-salaris.html

[3] https://www.consultancy.nl/nieuws/32270/95-van-corporate-tech-innovaties-sneuvelt-nog-voor-lancering?utm_source=chatgpt.com

[4] De politie onderweg naar toekomstbestendige opsporing en vervolging? (2020). P. van Egmond, A. Swami-Persaud, A. Verwest Politiekunde 105, Q-teams | Politie en Wetenschap

[5] Nederlands leger moet veel groter: defensie wil groeien naar 200.000 medewerkers

[6] Capgemini Research Institute. (2020) What's the big idea? Why innovations fail to scale and what to do about it?.

[7] https://www.researchgate.net/publication/352294628_Preparing_Organizations_for_Greater_Turbulence

[8] Defensie wil snel en veel mensen aantrekken, maar mist opleidingsplekken

[9] Nederlands leger moet veel groter: defensie wil groeien naar 200.000 medewerkers

[10] Capgemini Research Institute. (2020) What's the big idea? Why innovations fail to scale and what to do about it?.

[11] Varga, S., Cholakova, M., Jansen, J., Mom, T., & Kok, G. (2023). From platform growth to platform scaling: The role of decision rules and network effects over time. Journal of Business Venturing, 38(6), Article 106346. https://doi.org/10.1016/j.jbusvent.2023.106346

# Wendbaarheid

**Tom Eskens**

Transitiemanager bij de Raad voor Rechtsbijstand

Interview:

# Een wendbaar IT-landschap om de rechtzoekende te helpen

De samenleving digitaliseert in hoog tempo en organisaties moeten zich aanpassen om effectief en efficiënt te blijven functioneren. Dit geldt ook voor de Raad voor Rechtsbijstand (de Raad). De Raad is in onze democratische rechtsstaat verantwoordelijk voor de optimale organisatie en het borgen van goede gesubsidieerde rechtsbijstand en mediation voor minder draagkrachtige burgers. Daarnaast voert de Raad (een deel van) de Wet schuldsanering natuurlijke personen en de Wet beëdigde tolken en vertalers uit. De Raad bevindt zich middenin een transitie om de dienstverlening toegankelijker, wendbaarder en toekomstbestendig te maken. Tom Eskens, transitiemanager bij de Raad, deelt zijn visie op de belangrijkste trends, uitdagingen en innovaties binnen het juridische domein.

### Digitalisering van juridische dienstverlening

De verwachting van rechtzoekenden verandert snel. Waar vroeger contact per post met een advocaat of juridische hulpverlener de norm was, is nu steeds meer behoefte aan digitale middelen zoals videobellen, online formulieren en data-gestuurde juridische hulp. Daarbij is het IT-landschap van de Raad flink verouderd waardoor de organisatie niet meer kan voldoen aan de huidige dienstverleningsstandaarden en wet- en regelgeving. Eskens: “Nog niet alle aanvragen van advocaten en mediators kunnen nu digitaal worden ingediend. Veel verloopt nog via de post. Daarna communiceren we met de rechtzoekende alles per post. Dit past niet meer in de huidige tijd.” Dit vraagt van de Raad een andere benadering van dienstverlening en infrastructuur. “We zien dat steeds meer burgers en rechtzoekenden verwachten dat zij digitaal zaken kunnen regelen. Digitalisering biedt kansen om rechtsbijstand toegankelijker te maken. Het brengt alleen ook obstakels met zich mee. Niet alle rechtzoekenden beschikken over de digitale vaardigheden of middelen om online juridische rechtsbijstand te zoeken en verkrijgen. We moeten ervoor zorgen dat digitalisering niet leidt tot een kloof tussen mensen die digitaal vaardig zijn en zij die dat niet zijn. Toegankelijkheid betekent ook dat er altijd een menselijke ondersteuning beschikbaar moet zijn voor wie dat nodig heeft”, licht Eskens toe. Daarom kijkt de Raad naar hybride modellen waarin digitale en fysieke dienstverlening elkaar aanvullen.

### Veranderende rol van de overheid

Een andere uitdaging voor de Raad is de veranderende wet- en regelgeving. Nieuwe wetgeving kan grote gevolgen hebben voor de manier waarop de Raad zijn diensten aanbiedt en hoe rechtsbijstandverleners te werk gaan. De Raad moet processen en systemen voortdurend actualiseren en tegelijkertijd zorgen dat rechtsbijstandverleners de rechtzoekenden op de hoogte blijven van nieuwe juridische richtlijnen, procedures en zorgdragen dat met de toevertrouwede informatie veilig wordt omgegaan. Dit vereist een flexibele en snel aanpasbare organisatie die tijdig inspeelt op veranderingen zonder dat de dienstverlening hieronder lijdt. Eskens: “De overheid transformeert van een uitvoerende instantie naar een meer regisserende rol, waarbij digitale hulpmiddelen een steeds grotere rol spelen in de rechtsbijstand. Dit vereist meer samenwerking met ketenpartners. Wij moeten ons hierop voorbereiden

door ons flexibel op te stellen en te anticiperen op nieuwe wetgeving en beleidsontwikkelingen."

Om hierop in te spelen, zoekt de Raad naar innovatieve manieren om juridische hulp efficiënter te maken zonder dat de kwaliteit in het geding komt. "We moeten kijken naar hoe technologie ons kan helpen om processen te versnellen, zonder dat rechtzoekenden zich verloren voelen in een systeem dat steeds abstracter wordt", aldus Eskens.

**Complexiteit van juridische problemen**

Het juridische landschap wordt dus steeds complexer. Maar de dienstverlening moet eenvoudig blijven. Eskens: "In essentie verandert de dienstverlening niet. Iemand heeft rechtsbijstand nodig, die wordt aangevraagd, toegekend, verleend, en betaald. De Raad werkt samen met eerstelijnsorganisaties zoals het Juridisch Loket en Rechtswinkels. Binnen de eerstelijns wordt altijd directe rechtshulp geboden. Is er sprake van tweedelijnsrechtsbijstand, dus inschakeling van een advocaat of mediator, dan zorgt de Raad daarvoor. Op basis van de hulpvraag matcht de Raad rechtzoekende aan de best passende advocaat of mediator. Maar het toegankelijk en eenvoudig houden, daar ligt een groot deel van onze uitdaging."

**De burger in het hart van de organisatie**

De Raad voor Rechtsbijstand stelt de burger centraal in zijn dienstverlening. Volgens Eskens is dit een fundamenteel uitgangspunt voor alle toekomstige ontwikkelingen. "We willen dat rechtzoekenden snel en eenvoudig toegang hebben tot juridische bijstand. Dit betekent dat we moeten kijken naar gebruiksvriendelijke, toegankelijke communicatiekanalen en slimme IT-oplossingen die complexe vragen aankunnen." Digitale toegankelijkheid is cruciaal. Eskens: "Denk aan zelfhulpmodules, chat en online aanvraagprocedures. Daarnaast willen we papieren oplossingen behouden voor de burgers die minder digivaardig zijn. Wendbaarheid betekent ook dat we altijd alternatieven moeten blijven bieden. Traditionele vormen van dienstverlening zullen daarom niet verdwijnen.

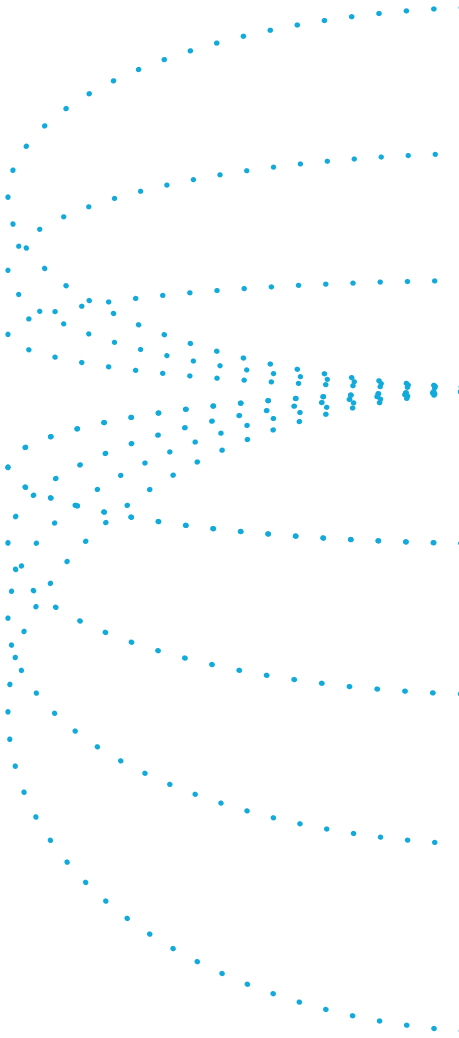
**Wendbaarheid in een digitale samenleving**

Om de veranderende samenleving optimale dienstverlening te blijven bieden, herziet de Raad zijn IT. "Onze systemen moeten flexibel genoeg zijn om in te spelen op veranderingen in wetgeving en technologie. Daarbij moeten we ook zorgen voor veiligheid en betrouwbaarheid in onze digitale dienstverlening," aldus Eskens. Om dit te bereiken is de Raad bezig met een grootschalige herziening van de IT-systemen. "We werken toe naar een modulair systeem dat eenvoudiger aanpasbaar is aan nieuwe wetgeving en maatschappelijke ontwikkelingen. Dit voorkomt dat we elke paar jaar tegen een grote en dure systeemvervanging aanlopen. Een groot aandachtspunt hierbij is de cybersecurity van de systemen. Eskens: "Met de toenemende cyberdreigingen is het essentieel dat onze systemen niet alleen wendbaar zijn, maar ook bestand tegen aanvallen. We moeten voorkomen dat gevoelige juridische informatie in verkeerde handen valt." Daarnaast zoekt de Raad naar manieren om processen efficiënter te maken zonder dat dit ten koste gaat van de kwaliteit. "Zo kunnen we bijvoorbeeld gebruikmaken van geautomatiseerde besluitvorming voor eenvoudige juridische vragen met een positief besluit, terwijl complexere zaken doorgeschakeld worden naar een professional die de zaak uitgebreider onderzoekt. De eenvoudige zaken kunnen automatisch goedgekeurd worden zodat de burger niet lang hoeft te wachten."

**Toekomstbestendigheid en flexibiliteit**

Wat betekent wendbaarheid voor de toekomst van de Raad voor Rechtsbijstand? Eskens: "Het gaat erom dat we blijven anticiperen op maatschappelijke en technologische veranderingen. We willen een organisatie zijn die snel en adequaat reageert op nieuwe behoeften en uitdagingen. Dit vereist een flexibele IT-infrastructuur, maar ook een cultuur van innovatie. We moedigen onze medewerkers aan om mee te denken over verbeteringen en nieuwe manieren van werken. Wendbaarheid zit niet alleen in systemen, maar vooral in mensen."

"We willen als organisatie niet alleen reactief zijn, maar ook proactief bijdragen aan het verbeteren van de toegang tot het recht. Dit betekent dat we voortdurend in gesprek zijn met partners, innovatie stimuleren en experimenteren met nieuwe methoden. Maar het belangrijkste is dat rechtsbijstand toegankelijk blijft voor iedereen, ongeacht technologische of maatschappelijke veranderingen. Dat is onze uitdaging, maar vooral onze verantwoordelijkheid."



09

# Stop de Sabotage: Bouw Nationale Hybride Weerbaarheid op bestaande cybersecurity-initiatieven

## Hoe kunnen we de bestaande blauwdruk voor cyberweerbaarheid inzetten om ons beter te beschermen tegen het volledige spectrum van hybride dreigingen?

**Dit artikel bespreekt hoe bestaande cyberweerbaarheidsinitiatieven, zoals het Cyberweerbaarheidsnetwerk en het Nationaal Detectie Netwerk, kunnen worden uitgebreid om hybride dreigingen beter te bestrijden.**

### Highlights

- Hybride dreigingen combineren digitale en fysieke aanvallen
- Cyberweerbaarheidsnetwerk kan breder ingezet worden voor hybride dreigingen
- Integratie van fysieke en digitale monitoring is cruciaal
- Samenwerking met veiligheidsinstanties versterkt dreigingsdetectie
- Bestaande technologieën kunnen hybride dreigingen effectief detecteren

Hybride dreigingen vormen een groeiende uitdaging voor nationale en internationale veiligheid. Waar de focus tien jaar geleden nog lag op het beschermen van digitale systemen tegen ransomware en datalekken, is het dreigingslandschap inmiddels veel breder geworden. Risico's beperken zich niet langer tot IT-systemen, maar raken steeds vaker ook fysieke, economische en informatieve domeinen, met potentieel ontwrichtende gevolgen voor de samenleving.

Recente incidenten onderstrepen die ontwikkeling. Zo werd een politienetwerk langdurig geïnfiltreerd zonder detectie1, en werden stroom- en glasvezelkabels op de bodem van de Oostzee doelwit van sabotage2. Ook Nederland is kwetsbaar: onze samenleving leunt sterk op onderzeese kabels en pijpleidingen, waarvan de beveiliging nog verre van sluitend is3. Zulke aanvallen zijn typerend voor hybride oorlogsvoering, waarbij digitale aanvallen worden gecombineerd met fysieke sabotage of desinformatie om maximale maatschappelijke ontwrichting te veroorzaken.

De Adviesraad Internationale Vraagstukken (AIV) pleit daarom terecht voor een integrale strategie, waarin overheid, bedrijfsleven en kennisinstellingen nauwer samenwerken4. Maar in plaats van nieuwe structuren van de grond af op te bouwen, zou Nederland moeten voortbouwen op wat er al is.

De afgelopen jaren zijn er immers grote stappen gezet op het gebied van cybersecurity. De aanpak die daar is ontwikkeld – van netwerken tot detectiecapaciteit – biedt een waardevolle blauwdruk voor een bredere weerbaarheid tegen hybride dreigingen. In dit artikel laten we zien hoe bestaande initiatieven, zoals het Cyberweerbaarheidsnetwerk en het Nationaal Detectie Netwerk, kunnen dienen als fundament voor een toekomstbestendige aanpak.

**Cyberweerbaarheidsnetwerk (CWN) als Hybride Weerbaarheidsnetwerk**

Het Cyberweerbaarheidsnetwerk (CWN), de opvolger van het Landelijk Dekkend Stelstel (LDS), vormt een samenwerkingsverband dat zich primair richt op het versterken van de cyberweerbaarheid binnen de hightech- en industriële sector5. Het netwerk faciliteert de uitwisseling van dreigingsinformatie en biedt bedrijven en instanties een platform om gezamenlijk cyberrisico's te verminderen. Wanneer de infrastructuur van het CWN op de juiste manier wordt uitgebreid, kan het een leidend platform zijn bij de digitale beveiliging, maar ook in de bredere context van hybride dreigingen worden ingezet.

Hybride dreigingen kenmerken zich door een combinatie van digitale aanvallen, fysieke sabotage en desinformatiecampagnes6. Een cyberaanval kan bijvoorbeeld gepaard gaan met een verstoring van kritieke infrastructuur, zoals het doorsnijden van internetkabels of het saboteren van stroomnetwerken. Nu focust het LDS voornamelijk het delen van digitale dreigingsinformatie, maar vraagt de aanpak van moderne hybride dreigingen een aanzienlijk bredere opzet van zo'n netwerk en stelt het specifieke eisen aan de inrichting. Het CWN zal naar verwachting al significant beter voor dit doeleinde geschikt zijn.

Het CWN biedt in de nabije toekomst een structuur waarin dreigingsinformatie snel en effectief gedeeld kan worden, waarbij het netwerk het meest effectief is, wanneer het is aangepast aan de bredere veiligheidsdimensie. Door nauwer samen te werken met fysieke veiligheidsinstanties en departementen van inlichtingendiensten, die over meer inzichten beschikken dan alleen digitale dreigingsinformatie, kan het CWN transformeren tot een breed inzetbaar dreigingsinformatie-platform. Dit vraagt om een geïntegreerde aanpak waarin digitale en fysieke monitoring worden gecombineerd en waarin niet alleen cyberaanvallen, maar ook bijvoorbeeld sabotage en desinformatie worden gesignaleerd en geanalyseerd.

Het benutten van het CWN voor hybride dreigingsinformatie heeft duidelijke voordelen. Het netwerk biedt al een functionerend model voor samenwerking en informatie-uitwisseling, waardoor nieuwe structuren niet vanaf de grond hoeven te worden opgebouwd. Dit bespaart tijd en middelen en voorkomt versnippering van initiatieven. Daardoor kan een uitbreiding van het CWN bijdragen aan snellere respons en betere coördinatie tussen verschillende sectoren in het geval van een hybride aanval waar meerdere methodes tegelijk worden gebruikt.

Tegelijkertijd brengt deze uitbreiding uitdagingen met zich mee. Het CWN is oorspronkelijk opgezet met een focus op cyberveiligheid en mist op dit moment de multidisciplinaire expertise die nodig is om fysieke dreigingen en desinformatie adequaat te verwerken. Daarnaast vereist een bredere taakstelling extra middelen en betrokkenheid van partners buiten de huidige scope van het netwerk. Als deze bredere taakstelling niet zorgvuldig wordt ondersteund met extra middelen en expertise, bestaat het risico dat de kernfunctie van het CWN, cyberweerbaarheid, verzwakt raakt doordat het netwerk overbelast raakt en onvoldoende focus kan behouden.

Ondanks deze uitdagingen biedt het CWN een solide basis voor de aanpak van hybride dreigingen. Door zorgvuldige aanpassingen en samenwerking met andere veiligheidsinstanties kan het netwerk uitgroeien tot een essentieel instrument in de bescherming tegen de steeds complexer wordende dreigingsomgeving.

**Het Nationaal Detectie Netwerk als Hybride Detectie Netwerk**

Een effectieve respons op hybride dreigingen vraagt om een fundamentele verbreding van het bestaande cybersecuritybeleid. Waar dreigingen tot voor kort vooral digitaal van aard waren, zien we steeds vaker dat digitale aanvallen gecombineerd worden met fysieke sabotage van cruciale infrastructuur. In dit veranderende dreigingslandschap is het tijdig beschikken over de juiste informatie, uit zowel digitale als fysieke bronnen, essentieel om adequaat te kunnen reageren en schade te beperken.

Het Nationaal Detectie Netwerk (NDN), een samenwerkingsverband van NCSC, AIVD en MIVD, speelt hierin een sleutelrol. Binnen dit netwerk worden digitale sensoren ingezet bij aangesloten organisaties om vroegtijdig indicatoren van compromittering te signaleren . Deze digitale monitoring biedt een belangrijke eerste verdedigingslinie en vormt een onmisbare bouwsteen in de Nederlandse Cybersecurity Strategie 2022–2028 . Toch is het de vraag of deze digitale aanpak nog volstaat in een tijd waarin de grenzen tussen cyberaanvallen en fysieke dreigingen vervagen.

Aanvallen beperken zich steeds minder tot het binnendringen van IT-netwerken; sabotage van onderzeese datakabels, verstoringen in de energievoorziening of onopgemerkte ingrepen in spoor- en waterinfrastructuur zijn reële scenario's geworden . Om de weerbaarheid tegen dit soort hybride dreigingen te versterken, is uitbreiding van het huidige detectienetwerk naar de fysieke wereld noodzakelijk. Een logisch vervolg zou zijn om het Nationaal Detectie Netwerk te transformeren tot een Hybride Detectie Netwerk: een geïntegreerd systeem waarin niet alleen digitale maar ook fysieke sensoren een plaats krijgen.

In zo'n systeem zouden sensoren kunnen worden geplaatst langs kwetsbare schakels in onze samenleving, zoals bij onderzeese datakabels, hoogspanningsstations, spoorwegen, bruggen en drinkwatervoorzieningen. Deze sensoren kunnen afwijkingen registreren in bijvoorbeeld trillingen, drukveranderingen, temperatuur of chemische samenstellingen, en daarmee vroegtijdig signalen van sabotage of voorbereidende handelingen detecteren. Cruciaal daarbij is dat deze sensoren in realtime gekoppeld worden aan bestaande meldstructuren, zodat signalen direct kunnen worden geanalyseerd in samenhang met digitale dreigingsinformatie.

Technologische oplossingen voor deze verbreding zijn geen toekomstmuziek: ze bestaan al en worden wereldwijd steeds vaker ingezet. Zo maken innovatieve detectiesystemen zoals Distributed Acoustic Sensing het mogelijk om via bestaande glasvezelkabels zeer nauwkeurig trillingen en verstoringen in de directe omgeving van onderzeese infrastructuren te detecteren . Ook condition monitoring-systemen controleren continu parameters zoals stroomdoorvoer, temperatuur en spanning binnen kabels, waardoor afwijkingen – Zoals een beginnende of lopende sabotage– in een vroeg stadium kunnen worden vastgesteld . Daarnaast zijn er modulaire sensortechnologieën die onderzees of langs vitale knooppunten in het elektriciteits- en spoornetwerk geplaatst kunnen worden om fysieke aantastingen real-time te signaleren. Deze technologieën maken het mogelijk om afwijkingen of verdachte situaties onmiddellijk te koppelen aan centrale meldpunten, en zo sabotage of grootschalige verstoringen tijdig te herkennen en te duiden. Het uitbreiden van het Nationaal Detectie Netwerk naar een Hybride Detectie Netwerk is daarmee geen futuristisch idee, maar een noodzakelijke en realistische stap om Nederland ook in het tijdperk van hybride dreigingen weerbaar te houden.

### Van aparte silo's naar geïntegreerde weerbaarheid

De hybride dreiging vraagt niet alleen om nieuwe technologie, maar vooral om een andere manier van denken over veiligheid. De traditionele scheidslijn tussen digitaal en fysiek vervaagt – en daarmee ook de effectiviteit van gescheiden beveiligingsstructuren. De Nederlandse cybersecurity-infrastructuur biedt al waardevolle bouwstenen, maar heeft uitbreiding en integratie nodig om ook de fysieke dimensie van moderne dreigingen te adresseren. Door het Cyberweerbaarheidsnetwerk en het Nationaal Detectie Netwerk strategisch uit te breiden en beter te koppelen aan andere veiligheidspartijen, kan Nederland een robuust en toekomstbestendig Hybride Detectie Netwerk realiseren. De technologie is beschikbaar, de urgentie is hoog – nu is het tijd voor actie.

## Over de auteurs

**Koen de Wolf**
**Cybersecurity Consultant – Risk, Strategy & Compliance**

Koen houdt zich binnen zijn opdracht bezig met implementatie van de NIS 2 bij de Nederlands Spoorwegen. Daarnaast heeft hij recent een MA in Militaire Strategische Studies afgerond aan de NLDA.

koen.de.wolf@capgemini.com

https://www.linkedin.com/in/koen-de-wolf-57b79b1aa/

**Pim Kruijver**
**Managing Cybersecurity Consultant GRCS**

Pim is werkzaam bij de Cyber Security Unit. Hij is zeer ervaren en kundig bij het geven van strategisch advies op het gebied van risicobeheersing, compliance aan diverse normenkaders en de aanpak van het proces informatiebeveiliging in organisaties. Momenteel werkt hij als Quality Assurance functionaris aan het beheersen van informatiebeveiligingsrisico's bij het Openbaar Ministerie.

pim.kruijver@capgemini.com

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

Bronnen

1. https://www.politie.nl/nieuws/2024/november/8/stand-van-zaken-onderzoek-en-veiligheidsmaatregelen-datalek-politie.html
2. https://nos.nl/artikel/2553366-onderzeekabel-in-oostzee-beschadigd-door-invloed-van-buitenaf
3. https://hcss.nl/news/nieuwsuur-hoe-kwetsbaar-zijn-kabels-en-pijpleidingen-in-de-noordzee/
4. https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid
5. https://open.overheid.nl/documenten/dpc-ad1d121da28d29b90dc746ce5281962fbada6cf0/pdf
6. https://www.nctv.nl/documenten/rapporten/2019/04/18/duiding-fenomeen-hybride-dreiging
7. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/nationaal-detectie-netwerk-infosheet
8. https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028/pijler-iii-tegengaan-van-digitale-dreigingen-van-staten-en-criminelen
9. https://www.adviesraadinternationalevraagstukken.nl/documenten/publicaties/2024/06/04/hybride-dreigingen-en-maatschappelijke-weerbaarheid
10. https://www.tno.nl/nl/newsroom/2024/06/tno-ontwikkelt-detectiesysteem-noordzee/
11. Hier een relevant voorbeeld van condition monitoring immplementatie door Capgemini bij een klant in de energiesector: https://www.capgemini.com/news/client-stories/integrated-monitoring-solution-helps-major-energy-company-increase-safety-and-profitability/


# Data

## Merle Zwiers

Chief Data Officer bij het Ministerie van Defensie

Interview:

# Digitale transformatie moet ons kloppend hart worden

De opkomst van AI en een razendsnelle veranderende geopolitieke situatie: de omgeving van Merle Zwiers wordt met de dag dynamischer. Als Chief Data Officer bij het ministerie van Defensie houdt ze zich bezig met vraagstukken rondom autonome systemen, nieuwe eisen aan de data-infrastructuur en de verantwoordelijkheden rondom datagedreven beslissingen die soms binnen 20 seconden moeten worden gemaakt.

Vraag Merle Zwiers wat de belangrijkste ontwikkelingen zijn in haar werkveld, dan staat generatieve AI met stip bovenaan. Zwiers: “Die ontwikkeling gaat razendsnel en is niet meer weg te denken. Het maakt ons werk gemakkelijker en effectiever, denk aan het optimaliseren van onze logistieke ketens en het voorspellen van onderhoud. En met DefGPT kijken we bijvoorbeeld hoe we Kamerbrieven sneller kunnen schrijven. Daarnaast zijn er uiteraard talloze toepassingen in het militaire domein.”

Daarover straks meer. Als tweede noemt ze cybersecurity: “We zien steeds meer digitale dreigingen en een combinatie van cyber en AI, en we kunnen het ons niet veroorloven hierin achter te blijven. Een derde ontwikkeling is de rol van grote techbedrijven en de AI-ontwikkelingen die ze op de markt brengen. Hoe moeten we daarmee omgaan? Alle grote AI-doorbraken brengen kansen maar ook risico’s met zich mee: afhankelijkheid, vendor lock-in en kwetsbaarheid wat betreft informatie.”

### AI en desinformatie als tactische wapens

“Onze focus ligt op het verantwoord inzetten van AI binnen heldere kaders, met als doel Defensie effectiever te laten opereren. AI wordt dus vooral gebruikt om onze taken beter en sneller te kunnen uitvoeren. Dat sluit aan bij hoofdtaak 1 van Defensie: het voorbereiden en uitvoeren van militaire operaties, waaronder het verdedigen van het NAVO-grondgebied. Er bestaan echter ook veel vooroordelen en zorgen over AI in combinatie met defensie, denk aan ‘killer robots’. Daarom willen we zo transparant mogelijk zijn over hoe wij AI inzetten. Dat gebeurt altijd binnen wetgeving en ethische kaders.”

“We zien dat mensen soms ver van onze dagelijkse realiteit afstaan. De grootste dreiging komt misschien wel van desinformatie. Als mensen geloven dat ze gemanipuleerd worden, dan wordt het moeilijker om ze te mobiliseren of voor te bereiden op echte dreigingen. Dat is een veiligheidsuitdaging waarmee we steeds meer rekening moeten houden.”

De burger staat dan ook meer centraal in het overheidsbeleid en dienstverlening. Zwiers: “Voor Defensie is dat belangrijk voor de beeldvorming en onze veranderende relatie met de samenleving en bescherming van burgers. Gezien de huidige dreigingen is dat relevanter dan ooit. Het gaat ook om onze paraatheid als Nederland. We moeten mensen bewust maken van risico’s en ze voorbereiden op mogelijke crisissituaties. Niet voor niets roept de overheid op om een noodpakket in huis te hebben.”

### Zelflerende systemen veranderen het slagveld

Verandert oorlogsvoering door zelflerende systemen? Zwiers sluit de inzet ervan niet uit, in de verre toekomst, maar vooralsnog wil Defensie niet dat een systeem zelflerend is tijdens een operatie, licht ze toe. “Omdat we verwachten dat het onvoorspelbaar kan worden. We weten nu simpelweg niet hoe snel de techniek zich ontwikkelt. Daarom ontwikkelen we systemen in huis waardoor we weten: dit systeem werkt en het doet wat het moet doen. Wij

hebben het getest en het voldoet aan alle wetgevingskaders en het internationaal humanitair oorlogsrecht. Dan pas kunnen we het op een verantwoorde manier inzetten, evenals onze mensen in het veld. Zij moeten erop kunnen vertrouwen dat een systeem veilig is. Bij zelflerende systemen is dat niet automatisch het geval. Niemand kan deze systemen 100% monitoren. Dan verlies je de grip; we kunnen de uitkomst niet voorspellen. Dat is ondenkbaar in ons beroep. Daarom zijn we op dit moment nog terughoudend hiermee."

Toch ziet Zwiers dat AI op het slagveld al een doorslaggevende rol speelt: "AI gaat een serieuze, strategische voorsprong opleveren. Dat zien we nu al in Gaza en Oekraïne. Inlichtingenwerk verbetert enorm dankzij AI: er is extreem veel data dankzij drones, camerabeelden, sensoren, social media, et cetera. AI kan al die informatiestromen parallel aan elkaar analyseren en razendsnel de juiste informatie filteren."

**Edge computing**

Defensie wil op termijn ook de stap kunnen zetten naar meer edge computing. Zwiers: "Moderne oorlogsvoering is afhankelijk van snelle, betrouwbare en veilige informatieverwerking. We willen AI inzetten op het veld en dicht bij de wapensystemen. We willen toe naar een compleet geïntegreerd systeem waarbij ook de IT-infrastructuur zo wordt ingericht dat AI erop kan draaien. De IT-infrastructuur moet koppelingen hebben met de IT-er in het veld. Met edge computing kunnen gegevens lokaal, direct op het slagveld of in geavanceerde militaire voertuigen, worden verwerkt zonder afhankelijk te zijn van een centrale (cloud)omgeving. Door data lokaal te analyseren en te interpreteren, kunnen militairen direct handelen zonder te wachten op een externe verbinding. Dit verhoogt de operationele effectiviteit evenals de autonomie van onze systemen."

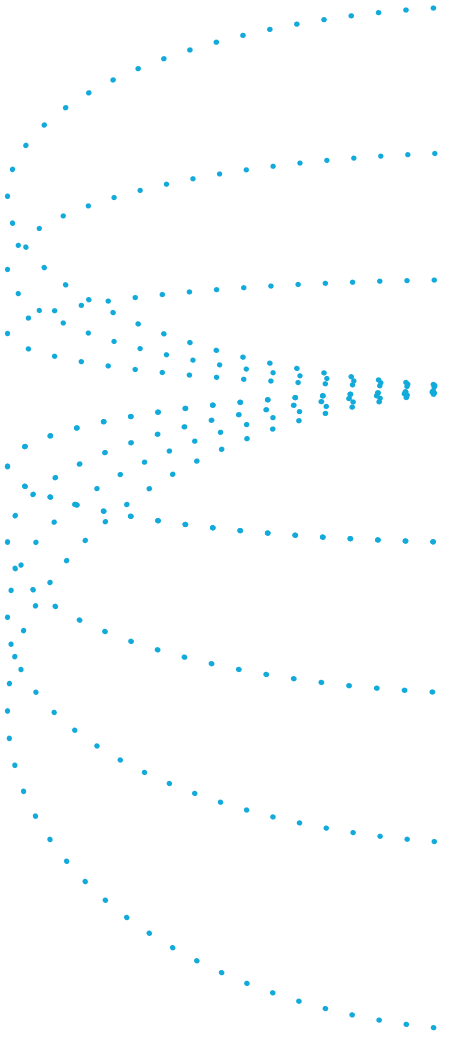
"We kunnen dan bijvoorbeeld ook beslissingen nemen op basis van realtime informatie, zelfs in gebieden waar netwerkverbindingen onbetrouwbaar of volledig afwezig zijn. Ook zijn onze mensen afhankelijk van betrouwbare satelliet- en netwerkverbindingen. Met edge computing zal dat sterk verminderen. Als je gevoelige data lokaal kunt verwerken, verklein je ook het risico op onderschepping door vijandelijke actoren behoorlijk. We verwachten dan ook dat edge computing veel gaat veranderen op het slagveld."

**Ethische oorlogsvoering**

Een groot onderwerp binnen Defensie is het inzetten van AI op een ethische manier. Zwiers: "Onze tegenstanders gebruiken deze technologieën ook, dus we moeten versnellen. Tegelijkertijd zijn er normen en waarden die bepalend zijn voor de inzet. Het Israëlische systeem Lavender maakt bijvoorbeeld gebruik van een grote hoeveelheid aan bronnen. Die gegevensverwerking ging op een gegeven moment zo snel dat er nog slechts beperkt 'betekenisvolle menselijke controle' mogelijk was. Iemand had slechts 20 seconden om te beoordelen of een target ook een legitiem doelwit was. Kan dat wel? Wij vinden dat iemand een gewogen besluit moet kunnen nemen: 20 seconden is erg weinig. Ons werk gaat immers soms over leven of dood. Dan moet het systeem adequaat en betrouwbaar zijn ingericht, op een manier die achteraf te valideren is."

Het voorbeeld geeft volgens Zwiers vooral ook aan hoe snel het gaat met AI, en met welke vraagstukken Defensie wordt geconfronteerd. Ook het omgaan met 'onethische AI' van tegenstanders is een groot vraagstuk. "Dit dilemma is voor ons urgenter dan voor andere veiligheidsinstanties, omdat onze tegenstanders vaak een heel ander ethisch kader hanteren en vanuit andere normen AI-toepassingen ontwikkelen voor potentiële conflictsituaties. Daar moeten we als Defensie op voorsorteren. Daarom is het belangrijk dat Defensie investeert in research & development op het vlak van 'counter AI'."

"Kijk bijvoorbeeld naar de inzet van droneswarms met kamikazedrones. Als zulke technologieën tegen ons worden ingezet, hebben we de plicht om onze mensen te beschermen. Dan heb je geen tijd voor een operator die eerst een betekenisvolle menselijke controle uitvoert. Iedere seconde telt. De snelheid van handelen is cruciaal om militairen en burgers te beschermen. We kunnen ons niet permitteren dat er vertraging



optreedt waardoor er onnodige slachtoffers vallen. De uitdaging is dus om ethisch verantwoord te werken, zonder onnodige risico's voor onze troepen en de bevolking."

**Competenties voor de toekomst**

De toekomst vraagt ook om andere, digitale en datagedreven vaardigheden, vertelt Zwiers. "Die willen we in alle militaire opleidingen te laten terugkomen, zodat de militair van de (nabije) toekomst op hoofdlijnen weet hoe een AI-systeem te interpreteren. Denk aan beeldherkenningsmodellen. Dan zie je een vierkantje met daarin '60%'. Maar wat moet een militair in het veld met die 60%? Is dat voldoende informatie om naar te handelen? Onze mensen moeten leren begrijpen wat die getallen betekenen, hoe ze te interpreteren en ermee om te gaan. Enige basiskennis van statistiek en data science én AI dus. Maar vooral de bewustwording van hun eigen rol en hoe ze deze technologie kunnen gebruiken ter ondersteuning in het veld."

**Wendbaar zijn**

Om alle nieuwe technologieën te kunnen adopteren, moet Defensie sneller en wendbaarder zijn. Zwiers: "Onze data science-afdelingen kijken daarom vooral wat de behoefte is vanuit de business. Als iets succesvol blijkt, dan proberen we het snel op te schalen. We werken erg pragmatisch, zonder teveel structuren of ingewikkelde bureaucratische processen. Je moet snel kunnen reageren op actuele situaties; een crisis kondigt zich meestal niet netjes van tevoren aan."

"De Wet op Gereedheid gaat daarbij helpen. Die moet ervoor zorgen dat er meer ruimte komt voor experimenten en wendbaarheid, ook in het digitale domein. De huidige geopolitieke situatie vereist dat we pragmatisch zijn en tegelijkertijd voldoen aan de wet- en regelgeving. Zonder alles aan de voorkant dicht te timmeren. Die flexibiliteit gaat deze wet ondersteunen. Want ons innovatievermogen versnellen is hard nodig; daar zien we dagelijks de voorbeelden van. Niets doen is geen optie."

**Ambities voor de toekomst**

Wil Defensie echt datagedreven werken, dan is een aantal keuzes nodig, meent Zwiers. "We moeten zaken echt anders organiseren. Snelheid, wendbaarheid, innovatie: dat moet voorop staan in onze doelen. Daar is het huidige Defensie niet op ingericht; we komen uit tijden van bezuinigingen en krapte. Het omgekeerde moet nu gebeuren; er is heel snel, heel veel nodig. Dat vraagt om meer absorptievermogen, snelle besluitvorming en het versneld vrijmaken van meer en grotere innovatiebudgetten."

Volgens Zwiers is het belangrijkste vraagstuk de volledige digitale transformatie van Defensie. "De toekomst vereist dat we veel meer datagedreven werken. We moeten uit de experimenteerfase komen en werken aan structurele digitalisering. Digitale transformatie moet het kloppend hart worden van onze organisatie."

10

# AI Factory: Grip op AI in het veiligheidsdomein

## Hoe kan de veiligheidssector AI veilig en flexibel opschalen in een nieuw AI en geopolitiek landschap?

**De AI Factory biedt organisaties een beproefde methode om AI gecontroleerd in te zetten: snelle innovatie zonder concessies aan security en flexibiliteit.**

### Highlights

- De AI Factory biedt een veilige en schaalbare manier om AI te implementeren – met behoud van regie over data, modellen en infrastructuur. Essentieel in domeinen waar soevereiniteit en betrouwbaarheid zwaar wegen
- Zelf modellen bouwen wordt steeds minder rendabel. Organisaties maken vaker de afweging om bestaande modellen slim én gecontroleerd in te zetten – zonder afhankelijk te worden van buitenlandse aanbieders
- Een AI Factory combineert vier essentiële bouwblokken: Services (technisch fundament), Templates (herbruikbaarheid), Factory (ontwikkeling) en Governance (controle) vormen samen een solide basis voor AI die past binnen strategische en juridische kaders
- Met centrale sturing, heldere 'guardrails' en technische standaarden voorkomt een AI Factory wildgroei – en ontstaat ruimte om consistent en veilig te innoveren, ook in politiek of juridisch gevoelige contexten.
- De AI Factory ondersteunt de transitie van proeftuin naar strategische impact. In een tijd waarin autonomie en digitale weerbaarheid centraal staan, biedt dit organisaties een concreet en beheersbaar groeipad

**Snelle AI innovatie als geopolitiek wapen**

De urgentie om AI te benutten wordt groter. Dat is het minste dat het conflict in Oost-Europa ons leert. Nieuwe innovaties binnen AI volgen elkaar in hoog tempo op. Gedreven door Sylicon Valley's onbegrensde vertrouwen in techniek en AI in het bijzonder. Voor de 'beste' AI-modellen worden we daardoor afhankelijker van grote aanbieders, hoofdzakelijk uit Amerika.

Een voorbeeld is Bloomberg, dat in maart 2023 haar eigen LLM 'Bloomberg GPT' lanceerde, met sterke financiële sector kennis. Het presteerde beter dan het toen beschikbare GPT-3.5, maar al binnen een halfjaar werd het ingehaald door GPT-4. De investering van ruim 10 miljoen dollar kon daarmee niet worden terugverdiend. Het alternatief: aanhaken bij een grote publieke aanbieder van deze technologie.

Een ander voorbeeld is DeepSeek, een Chinees model dat laat zien dat prestaties niet alleen afhangen van schaal. Met minder rekenkracht levert DeepSeek vergelijkbare kwaliteit. Het model is vijf keer goedkoper dan GPT-4o, en is daarmee een serieus alternatief wanneer kosten en efficiëntie zwaar meewegen. Maar hoe goed kunnen we China vertrouwen?

Met oplopende geopolitieke spanningen komt er meer druk op strategische autonomie. Denk aan het toenemende belang van soevereine controle over data, modellen en infrastructuur – zeker in een wereld waar technologie uit de VS of China steeds vaker een dubbele rol speelt, commercieel én militair. Een autonome robot hond uit de VS of China lijkt schattig, maar met een kleine aanpassing lopen er duizenden bewapend het slagveld op.

**De noodzaak voor grip op AI**

Tegelijk worstelen veel organisaties met grip op AI-initiatieven. Door snelle innovaties zijn oplossingen vaak versnipperd, zijn modellen niet herleidbaar en ontbreekt de governance. De roep om transparantie groeit, met initiatieven als algoritmeregisters als voorbeeld. Nog niet te spreken over data die weglekt via publieke aanbieders als ChatGPT of DeepSeek.

Daarnaast kiezen sommige partijen bewust voor een andere afweging in het internationale speelveld. Zo zet Frankrijk in op eigen AI-modellen, ondanks de hogere kosten en complexiteit. Reden: soevereiniteit. De zekerheid dat gevoelige data en beslismodellen onder eigen controle blijven, weegt zwaarder dan de directe functionele voordelen van commerciële alternatieven.

Flexibiliteit en schaalbaarheid speelt hierbij een cruciale rol. Traditionele oplossingen als zelf hosten voldoet niet langer. Een pijnlijke les die de oorlog in het Oosten van Europa ons leert. De kans is groot dat u eigen infrastructuur in de eerste dagen zo niet uren van een conflict platgaat. Hoe zorg u in dit scenario voor continuïteit?

Om de snelle innovaties, het versnipperde AI landschap binnen organisaties en de vraag naar soevereiniteit effectief

het hoofd te bieden is een AI Factory onmisbaar. Het maakt het mogelijk om snel over te kunnen stappen naar nieuwe modellen en infrastructuur op een veilige manier. Waarbij de risico's van AI centraal geborgd worden.

**De bouwblokken van een AI factory**

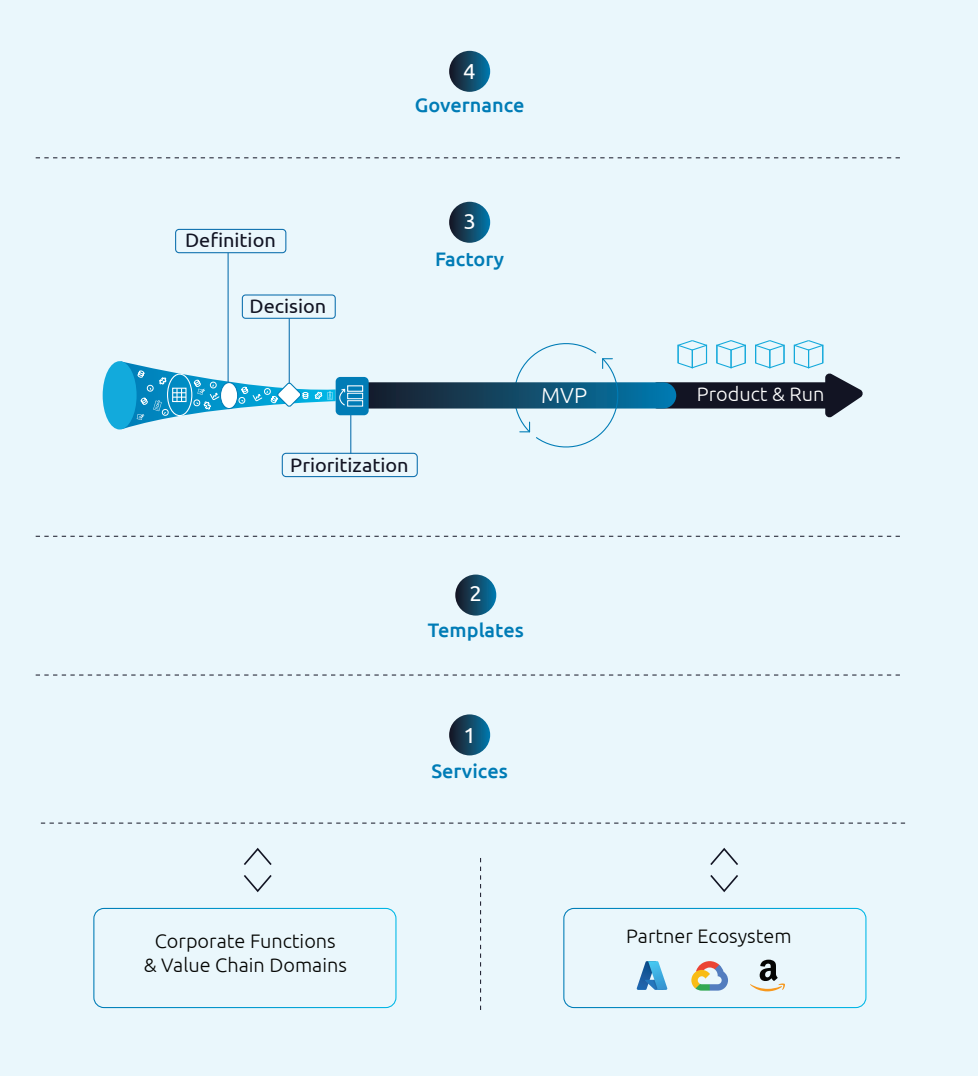
Een AI Factory bevat vier essentiële bouwblokken die samen een krachtig en schaalbaar AI-ecosysteem vormen.

1. Services: De Motor van AI-Innovatie
   Dit zijn de technische fundamenten zoals data platforms, compute- en data-capaciteit en beveiligingsvoorzieningen. Deze kunnen flexibel worden gecombineerd om oplossingen te bouwen die aansluiten bij specifieke bedrijfsbehoeften. Denk bijvoorbeeld aan een defensieorganisatie die standaardiseerbare infrastructuurcomponenten inzet om verschillende LLM's veilig en snel te testen – zonder dat er telkens een nieuw platform hoeft te worden ingericht.
2. Templates: Versnellers voor AI-Ontwikkeling
   Herbruikbare frameworks en componenten die zorgen voor versnelling en consistentie. Ze bevatten best practices en bewezen methodologieën, waardoor teams niet steeds opnieuw het wiel hoeven uit te vinden. Dit zorgt voor een consistente kwaliteit, snellere time-to-market en efficiëntere ontwikkeling.
   Bij een luchtmachtonderdeel is bijvoorbeeld een MLOps pijplijn opgezet om modellen en dataproducten getest en geverifieerd beschikbaar te stellen aan eindgebruikers.
3. Factory: waar ontwikkeling en validatie samenkomen
   De plek waar AI-oplossingen worden gebouwd, gevalideerd en klaargemaakt voor productie met behulp van moderne tools en technieken. Een gestructureerde aanpak zorgt voor gecontroleerde ontwikkeling, betrouwbare resultaten en een schaalbare implementatie.
   In een civiele veiligheidsorganisatie kunnen hier bijvoorbeeld modellen voor risicosignalering worden ontwikkeld, getest en geverifieerd op bias voordat ze in operatie worden gebracht.
4. Governance: borging van kwaliteit en vertrouwen.
   Governance zorgt voor grip op veiligheid, compliance en verantwoording. Dit omvat duidelijke richtlijnen en processen, bescherming van data, privacy en monitoring van prestaties en controle op bias en fairness. Zo werd in een overheidsinstantie een 'modelregister' gekoppeld aan de AI Factory, waarmee elk gebruikt model is terug te herleiden tot trainingsdata, gebruikscontext en verantwoordelijke eigenaar.

Door deze bouwblokken samen te brengen ontstaat een professionele AI-omgeving die organisaties helpt om effectief en verantwoord AI te implementeren. Het stelt teams in staat om snel nieuwe oplossingen te ontwikkelen zonder concessies te doen aan kwaliteit of betrouwbaarheid.

De sleutel tot succes ligt in de balans tussen innovatie en controle - tussen snelheid en zorgvuldigheid. Met een goed opgezette AI Factory kunnen organisaties deze balans vinden en AI op schaal inzetten voor blijvende waarde. Zelfs in onzekere scenario's waarin eigen infrastructuur niet meer toereikend blijkt.

## De bouwblokken van een AI factory




Afbeelding 1: de bouwblokken van een AI factory

**De bouwblokken van een AI factory**

De AI Factory helpt organisaties om de overgang te maken van proeftuin naar een hoge mate van impact door AI-oplossingen te professionaliseren en op te schalen. Dit omvat het aanpakken van veelvoorkomende uitdagingen zoals een gebrek aan strategie, onduidelijke governance, verspreide technologie-implementatie en moeilijk meetbare ROI.

Wat vaak misgaat – en wat de AI Factory voorkomt:

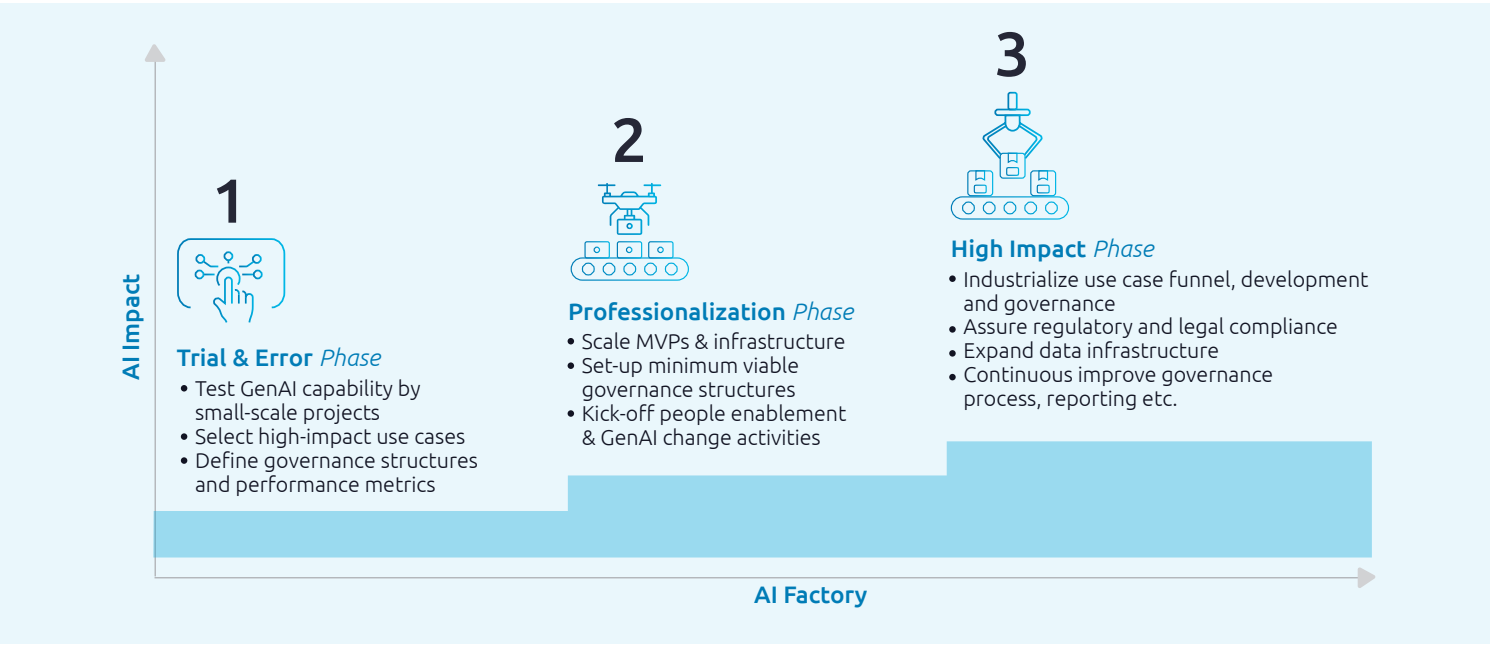
- Elke afdeling experimenteert los van elkaar, zonder herbruikbare bouwstenen
- AI-projecten zijn moeilijk op te schalen door gebrek aan centrale infrastructuur
- De gebruikte infrastructuur is niet gemakkelijk over te zetten naar een andere omgeving zoals de cloud
- Beslissingen van modellen zijn niet herleidbaar of uitlegbaar
- Data- en privacyrisico's zijn moeilijk te beheersen
- Geen helder eigenaarschap of zicht op wie waarvoor verantwoordelijk is

Een succesvolle AI Factory realiseert waarde langs vier assen:

- Business impact: Realiseren van impact op relevante vraagstukken binnen de strategie van de organisatie.
- Kostenefficiëntie: Vermindering van ontwikkelings- en operationele kosten van AI-workloads.
- Schaalbaarheid: Optimalisatie van tijd tot markt, beschikbaarheid en herbruikbaarheid van use cases.
- Betrouwbare AI: Bescherming van gebruikers en data tegen misbruik en fouten.

Dit kan alleen gerealiseerd worden door een georkestreerde aanpak op AI. Geen losse proeftuintjes versnippert door de organisatie, maar onder centrale regie hergebruiken van componenten. Alle AI-oplossingen kunnen daarmee aantoonbaar voldoen aan de juist 'guard rails' om ongewenst gedrag te voorkomen. Schaarse resources kunnen efficiënter verdeeld en hergebruikt worden. En de modulaire aanpak maakt het mogelijk om snel bouwblokken uit te wisselen of te verbeteren.

## Een AI-fabriek stelt organisaties in staat om door te groeien naar grootschalige impact




Afbeelding 2: Fases voor gebruik AI

**De Weg naar Succes**

Grote kans dat uw organisatie zich al op het pad van een AI Factory bevindt. Dit pad kent drie grote fases:

1. Proeftuinfase: de meeste organisaties hebben zich de afgelopen jaren gericht op het beproeven van AI. Kleinschalige projecten om de daadwerkelijke impact van de technologie binnen een organisatie te beproeven. Voorbeelden zijn proof-of-concepts zoals beeldherkenning, tekstsamenvatting of voorspellend onderhoud – vaak losstaand, zonder integratie met bestaande processen.
2. Professionaliseringsfase: na het beproeven van de technologie en een duidelijker beeld van de impact verschuift de focus naar het schalen van de MVP's en de onderliggende infrastructuur. Het gaat hierbij niet alleen om techniek, maar vooral ook om de transformatie die hierbij komt kijken. Hier worden rollen zoals AI product owner en data stewards ingericht en ontstaat behoefte aan centrale infrastructuur, modelregistratie en lifecycle management.
3. "High Impact"-fase: deze laatste fase is de AI Factory. Hierbij is een funnel van impactvolle projecten gerealiseerd, zijn wet- en regelgeving geborgd en wordt er continue geoptimaliseerd op de geboden oplossingen. De AI-operatie is verankerd in de organisatie, modellen draaien in productie, er is toezicht en continue optimalisatie op prestaties, risico's en naleving.

De AI Factory biedt in haar aanpak niet alleen een kijk op de techniek. Het biedt vooral ook een framework en proces om gestructureerd te blijven innoveren op de meest impactvolle thema's binnen de strategische kaders van uw organisatie. Wel gedragen door een technische architectuur op een schaalbare infrastructuur die herbruikbaar en uitwisselbaar wordt ingericht.

### Maar waar begint u als organisatie?

De eerste stap is het in kaart brengen van bestaande AI-initiatieven, infrastructuur en governance – hoe versnipperd of onvolledig die ook zijn. Vervolgens kunt u starten met het opzetten van een eerste, kleinschalige AI Factory-pilot. Denk hierbij aan één prioritaire use case binnen een gecontroleerde omgeving, ondersteund

door centrale services en duidelijke ‘guardrails’. Vanuit daar kunt u leren, verbeteren en stapsgewijs opschalen.

De AI Factory biedt hiermee een antwoord op de versnippering van AI-initiatieven. Het creëert niet alleen overzicht, maar maakt het ook mogelijk om snel en verantwoord op te schalen. Door grip, herbruikbaarheid en centrale sturing te combineren, ontstaat een stevig fundament voor AI die niet alleen technisch werkt, maar ook organisatorisch gedragen en bestuurbaar is.

In een tijd van toenemende geopolitieke spanningen en afhankelijkheid van buitenlandse technologiepartners, helpt de AI Factory bovendien om soevereiniteit en autonomie te borgen – juist daar waar controle over data en besluitvorming cruciaal is. Nu is het moment om het initiatief te nemen. Begin klein, maar denk groots – en bouw vandaag aan het fundament voor verantwoorde AI op schaal.

## Over de auteurs

**Joost Carpaij**
**Head of (Gen)AI, Data Science and Analytics**

Als head of (Gen)AI, Data Science and Analytics is Joost verantwoordelijk voor de doorontwikkeling van dit vakgebied en de collega’s binnen Capgemini. Daarbij is hij hoofdzakelijk betrokken bij partijen in het publieke veiligheidsdomein.

joost.carpaij@capgemini.com

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

**Sjoukje Zaal**
**CTO Insights & Data Europe**

Als Chief Technology Officer bij Capgemini breng ik meer dan 20 jaar ervaring mee in architectuur, ontwikkeling en advies, met een sterke focus op AI, data, cloud en innovatie.

sjoukje.zaal@capgemini.com

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

11

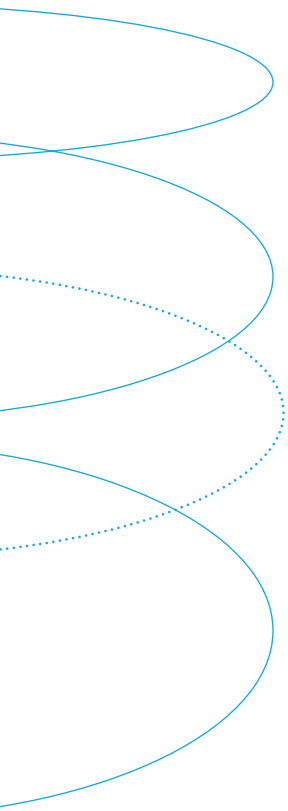
# Data governance: fundament voor informatiedominantie bij Defensie

## Hoe ondersteunt data governance Defensie in haar streven naar informatiedominantie?

**Sterke data governance is cruciaal voor informatiedominantie: het geeft Defensie grip op data, versnelt besluitvorming en versterkt operationele slagkracht.**

## Highlights

- Informatiedominantie is cruciaal op het slagveld van vandaag
- Geavanceerde technieken als AI kunnen voor deze informatiedominantie zorgen
- Dergelijke technieken leveren alleen waarde als data op orde is
- Data governance zorgt voor grip op data zodat data op orde komt
- De eerste stappen richting volwassen data governance en daarmee informatiedominantie zijn gezet



Stel je een scenario voor waarin elk onderdeel van Defensie – waaronder de Luchtmacht, Landmacht en Marine – naadloos samenwerkt dankzij betrouwbare en bruikbare data. Een commandant van de Landmacht kan in één oogopslag zien welke pantservoertuigen inzetbaar zijn en welke logistieke routes het meest efficiënt zijn voor een snelle troepenverplaatsing. Bij de Luchtmacht ontvangt een F-35-piloot real-time dreigingsinformatie vanuit diverse sensoren en bondgenoten, waardoor hij zijn missie met uiterste precisie kan uitvoeren. Ondertussen kan de commandant van een fregat in één oogopslag de actuele status van brandstofvoorraden en wapensystemen controleren, terwijl predictive maintenance voorspelt waar onderhoud het hardst nodig is.

Tijdige informatie stroomt moeiteloos binnen vanuit wapensystemen, drones, satellieten en eenheden op de grond en op zee. Deze data wordt direct vertaald naar bruikbare inzichten: waar vijandelijke bewegingen worden gedetecteerd, welke troepen gereed zijn voor inzet en hoe logistieke bevoorrading soepel verloopt. Hierdoor worden beslissingen snel en accuraat genomen, en kunnen operaties met maximale effectiviteit worden uitgevoerd. Dit scenario, waarin informatiedominantie centraal staat, is alleen haalbaar als Defensie optimaal grip heeft op haar data. De sleutel? Sterke data governance.

### Grip op data krijgen middels data governance

Hoewel data governance misschien niet het eerste is waar je aan denkt bij effectieve militaire operaties, vormt het de basis voor betrouwbare en bruikbare data.

Om informatiedominantie te bereiken, maakt Defensie gebruik van geavanceerde data science-technieken. Kunstmatige intelligentie (AI) analyseert grote hoeveelheden data en identificeert patronen die anders onopgemerkt blijven. Machine learning helpt bij het voorspellen van logistieke knelpunten of het vroegtijdig detecteren van dreigingen. Ook digital twins – virtuele modellen van systemen of operaties – maken het mogelijk om scenario's te simuleren en risico's te minimaliseren. Het loslaten van simulaties op "gedigitaliseerd" materieel is hier een voorbeeld van.

Deze technieken hebben één ding gemeen: ze zijn afhankelijk van kwalitatief hoogwaardige data. Ze zijn namelijk slechts zo krachtig als de data die ze voeden. Slechte input leidt tot slechte output – ofwel garbage in, garbage out. Zonder betrouwbare en beschikbare data blijft het potentieel van AI en machine learning onbenut. Vorig jaar schreven we al in Trends in Veiligheid dat de maximalisatie van de waarde en minimalisatie van de risico's van AI afhankelijk is van data. Data die als input dient voor de AI-modellen. Om ervoor te zorgen dat data geschikt is als input en (o.a.) beschikbaar, betrouwbaar, volledig en begrijpelijk is, moet een organisatie grip op haar data hebben om deze op orde te krijgen.

Data governance zorgt hiervoor. Het omvat al het beleid, processen en rollen die zorgen voor effectief datagebruik en -beheer binnen een organisatie. Het gaat verder dan technische oplossingen; het is een strategisch raamwerk dat bepaalt hoe data wordt verzameld, opgeslagen, gedeeld en gebruikt. Data governance zorgt ervoor dat dataverantwoordelijkheden helder worden belegd. Data-eigenaren zijn eindverantwoordelijk voor de data binnen hun domein, waarbij data stewards de data-eigenaren ondersteunen in het uitvoeren van hun taken en verantwoordelijkheden in de praktijk. Daarnaast stelt data governance richtlijnen op voor o.a. dataopslag, gebruik en deling, zodat data op een uniforme en veilige manier wordt beheerd, en beschikbaar is wanneer dat nodig is.

Zonder een goed ingerichte data governance kan de enorme hoeveelheid data binnen Defensie leiden tot chaos in plaats van een strategisch voordeel, je ziet door de bomen het bos niet meer. Door grip op data te hebben – ongeacht de bron of het krijgsmachtonderdeel dat ermee werkt – wordt het mogelijk om technologieën als AI en machine learning optimaal te benutten in het snel veranderende slagveld van vandaag.

**Data governance als besturende as voor datamanagement**

In het eerder geschetste scenario in de inleiding moet een aantal datamanagementaspecten ingericht worden voordat technieken als data science toegepast kunnen worden en data veilig en met de juiste kwaliteit gedeeld kan worden. Waar data governance met name gaat over kaders, rollen en verantwoordelijkheden, gaat datamanagement over het daadwerkelijk verwerken (verzamelen, organiseren, rubriceren, opslaan) van data. Datamanagementaspecten waar minimaal aan gewerkt dient te worden om samen te werken zoals in eerdergenoemd scenario zijn interoperabiliteit, datakwaliteit en databeveiliging.

**Interoperabiliteit** - Om ervoor te zorgen dat de verschillende onderdelen van de krijgsmacht gebruik kunnen maken van elkaars data, dienen zij interoperabel te zijn. Dit vereist eenduidige standaarden, formats en protocollen, zodat data kan worden gedeeld en geïnterpreteerd.

Data governance speelt hierin een cruciale rol door rollen en verantwoordelijkheden duidelijk te beleggen. Data-eigenaren bepalen hier de standaarden zodat data op een uniforme manier wordt beheerd en gebruikt. Data stewards zien toe op naleving en de implementatie ervan. Hierdoor ontstaat een gemeenschappelijk begrippenkader dat voorkomt dat data op verschillende manieren wordt geïnterpreteerd binnen Defensie. Daarnaast harmoniseert data governance technische standaarden, zodat systemen compatibel zijn en gegevens direct bruikbaar blijven.

**Datakwaliteit** - Beslissingen tijdens een missie kunnen van levensbelang zijn. Daarom is het cruciaal dat data tijdig beschikbaar, correct en volledig is. Slechte datakwaliteit kan leiden tot verkeerde inschattingen en inefficiënte operaties.

Op het gebied van datakwaliteit stellen datahouders de kaders voor kwalitatief goede data op en zorgen data stewards ervoor dat de kwaliteit van de data daadwerkelijk op het juiste niveau komt. Eenduidige definities, validatieregels en kwaliteitscontroles zorgen ervoor dat data consistent en betrouwbaar blijft. Hierdoor kan op de juiste manier data-analyse en machine learning toegepast worden, waardoor Defensie kan vertrouwen op de uitkomsten en in kritieke situaties accurate beslissingen kan maken.

**Beveiliging** - In bovenstaand scenario moet strikt uitgesloten kunnen worden dat ongeautoriseerden toegang hebben tot gevoelige informatie.

Een goed ingerichte data governance zorgt ervoor dat gevoelige informatie beschermd, maar wel toegankelijk en beheersbaar blijft. Data-eigenaren bepalen op het gebied van beveiliging de toegangsrechten en classificeren data op basis van gevoeligheid. Data stewards zien toe op de naleving van beveiligingsrichtlijnen en regelgeving. Hierdoor wordt de kans op datalekken geminimaliseerd en blijft kritieke informatie uitsluitend toegankelijk voor bevoegde personen.

**De eerste stappen in de praktijk; op weg naar een informatiegestuurde krijgsmacht**

De afgelopen jaren worden binnen Defensie grote stappen gezet op het gebied van data governance. Een solide data governance is opgebouwd uit verschillende cruciale elementen. Dit omvat onder andere het duidelijk beleggen van rollen en verantwoordelijkheden, het vaststellen van kaders en beleid, en het implementeren van datamanagementtooling. Daarnaast zijn een volwassen datacultuur, getrainde medewerkers en goed geïntegreerde systemen essentieel voor een succesvolle uitvoering van data governance.

De Defensieonderdelen zijn gestart met het fundament: het inrichten van de data governance-structuur. Dit houdt in dat data-eigenaren en data stewards zijn benoemd en deze rollen officieel zijn vastgelegd in het beleid van Defensie. Deze professionals werken domeinoverstijgend samen en nemen deel aan overlegstructuren, zodat verantwoordelijkheden helder zijn en effectief wordt samengewerkt.

Parallel aan de organisatorische inrichting wordt actief gestuurd op datakwaliteit. Data-eigenaren stellen richtlijnen op voor kwalitatief goede data binnen hun domeinen, terwijl data stewards ervoor zorgen dat deze kwaliteit daadwerkelijk wordt verhoogd. Ze doen dit bijvoorbeeld door dashboards te ontwikkelen waarin datakwaliteits-KPI's inzichtelijk maken hoe de huidige datakwaliteit ervoor staat, waardoor gerichte verbeteracties mogelijk worden. De volgende stap is om deze initiatieven te professionaliseren en op een eenduidige manier te sturen op datakwaliteit. Zo kan over de hele organisatie een goed beeld gevormd worden van die kwaliteit en wordt ervoor gezorgd dat er alleen gestuurd wordt op data die de actuele situatie representeert.

Op het gebied van databeveiliging zijn handvatten beschikbaar om data op de juiste manier te rubriceren. Dit houdt in dat data op basis van gevoeligheid en relevantie wordt geclassificeerd, zodat de juiste beveiligingsmaatregelen kunnen worden genomen. Data kan optimaal worden ingezet, terwijl het risico op onbedoeld misbruik wordt geminimaliseerd. Zo wordt bijvoorbeeld voorkomen dat de vijand inzicht heeft in de gereedheid van onze troepen.

Zoals eerder genoemd maakt Defensie gebruik van algoritmes om voorspellingen te doen en situatie's te simuleren, bijvoorbeeld het vroegtijdig detecteren van dreigingen en de impact daarvan. Het is van belang dat deze data science technieken ethisch en verantwoord worden ontwikkelt en ingezet. De algoritmes worden daarom middels checklists gecontroleerd, waarbij potentiële risico's en bias in het gebruik van data tijdig worden geïdentificeerd en gemitigeerd.

Defensie heeft al waardevolle stappen gezet naar een informatiegestuurde krijgsmacht. Om bovenstaand scenario van een volledig informatiegestuurde krijgsmacht werkelijkheid te maken zijn er echter nog een aantal stappen die gezet moeten worden. Zo is het van belang om de data governance verder uit te breiden naar een Defensiebrede aanpak, waarbij standaarden, richtlijnen en datadefinities voor alle Defensieonderdelen uniform worden vastgesteld. Dit biedt de basis voor een uniforme en gestructureerde inzet van data door de hele organisatie, wat uiteindelijk leidt tot een efficiënter en effectiever gebruik van beschikbare informatie.

**Conclusie**

Data governance speelt een cruciale rol binnen Defensie om informatiedominantie te bereiken. Door het uniform en betrouwbaar beschikbaar stellen van data, kan Defensie innovatieve technieken zoals AI en machine learning effectief toepassen. Dit zorgt ervoor dat data gezien kan worden als een waardevolle asset en maakt naadloze samenwerking tussen de verschillende Defensieonderdelen mogelijk. Deze verbeterde operationele samenwerking vertaalt zich in snellere en nauwkeurigere besluitvorming, wat essentieel is in een tijdperk waarin de beschikbaarheid van betrouwbare informatie vaak het verschil maakt. Sterke data governance is daarmee niet slechts een voorwaarde, maar een strategische troef die helpt Defensie haar voorsprong te behouden.

## Over de auteurs

Pleun, Bas en Jeroen werken alledrie aan een organisatiebrede implementatie van data governance voor het Ministerie van Defensie.

**Jeroen Jeschke**
Managing Consultant Insights & Data

Jeroen is werkzaam bij Insights & Data. Jeroen is een expert op het gebied van datagedreven werken en werkt momenteel aan een data governance implementatie binnen de Koninklijke Luchtmacht.

jeroen.jeschke@capgemini.com

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

**Bas Biemans**
Managing Consultant Insights & Data

Bas is werkzaam bij Insights & Data. Bas is Strategisch Adviseur Data Governance en werkt momenteel aan de data governance implementatie binnen Defensie.

bas.biemans@capgemini.com

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

**Pleun Mekel**
Senior Consultant Insights & Data

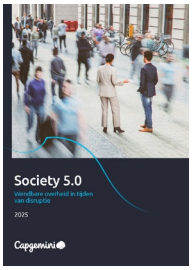
Pleun is werkzaam bij Insights & Data. Pleun is Data Governance Expert en werkt momenteel aan de data governance implementatie binnen Defensie.

pleun.mekel@capgemini.com

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

# Publicaties

Naast ons Trends in Veiligheid rapport publiceren wij nog andere rapporten, onderzoeken en whitepapers die voor u relevant kunnen zijn. Onderstaand treft u een verkort overzicht aan. Het complete overzicht vindt u op: www.capgemini.nl




**Society 5.0**
Wendbare overheid in tijden van disruptie
Europa en Nederland bevinden zich momenteel in een tijd van geopolitieke verschuivingen, technologische transities en economische uitdagingen.
Het rapport Society 5.0: Wendbare overheid in tijden van disruptie biedt inzichten in hoe de publieke sector kan inspelen op de huidige turbulente tijden en veerkracht kan vergroten. Het rapport geeft een beeld van de aspecten die aangepakt dienen te worden om de wendbaarheid en weerbaarheid van de publieke sector te vergroten.

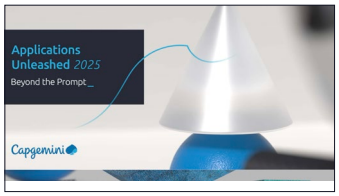
https://www.capgemini.com/nl-nl/wendbare-overheid-in-tijden-van-disruptie/


**Trends in Cybersecurity 2024**
**Navigeren door de cyberwereld**

Dit is de 4e editie van Trends in Cybersecurity, met als thema dit jaar: Navigeren door de Cyberwereld. In een wereld waar digitale dreigingen constant evolueren, is dit rapport uw gids om veilig te navigeren door de complexe cyberwereld. Het rapport richt zich op het bieden van cruciale inzichten en strategieën voor cybersecurity professionals.

Verken onderwerpen zoals de rol van Generatieve AI in cyberbeveiliging en de uitdagingen van opkomende OT-technologieën. Ontdek hoe u uw organisatie kunt beschermen tegen hedendaagse bedreigingen en tevens kunt voldoen aan de compliance eisen.

https://www.capgemini.com/nl-nl/trends-in-cybersecurity-2024/



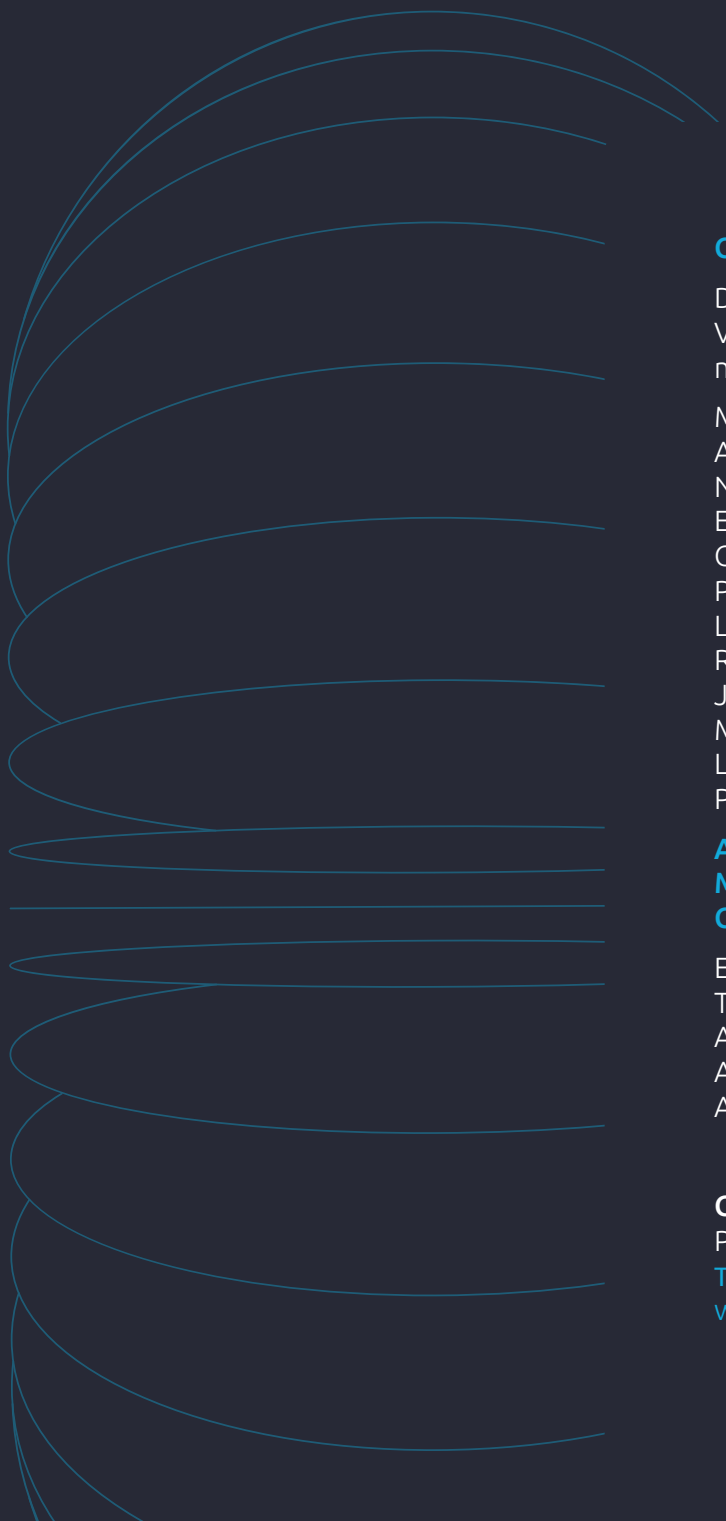

**Applications Unleashed 2025**
Beyond the Prompt
Applicaties. Ze draaien, crashen, updaten en transformeren sneller dan je 'Patch Tuesday' kunt zeggen. Ooit waren ze keurig ingekaderde softwarepakketten, braaf binnen de lijntjes van hun architectuur en ontwerp. Maar inmiddels zijn ze ontketend ('unleashed', inderdaad) – en ze hebben geen plannen om zich weer netjes te gedragen. Dankzij AI worden ze slimmer, adaptiever en, laten we eerlijk zijn, soms ook een tikje eigenwijs. Wie heeft er immers documentatie nodig als je ook vage beloftes over zelflerend vermogen kunt krijgen?

https://www.capgemini.com/nl-nl/expertise/research/applications-unleashed-2025-beyond-the-prompt/


**Data foundations voor de overheid**
**Van AI-ambitie naar actie**

In 2025 zetten overheden wereldwijd AI in om de efficiëntie te verhogen en tegelijkertijd burgergerichte diensten te leveren, economische groei te stimuleren en innovatie te stimuleren. Maar beschikken ze ook over de benodigde datafundamenten om hun doelen te bereiken?
In het rapport Data foundations for government: From AI ambition to action van het Capgemini Research Institute wordt onderzocht in hoeverre de publieke sector vandaag de dag klaar is om het potentieel van zijn data-infrastructuur te benutten – om besluitvorming, efficiëntie en effectiviteit te verbeteren – maar ook om AI in te zetten om de toekomst van de overheid te transformeren.

https://www.capgemini.com/nl-nl/expertise/research/data-foundations-voor-de-overheid/



## Colofon

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

Martijn van de Ridder
Aydan Gunduz
Natasja Pieterman
Erik Staffeleu
Gerard Pieter Borren
Puck Bijleveld
Louise van 't Erve
Roeland de Koning
Joris Commissaris
Marcel Kordes
Luuk Tubbing
Paul Lengkeek

**Advies, ontwerp en productie: Marketing & Communicatie, Capgemini Nederland B.V.**

Ernes Mahmutovic
Thomas de Klerk
Arundhati Bhattacharya
Arindam Dey
Ashim Karmakar

**Capgemini Nederland B.V.**
Postbus 2575 – 3500 GN Utrecht
Tel. + 31 30 203 05 00
www.capgemini.nl

## Over Capgemini

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, generative AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2024 global revenues of €22.1 billion.

Get the future you want | www.capgemini.com

Capgemini Nederland B.V.
Postbus 2575 - 3500 GN Utrecht
Tel. + 31 30 203 05 00

2D-005.25