

GOV

#21

magazine
over de digitale
overheid

Soevereiniteit en continuïteit



Gijs Tuinman
Digitale
transformatie
bij Defensie



Stéphanie Obertin
Digitale soevereiniteit
in Luxemburg



Eddie van Marum
Nederlandse
Digitaliseringsstrategie





4
STÉPHANIE OBERTIN

8
GIJS TUINMAN

16
EDDIE VAN MARUM

14 GASTCOLUMN
Quirine van Eeden
Rathenau Instituut
“Digitale afhankelijkheid zet regie over publieke sectoren op het spel”

20 Bert Voorbraak
Logius
“Waar het om gaat is: ben je weerbaar tegen allerlei invloeden?”

24 Matthijs van Amelsfort
NCSC
“We hebben te maken met een veelkoppig monster en 100 procent veiligheid is een illusie”

28 Peter Verkoulen
CoE-DSC / Gaia-X
“Bij Europese aanbestedingen ook kijken naar aspecten van soevereiniteit”

32 Christiane Kirketerp de Viron
Europese Commissie
“Bouwen aan de veerkracht van Europa door innovatie, investeringen en soevereiniteit”

34 Hans Koolen & Jitka Beukenkamp
Atos Nederland
“We zetten technologie in om alles wat van waarde is te beschermen en te versterken”

40 Maaike Okano-Heijmans
Clingendael
Martijn Lucassen
Ministerie Economische Zaken
“Het vraagstuk van onze afhankelijkheid op digitale technologie is een vraagstuk van schaal en van kapitaal”

46 Ron Kolkman
Rijkswaterstaat
“Soevereiniteit op data gaat over evidente data die we nodig hebben om Nederland veilig, leefbaar en bereikbaar te houden”

50 CASE
Data als basis voor inspirerend verkeersmanagement

VOORWOORD

Technologische soevereiniteit met als doel bedrijfscontinuïteit

De huidige geopolitieke situatie vraagt om een strategische (digitale) autonomie van Europa. De samenwerking tussen de EU-lidstaten wordt daarmee steeds belangrijker, juist als het gaat om onze concurrentiepositie en de continuïteit van bedrijfsvoering - en daarmee samenhangende dienstverlening.

Om dat te kunnen bereiken is samenwerking nodig, met publieke en private partijen. Marktpartijen die (technologische) soevereiniteit voor Europa kunnen realiseren met een passend portfolio van producten en diensten voor digitale toepassingen, die helpen de maatschappelijke opgaven te realiseren. En voor een veilige, inclusieve en kansrijke digitale samenleving is een strategie nodig die de Europese waarden respecteert en faciliteert, juist op het vlak van privacy, ethiek, mensenrechten, transparantie en regie op eigen gegevens.

De ‘wake-up’ call met betrekking tot de risico’s van (digitale) afhankelijkheid kwam extra hard binnen toen de hoofdaanklager en een aantal rechters van het Internationaal Strafhof (ISH) in mei 2025 door Microsoft de toegang tot hun e-mailaccount werd ontzegd. Dit naar verluidt als gevolg van de door de Amerikaanse president Donald Trump afgekondigde sancties tegen het ISH. Het ISH verklaarde aan GOV magazine desgevraagd geen commentaar te geven op dit onderwerp. Kamervragen en de beantwoording daarvan laten zien dat de bedrijfscontinuïteit, en in het bijzonder het onafhankelijk functioneren van het Hof, in het geding kan komen door deze sancties.

Een tweede belangrijk thema is digitale weerbaarheid. Op de One Conference in september jl. vroeg minister-president Dick Schoof, vanuit zijn kennis en achtergrond van de AIVD en de NCTV, hiervoor expliciet aandacht. De digitale aanvallen op de systemen van het Openbaar Ministerie en de hack bij Bevolkingsonderzoek Nederland maken duidelijk dat statelijke actoren steeds vaker actief zijn. Een cyberaanval in diezelfde maand bij de Britse autofabrikant Jaguar Land Rover toont aan dat de gevolgen verder reiken dan het concern zelf. Talloze (toe)leveranciers zijn ook getroffen omdat uit voorzorg de ICT-systemen van de productie zijn stilgelegd; met als gevolg directe impact op de bedrijfscontinuïteit en miljarden Euro’s aan schade.



Het maakt duidelijk dat digitale technologie waarvoor strategische afhankelijkheden gelden, met een hoog risico, een ‘plan B’ vereisen. Juist om die bedrijfscontinuïteit en dienstverlening te kunnen garanderen. In deze 21e GOV magazine editie presenteren we voorbeelden uit de praktijk, met onder meer Stéphanie Obertin, minister van Digitalisering in het groothertogdom Luxemburg dat als voorbeeld is genoemd voor de soevereine cloud; de demissionair staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties Eddie van Marum over de Nederlandse Digitaliseringsstrategie en het speerpunt Digitale Weerbaarheid en demissionair staatssecretaris van Defensie Gijs Tuinman over de Digitale Transformatie Strategie, met als doel de digitale slagkracht en daarmee de gevechtskracht te versterken. Ik wens u véél leesplezier en inspiratie toe!

Met vriendelijke groet,

Willem Beelen
Atos groep Nederland

Digitale soevereiniteit in Luxemburg

Luxemburg beschikt sinds 2018 over een ministerie voor Digitalisering. De huidige minister is Stéphanie Obertin. In maart van dit jaar ontving zij Zsolt Szabó, toenmalig staatssecretaris voor Koninkrijksrelaties en Digitalisering. Na afloop van dit bezoek was Szabó vol lof over hoe het groothertogdom erin is geslaagd een soevereine cloud te realiseren. Reden voor GOV magazine om Obertin te vragen hoe een relatief klein land als Luxemburg tot de meest digitaal geavanceerde EU-lidstaten is gaan behoren.

Obertin vertelt dat zij en Szabó elkaar bijpraatten over de ontwikkelingen in beide landen op het gebied van digitalisering van de overheidsdiensten. “Ik heb hem de hoofdlijnen gepresenteerd van onze nationale datastrategie, ontwikkelingen als de platformen Guichet.lu en MyGuichet.lu, en de inspanningen van onze overheid om digitale soevereiniteit te bereiken.”

AI in 2016 introduceerde Luxemburg een eerste overheidscloudstrategie, vertelt Obertin. “Die betrof de oprichting van GovCloud: een soevereine cloudinfrastructuur die beschikbaar is voor alle overheidsdiensten. Die strategie van toen kwam met een set heldere regels voor het gebruik van clouddiensten door overheidsinstanties. Daarmee konden we gegevensbescherming en soevereiniteit blijvend prioriteit geven.” Dankzij die vroege toepassing van een overheidscloudstrategie en daarbij de inzet voor datasoevereiniteit en -beveiliging, is Luxemburg koploper geworden op het gebied van de implementatie van een soevereine cloud binnen de EU, stelt Obertin niet zonder trots vast. Zelfs negen jaar na dato speelt de GovCloud nog steeds een centrale rol in de digitale infrastructuur van het groothertogdom als host van overheidsapplicaties en -data, met het hoogste niveau van gegevensbescherming, benadrukt Obertin. De omgeving wordt volledig beheerd door het CTIE (*Le Centre des technologies de l'information de l'État*), het IT-centrum van de overheid.

Integratie van AI

Het CTIE ziet ook toe op het implementeren van de nieuwste functionaliteit en meest actuele technologie bij de doorontwikkeling van overheidsdiensten. Twee relevante aspecten daarbij zijn de integratie van Artificiële Intelligentie (AI) technologie die GovCloud in staat stelt om platformen en Large Language Models (LLMs) te ondersteunen. LLMs die in AI-toepassingen worden gebruikt om tekstdata in menselijke taal om te zetten, te begrijpen, te genereren en te verwerken. “Door deze technologie intern te hosten, houden we de ontwik-

keling en implementatie van AI onder nationaal beheer en blijven we tegelijkertijd op één lijn met de strategische besluiten van ons land die direct met AI samenhangen”, aldus Obertin.

De tweede relevante ontwikkeling is dat het GovCloud-aanbod wordt uitgebreid met een directe verbinding met Clarence, de eerste losgekoppelde soevereine cloud die in Luxemburg is geïmplementeerd, een unicum voor Europa aldus Obertin. Clarence is gebaseerd op zogenoemde Google Distribu-

tion Cloud-technologie in een *air-gapped* configuratie. Dit betekent dat deze volledig geïsoleerd is van externe netwerken en daarmee ook het internet. “Die verbinding met Clarence stelt ons CTIE in staat om de meest innovatieve *hypervisor* technologie te gebruiken. Dit gebeurt uiteraard onder naleving van nationale en Europese regelgeving. Dit garandeert dat alle activiteiten en data strikt onder onze controle blijven en de vertrouwelijkheid en veiligheid van onze data worden geborgd.”

Hoe is Luxemburg erin geslaagd om de overheidscloud los te koppelen van het internet waardoor de digitale soevereiniteit wordt versterkt?

“Dat doen we op basis van onze strategie: ‘Accelerating Digital Sovereignty 2030’ (*The strategic initiative “Accelerating digital sovereignty 2030” - The Luxembourg Government*).¹ Met die implementatie versterken we de digitale soevereiniteit van Luxemburg met zes ondersteunende maatregelen, te weten:

- 1) governance en regelgeving;
- 2) vaardigheden en talenten;
- 3) onze infrastructuur;
- 4) ons ecosysteem van diensten;
- 5) onderzoek, ontwikkeling en innovatie, en
- 6) internationale samenwerking.”

Deze belangrijke pijlers zijn integraal onderdeel van de drie nationale strategieën voor data-, AI- en quantum-technologie en vormen samen een belangrijke ondersteuning voor de toekomstige ontwikkeling van de digitale soevereiniteit van Luxemburg, aldus de minister. “Ter illustratie: een belangrijk project binnen onze datastrategie is de ontwikkeling van soevereine infrastructuren binnen onze overheidscloud. Deze werken onafhankelijk van het publieke internet. Het CTIE beheert daarmee een afgeschermd en veilig communicatienetwerk dat alle overheidsinstanties verbindt met onze datacenters, waardoor het veilige gebruik van IT-diensten wordt gewaarborgd, en de vertrouwelijkheid van gedeelde gegevens worden beschermd.”



Stéphanie Obertin is sinds 17 november 2023 minister voor Digitalisering én minister voor Research en Hoger Onderwijs in Luxemburg, namens de Democratische Partij. Na studies wiskunde en geneeskunde werd Obertin partner in een huisartsenpraktijk. Ook was zij gedurende vele jaren in diverse bestuurlijke functies in de medische wereld actief. In 2018 maakte Obertin haar entree in de politiek.

Het GovCloud-aanbod wordt uitgebreid met een directe verbinding met de eerdergenoemde Clarence. “Zowel GovCloud als Clarence profiteren daarbij van onze ‘state-of-the-art’ infrastructuur en worden gehost in onze Tier IV-datacenters. Die bieden de hoogste standaard in Europa voor wat betreft redundantie, beveiliging en betrouwbaarheid. Ook dat versterkt onze autonomie.”

Valorisatie van gegevens

Om de soevereiniteit verder te versterken, hebben we onlangs wetsontwerp nr. 8395 ingediend. Dit wetsontwerp moet bijdragen aan de valorisatie van gegevens in Luxemburg. Het hoofddoel is het moderniseren van ons gegevensbeheer door een vertrouwenskader voor gegevensuitwisseling en -hergebruik te creëren. Dit in lijn met de EU-verordening 2022/868, de Data Governance Act. Die heeft tot doel om het vertrouwen in het vrijwillig delen van gegevens te versterken

door het reguleren van organisaties die vraag en aanbod op de datamarkten bij elkaar brengen. Het wetsvoorstel bevordert de valorisatie van gegevens en draagt bij aan de administratieve vereenvoudiging door het ‘once only’ principe. Daarbij hoeven burgers en bedrijven informatie slechts één keer aan de overheid te verstrekken, waarna overheidsinstanties die gegevens intern met elkaar kunnen uitwisselen. De strikte controle hierop vindt plaats door onze Nationale Commissie voor Gegevensbescherming (National Commission for Data Protection Grand-Duchy of Luxembourg – CNPD).”

Hoe voorziet Luxemburg erin om minder afhankelijk te worden van Big Tech?

“Wij investeren als Luxemburgse overheid steeds meer in open, interoperabele en soevereine technologie. Het CTIE speelt hierbij een sleutelrol door zorgvuldig software te selecteren die voldoet aan onze

“Digitale vooruitgang moet altijd in lijn blijven met Europese waarden”

hoge veiligheidsnormen en tegelijkertijd economisch rendabel is. Hoewel deze software van diverse leveranciers kan komen, waaronder die van de Big Tech, geeft het CTIE de voorkeur aan geavanceerde state-of-the-art oplossingen die veilig en gebruiksvriendelijk zijn. Wanneer de opties gelijkwaardig zijn, geeft het CTIE de voorkeur aan *on-premises* installaties om zo meer controle te kunnen behouden.”

Het CTIE zet bovendien actief opensourcetechnologie in op veel gebieden en ontwikkelt toepassingen die de privacy centraal stellen, waaronder een onafhankelijk videoconferentieplatform, via MyGuichet.lu, voor veilige interactie tussen burgers en overheidsdiensten. Wat betreft cloud- en datasoevereiniteit hanteert het CTIE een gemengde cloudstrategie. Alle kritieke systemen en gevoelige persoonsgegevens worden *on-premises* gehost in de eigen datacenters van het CTIE om maximale veiligheid en controle te kunnen garanderen. Voor bepaalde gespecialiseerde technologieën maakt het CTIE gebruik van lokale diensten van partners zoals Clarence of LU-CIX (LuxChat4Gov). Voor niet-kritieke en niet-gevoelige systemen kan het ook een beroep doen op Europese cloudproviders om zo innovatieve diensten aan overheidsinstanties te kunnen aanbieden.

Digitale soevereiniteit

Op Europees niveau is Luxemburg een ‘deelnemende waarnemer’ in de European Digital Infrastructure Consortium (EDIC) op het gebied van digitale gemeenschapsgoederen (digital commons). Dit is een samenwerkingsverband dat zich richt op de ontwikkeling, het onderhoud en de uitbreiding van digitale producten en diensten in Europa. Een initiatief van meerdere landen, waaronder Nederland, Frankrijk, Estland en Duitsland, vanuit de visie dat als Europa meer producten en diensten zelf ontwikkelt, dit direct bijdraagt aan het versterken van de Europese digitale soevereiniteit.

Daarnaast promoot Luxemburg zelf open-source ecosystemen en draagt het bij aan *communities* zoals de Open-Source Conference, de Matrix Conference en de Interoperable Europe Board, stuk voor stuk pleitbezorgers voor digitaal soevereine en transparante alternatieven waar het gaat om *proprietary* software en tools. “We organiseren ook *hackathons* en innovatiesprints om de ontwikkeling en het gebruik van soevereine digitale software te stimuleren die daarbij is afgestemd op de eisen en wensen van de lokale publieke sector”, meldt Obertin. Ze benadrukt dat genoemde activiteiten onderdeel zijn van de prioriteitstelling zoals vastgelegd in de strategieën voor data, AI en quantumtechnologie. “Daarbij ligt de nadruk op autonomie, interoperabiliteit

“

Autonomie, interoperabiliteit en verantwoorde innovatie zijn de hoekstenen van onze digitale soevereiniteit

”

en verantwoorde innovatie - de hoekstenen van onze digitale soevereiniteit.” “Om onze inspanningen verder te stroomlijnen en te zorgen dat we onze onderscheidende en toekomstgerichte positie behouden, hanteren we als regering een aanpak waarbij geavanceerde technologiestrategieën op coherente wijze overheidsbreed worden geïntegreerd. De implementatie van dit soort projecten zal worden gefaciliteerd door nieuwe, specifieke begrotingsmiddelen voor de periode 2025-2030.”

Omdat datasoevereiniteit een prioriteit is voor Luxemburg, wordt de lokale hosting van gevoelige data ondersteund met behulp van diensten zoals Clarence, Lux-Chat (een beveiligd communicatieplatform) en Mistral AI, waarbij deze laatste generatieve AI-mogelijkheden *on-premises* biedt voor de Luxemburgse staat. “We hanteren daarvoor ook een duidelijk en publieksvriendelijk kader voor data governance, inclusief een one-stop-shop voor de Data Governance Act en het ‘*once only*’ principe, waardoor de administratieve lasten en -complexiteit worden verminderd. Daarnaast investeren we in veilige dataverwerkingsomgevingen, inclusief de analyse van differentiële privacytechnieken en de ontwikkeling van synthetische datafabrieken.” Deze laatste simuleren kenmerken van relaties tussen personen en objecten, waardoor de realiteit kan worden nagebootst zonder dat de persoon of het object geïdentificeerd wordt.

Quantumtijdperk

Om volledige controle te behouden over datastromen en digitale infrastructuur, omvatten alle strategische initiatieven ook supercomputers: MeluXina, MeluXina-AI en MeluXina-Q. High-performance systemen die draaien op hernieuwbare energie. Rond de MeluXina-AI heeft Luxemburg ook een AI-fabriek gebouwd, een van de eerste in Europa.

Het groothertogdom erkent ook het strategische belang van quantumtechnologie, aldus Obertin. “We bereiden ons gedegen voor op het naderende quantumtijdperk. Zo zijn LuxQCI en EuroQCI initiatieven die op basis van Quantum Key Distribution (QKD) de implementatie van quantumcommunicatienetwerken mogelijk maken waarmee we onze cyberbeveiliging verder kunnen verbeteren.”

Ter verduidelijking: QKD is een methode die gebruikmaakt van de principes van de quantummechanica om een veilige, geheime sleutel tussen twee partijen te distribueren. Luxemburg neemt ook deel aan quantuminfrastructuurprojecten in de ruimte zoals de ESA EAGLE-1-satelliet voor veilige quantumcommunicatie. De MeluXina-Q

quantumcomputer wordt ingezet voor onderzoek en simulatie. “We bereiden ons daarmee voor op post-quantumcryptografie om ‘nu opslaan, later ontsleutelen’-bedreigingen te voorkomen.”

Hoe zorgt Luxemburg ervoor dat zijn digitale strategie aansluit bij Europese waarden zoals privacy, ethiek, mensenrechten, transparantie en controle over persoonsgegevens?

“Dat doen we door die Europese kernwaarden te verankeren in onze regelgeving, processen en governance. Initiatieven hier sluiten aan op EU-kaders zoals de GDPR (in Nederland bekend als de AVG), de AI-wet en het AI-Verdrag van de Raad van Europa, wat een sterke juridische en ethische basis garandeert. Financieringsprogramma’s zoals de Tech-inGov-oproep voor projecten worden begeleid door een ethische adviesgroep. Daarnaast heeft ons CTIE een eigen projectmanagementmethode ontwikkeld die alle benodigde tools biedt om ervoor te zorgen dat IT-projecten voldoen aan EU-regelgeving en hun doelstellingen behalen op het gebied van functionaliteit, planning en budget. De nieuwste ontwikkelingen omvatten ook de integratie van de vereisten die de AI-wet stelt.”

Korte lijnen

Wat Luxemburg onderscheidt zijn “korte lijnen”, onderstreept Obertin: “We beschikken over een actief betrokken, flexibel ecosysteem dat het gemakkelijk maakt om principes zoals die van het Europees Interoperabiliteitskader snel toe te passen. Het zorgt voor samenhang tussen instellingen en maakt ethisch, interoperabel en mensgericht ontwerp mogelijk. We zijn toegewijd aan betrouwbare en verklaarbare AI (XAI: Explainable AI is een reeks processen en methoden waarmee gebruikers de resultaten en output van algoritmen kunnen begrijpen en vertrouwen - red.).” De minister noemt een drietal belangrijke projecten in dit kader:

- LLM4GOV, een benchmarkinginitiatief voor grote taalmodellen (LLM’s) die zijn afgestemd op de behoeften van de publieke sector en die richtlijnen bieden voor duurzaamheid, prestaties en ethisch gebruik.
- 4LM, een juridisch taalmodel met als basis de Luxemburgse en EU-jurisprudentie, ter ondersteuning van juristen en digitale rechtspraaktoepassingen.
- LLMs4EU, dat bijdraagt aan de ontwikkeling van interoperabele en transparante Europese AI-modellen.

Naast eerdergenoemde investeringen in soevereine infrastructuur zoals Clarence Cloud en Secure Processing Environments, ontwikkelt Luxemburg ook zogenaamde *AI regelgevende sandboxes* (een virtuele en afgeschermd computeromgeving) waar AI-systemen kunnen worden getest en gevalideerd voordat ze breder worden



© Ministry for Digitalisation / Sophie Margue

geïmplementeerd. Ook investeert Luxemburg in de European Digital Identity Wallet die veilige authenticatie in de hele EU mogelijk maakt. De wallet houdt zich aan kernprincipes van de EU als: gebruikerscontrole over persoonsgegevens, data-minimalisatie, privacy, beveiliging, transparantie, EU-brede interoperabiliteit en inclusiviteit. Want zoals Obertin stelt: “Digitale vooruitgang moet altijd in lijn blijven met Europese waarden.”



Gijs Tuinman is sinds 2 juli 2024 staatssecretaris (thans demissionair) van Defensie voor de BBB. Hij werd vanwege zijn verdiensten tijdens diverse missies in Afghanistan en Afrika in 2009 onderscheiden met de Bronzen Leeuw, de op één na hoogste militaire onderscheiding, uitgereikt door koningin Beatrix. In 2014 werd Tuinman door koning Willem-Alexander tot Ridder der Militaire Willems-Orde der vierde klasse geslagen.

Digitale transformatie bij Defensie

Gedurende tientallen jaren was het nagenoeg ondenkbaar dat we in Europa betrokken zouden raken bij een oorlog op eigen grondgebied. Echter, de praktijk is weer eens weerbarstig gebleken. Vrijheid en veiligheid zijn niet langer vanzelfsprekend en vereisen defensieve gereedheid. “Onze primaire focus ligt bij gevechtskracht”, stelt demissionair staatssecretaris van Defensie, Gijs Tuinman. De ontwikkelingen op het slagveld en digitaal gaan in hoog tempo. Om die reden heeft hij op 3 juli jl. de ‘Digitale Transformatie Strategie’ (DTS) naar de Tweede Kamer gestuurd.

Een strategie die als doel heeft: het vergroten van de gevechtskracht van Defensie door de digitale slagkracht te versterken en te kunnen versnellen met oplossingen, zoals cloud en satellietcommunicatie, om de strategische soevereiniteit te vergroten. Die DTS (zie kader) kan worden gezien als vervolg op de Defensienota 2024, getiteld ‘Sterk, slim, samen’, waarbij ook ‘gevechtskracht door rekenkracht’ is benoemd, om te duiden dat veel dreiging uit het digitale (cyber)domein komt.

De DTS gaat vergezeld van een uitvoeringsagenda. “Daar staan programma’s in die we moeten gaan uitrollen, en daar is een hoop geld mee gemoeid”, aldus Tuinman. Hij noemt programma’s op het vlak van cloud, AI en *battle management* - voor de Landmacht, de Marine, het Defensie Cyber Commando (DCC) en het Commando Lucht- en Ruimtestrijdkrachten (CLRS). Die laatste, CLRS, is de nieuwe naam van het voormalige Commando Luchtstrijdkrachten (CLSK). Voor NAVO-bondgenoten heet dit commando tegenwoordig ‘Royal Netherlands Air and Space Force’. Een aanpassing die gedaan is omdat de geopolitieke strijd zich steeds meer afspeelt in de ruimte. Om die reden heeft Tuinman op 8 september jl. ook groen licht gegeven om samen met Nederlandse kennisinstellingen en bedrijven versneld soevereine Nederlandse satellietcapaciteit te gaan ontwikkelen. “We noemen dat ‘*Military use of Space*’ en over anderhalf jaar gaan de eerste satellieten al de lucht in. Een andere belangrijke ontwikkeling is lasercommunicatie. Deze maakt gebruik van satellieten en is lastig om te *jammen* (opzettelijke verstoring van draadloze signalen - red.) en heeft in principe onbeperkte bandbreedte. Het betreft soevereine capaciteit, waardoor we van niemand afhankelijk zijn.”

Cultuuromslag

“Wat meespeelt in de digitale transformatie is dat we ook onze manier van werken moeten aanpassen; onze cultuur moet om. De krijgsmacht er is om te beschermen wat ons dierbaar is. Dat doen we op basis van afschrikking. Het principe van afschrikking is dat je eigenlijk niet wilt hoeven vechten omdat je zo goed bent in vechten, maar dat je zorgt dat je in gereedheid bent. Dat noemen we gevechtskracht. Gevechtskracht bestaat uit de personele gereedheid plus de materiële gereedheid. Je kunt wel de mensen en de spullen hebben, maar als je die niet bij elkaar weet te brengen, als er geen aandacht is voor geoefendheid, dan is van gereedheid geen sprake en dus ook niet van gevechtskracht en dus van afschrikking.”

Naast die traditionele personele en materiële gereedheid is er ook de noodzaak van IT-gereedheid, “want wat je wilt is snellere en betere besluiten kunnen nemen dan je tegenstanders. En dat gaat steeds sneller, ook doordat de technologie het mogelijk maakt. Dat zien we ook dagelijks in Oekraïne”, aldus Tuinman.

Oorlogsvoering, afschrikking, het is anno 2025 zonder digitale component onmogelijk. Om die reden is geoefendheid een simultane operatie tussen veld en simulatie. Het fysieke oefenterrein wordt samengebracht met een simulatieruimte op een kazerne, legt Tuinman uit. Hij heeft de Tweede Kamer per brief (3 februari 2025) geïnformeerd over ‘*Operational Training Infrastructure*’ (OTI). In de brief wordt aangegeven dat Defensie voornemens is om gespecialiseerde infrastructuur te verwerven die ondersteunt in het effectief trainen in realistische ➤

en veilige omstandigheden. “OTI bouwt een omgeving waarin je scenario’s kunt trainen – bijvoorbeeld dat je gejamd wordt – met zowel echt vliegende F-35’s als gesimuleerde F-35’s, en gesimuleerde dreigingen. Het is dus de echte wereld en een gesimuleerde wereld samen in een digitale virtuele omgeving.”

Dat klinkt als een computergame...

“Ja, maar niet alleen een computergame want dan zou je met z’n allen in de simulator zitten. Er wordt bij OTI ook ‘live’ gevlogen en als die F-35 een bepaalde manoeuvre uithaalt in een bepaald gebied, dan krijgt degene in de simulator ook een *threat warning* – dat is hoe digitalisering daadwerkelijk in onze bedrijfsvoering zit om besluitvorming te optimaliseren.”

Tijdigheid

Het credo van Tuinman is: stappen zetten. “Je kunt wel blijven overleggen en om je heen blijven kijken, maar je moet ook door. En dat is wat we nu ook gewoon doen. Tot voor kort keken we voornamelijk naar prijs en kwaliteit; en dat moet je eigenlijk interpreteren als: ‘de allerbeste kwaliteit voor de allerlaagste prijs’. We kijken

“
Wat meespeelt in de digitale transformatie is dat we onze manier van werken moeten aanpassen

”
Het hoeft niet altijd de meest uitgesproken specs te hebben, dat we er zo naar kijken is ook een cultuuring. Tijdigheid, dat vind ik eigenlijk het allerbelangrijkste. Dus dat het tijdig leverbaar en inzetbaar is. Natuurlijk kijken we ook naar herkomst, wat kan er uit Nederland komen, wat uit Europa? Je moet ook die drie *hyperscalers* niet uitsluiten.”

Die tijdigheid is extra relevant nu, gezien de geopolitieke ontwikkelingen?

Tuinman glimlacht: “Voor mij gaat het gewoon niet snel genoeg en dat is niet omdat ik dat vind, we zien allemaal wat er in Oekraïne gebeurt. Als je naar Oekraïne kijkt, dan zie je drie grote *take-aways*. De eerste zijn drones en daarmee de rol van autonome systemen; autonoom in die zin dat het mission modules zijn die je voor bepaalde taken en op bepaalde schaal kunt inzetten. Het tweede is *Deep Precision Strike*, hoe zorg je ervoor dat je dreiging heel diep in bijvoorbeeld het achtergebied van Moskou kunt inzetten? Bij het inzetten van een raket komt veel digitalisering kijken. Zo’n raket op zich heeft nul dreiging,

heeft nul afschrikking maar door toepassing van *electronic countermeasures* – en daar zit een database achter met heel veel rekenkracht die informatie verzamelt en berekent en op basis daarvan voorspellingen doet – kun je dat effectief inzetten. Het derde aspect zijn de systemen en de netwerken die er liggen en die we eigenlijk niet zien. Dat gaat echt over de vraag hoe Oekraïne het voor elkaar krijgt, terwijl alles wordt kapot gebombardeerd – want overal waar je een radio aanzet of een golflengte maakt of iets uitzendt, vergroot dat de kans op een bom – om stand te houden. Dat doen ze echt *cutting edge* met een combinatie van allerlei verschillende transmissiesystemen en een innovatieve Delta app. Dat is de reden dat Oekraïne überhaupt nog bestaat. En dat ze hun militairen die eerste maanden konden betalen is omdat ze met *hyperscalers* hebben samengewerkt om hun data op het gebied van betalingsverkeer snel het land uit te krijgen. Daar moest wel een speedwet aan te pas komen. Maar hun overtuiging was: als je je digitale soevereiniteit wilt behouden in situaties als deze, dan moet je bepaalde data per definitie niet in je eigen land willen hebben. Dat vindt navolging in de Baltische staten met *data embassy’s* en ik denk dat wij hier ook wel weten dat we daar naartoe moeten, maar die strategische dialoog hebben we nog niet scherp met elkaar.” In het kader van tijdigheid komen er veel simulators en satellieten bij, is er net een Twin Datacenter gelanceerd en worden stappen gezet in het kader van de modale cloudstrategie.

Helpt het op deze bestuurdersstoel om een militaire achtergrond te hebben?

“Ja, jawel. Je kunt af en toe goed doorvragen en als het een *bullshit* verhaal is, dan prik je daar doorheen. De andere kant is natuurlijk dat alle ontwikkelingen elkaar zo snel opvolgen, dat je jezelf ook echt open moet stellen om continu geïnspireerd en getriggerd te worden op jouw eigen beeld van de werkelijkheid. En het beeld van een paar jaar terug representeert niet meer de werkelijkheid van nu, dat is een feit.”



IT uit de kraan

Het digitale fundament is in Nederland goed op orde, vindt Tuinman. “Maar we moeten er wel in blijven investeren!” Hij refereert aan cybersecurity fusion centers, de noodzaak van een veilige, geïntegreerde, snelle cloudsolution waarop zogenaamde Large Language Modellen (LLM’s) kunnen draaien. Om die reden heeft Defensie ook geld vrijgemaakt voor de toekomstige AI-fabriek in Groningen. Een ander aandachtspunt van de bewindsman is samenhang brengen in het IT-portfolio van Defensie. Aan een brief daarover aan de Tweede Kamer wordt gewerkt. “We leven in een andere wereld en sommige projecten zijn we vijf, zes soms wel tien jaar geleden opgestart met een doelstelling en een plan van aanpak, vaak in een context van ‘gouden bergen, minimaal budget’. Want als je iets met IT wilde, dan moest je ook meteen een wereld aan problemen oplossen, bij wijze van spreken.”

Grote, complexe projecten opknippen is in dit geval de les die is geleerd. “Er moet meer IT uit de kraan”, noemt Tuinman dat, niet alles onnodig ingewikkeld maken. “Geweldig hoor die lange termijn plannen, maar hier en nu moet ik gewoon aan een knop kunnen draaien.”

Tuinman noemt het programma Grensverleggende IT (GrIT) exemplarisch voor een gefaseerde aanpak door middel van opeenvolgende releases. “We werken aan drie pijlers. De eerste – en daaraan werken we nu het allerhardst – is zorgen dat we IT naar onze gevechtseenheden krijgen. De tweede pijler betreft de IT voor onze IT, bijvoorbeeld datacenters. De derde pijler gaat over IT voor de bedrijfsvoering, zoals de werkplek. Daar noem ik bijvoorbeeld de vervanging van beeldschermen als project, dat is iets dat we naar achter hebben geschoven. Ja, een oud beeldscherm werkt allicht minder prettig, maar er stroomt geen bloed uit als we er nog een paar jaar langer mee moeten werken.”



“

Tijdigheid, dat vind ik eigenlijk het allerbelangrijkste

”

In het kader van de eerste pijler is recent een *private cloud* omgeving voor het Duits/Nederlandse legerkorps uitgerold. “Die hebben een rol binnen de NAVO en daar hebben ze nu de eerste oefeningen mee gedraaid. We hebben er bewust voor gekozen om dit niet in een laboratoriumomgeving te ontwikkelen. Wat wel de normale gang van zaken is: opbouwen totdat alle functionaliteiten werken, dan migreren en dan als een gek koppelingen bouwen. Maar in dit geval was de doelstelling: geen koppelingen, maar functionaliteiten zo snel mogelijk naar de systemen van de *warfighters* brengen en leren van hun feedback.”

Hoofdkwartier

Een tweede prioriteit is de koppeling van de *battle management* systemen aan het operating systeem. Dat wordt nu versneld door de recente lancering van het Netherlands Joint Force Command (NLD JFC), het hoofdkwartier voor militaire operaties. “Dat gaat niet over functionaliteit of over mensen maar over hoe je de informatiestormen bij elkaar brengt. Daarin hebben we keuzes gemaakt. Want je kunt bouwen met Lego, met Duplo, met Knex, maar ik kan je een ding zeggen: als de een Lego gebruikt, de ander Duplo en weer een ander Knex, dan heb ik een probleem. Want dan moet ik straks nog een keer 1 miljard euro uitgeven om die weer met elkaar te gaan verbinden. Wat je eigenlijk wilt, is meer agnostisch bouwen. Er is in het verleden best wel kritiek geuit op GrIT, ook vanuit de Tweede Kamer, maar het is goed dat we destijds die keuze hebben gemaakt en nu kunnen doorgroeien. Wat dat betreft is GrIT onze Lego.” Hij geeft aan dat ook programma's als FOXTROT (voor de modernisering en vervanging van tactische, land gebonden communicatiemiddelen) en Roger (SAP S/4 HANA – het nieuwe systeem voor de bedrijfsvoering) op GrIT aansluiten. “Roger brengt SAP tot in de loopgraaf”, aldus Tuinman.

Digitale Transformatie Strategie (DTS)

De Digitale Transformatie Strategie richt zich op vijf samenhangende speerpunten:

1. Communicatie en digitale samenwerking

Defensie investeert in veilige en effectieve digitale communicatie tussen operationele domeinen en met civiele en militaire partners. Dit bevordert snelheid en flexibiliteit, vergroot het aanpassingsvermogen in uiteenlopende scenario's en draagt bij aan het behouden van communicatie tijdens militaire operaties. Investeren in Europese satellietcommunicatie en een robuuste mix van communicatiemiddelen die verschillende soorten verstoringen aankunnen, zijn daarbij van cruciaal belang.

2. Digitaal fundament

Een robuust digitaal fundament garandeert in uiteenlopende omstandigheden toegang tot opslag- en rekenkracht. Dit maakt real-time data-analyse en AI-ondersteuning mogelijk, versterkt de informatiepositie en bevordert beslisdominantie. Daarom zet Defensie in op de integratie van diverse cloud- en edge-oplossingen.

3. Data, kunstmatige intelligentie en autonomie

Slimme algoritmen en autonome systemen versterken de operationele slagkracht van Defensie. Verhoogde inzet op dit terrein leidt tot snellere en beter onderbouwde besluitvorming. Succesvolle toepassing vraagt om een verantwoord en effectieve inzet van AI, met oog voor schaalbaarheid, integratie en ethische kaders. Defensie kan en moet op het gebied van AI en autonomie internationaal leidend zijn.

4. Elektromagnetisch spectrum, cyber en redundantie

De toenemende digitalisering vergroot de dreiging in het cyberdomein, binnen het elektromagnetisch spectrum en voor fysieke infrastructuur. Inzet van tegenstanders op deze terreinen kan het vermogen tot informatieverwerving en communicatie ernstig verstoren. Daarom investeert Defensie in cyberweerbaarheid, EMS-capaciteiten en redundantie.

5. Digitaal aanpassingsvermogen

Beschikken over digitale middelen is niet voldoende; het gaat om het effectief en adaptief toepassen ervan. Doorlopende innovatie en het snel kunnen inzetten van technologie voor operationeel voordeel zijn cruciaal. Dit vraagt om nauwe samenwerking tussen marktpartijen, ontwikkelaars en gebruikers (*de warfighter*).

ADVERTORIAL

Het belang van soevereine oplossingen

In onze IT-wereld zien we steeds vaker de wens voor een onafhankelijk, oftewel een soevereine benadering van IT opkomen. Geopolitieke ontwikkelingen spelen hierbij een prominente rol.

Organisaties dienen door complexe regelgevingen te navigeren en willen gevoelige data binnen beschermde kaders houden. Een soevereine cloudoplossing zorgt er in essentie voor, dat data binnen zelf gedefinieerde en vaak binnen bepaalde geografische grenzen blijft, waardoor organisaties kunnen voldoen aan regionale wetten en regelgevingen, betreffende privacy, gegevensresidentie en beveiliging. Dit is essentieel voor sectoren zoals overheid, gezondheidszorg, financiële dienstverlening en andere branches waar strenge regelgeving geldt.

Door gebruik te maken van soevereine cloudoplossingen, behouden organisaties volledige zeggenschap over hun data en vermijden ze risico's rond extraterritoriale toegang of grensoverschrijdende verplaatsing, zonder verlies van flexibiliteit.

AI meerdere decennia levert Dell Technologies technische oplossingen in private cloudinfrastructuur met een hoge mate van prestatie, gebruikersvriendelijkheid, automatisering en veiligheid. Hiermee helpt Dell Technologies organisaties te voldoen aan de hoogste security standaarden en

regelgevingen. Onlangs heeft Dell Technologies een nieuwe basis gelegd voor een geautomatiseerd platform om met een herbruikbare infrastructuur verschillende platformen aan te bieden, waarbij de mate van flexibiliteit en continuïteit voor een 'onzekere' toekomst wordt gewaarborgd.

In het thema van soevereine infrastructuur bundelen Atos en Dell Technologies hun krachten om soevereine oplossingen te leveren, waarmee organisaties strikte controle over hun data behouden en daarmee te voldoen aan lokale regelgeving. Deze samenwerking combineert de expertise van Atos op het gebied van het beheer van veilige digitale platforms met Dell Technologies' robuuste, schaalbare infrastructuur, waardoor oplossingen ontstaan die privacy, security en compliance waarborgen.

Moderne IT-omgevingen, inclusief de toepassing van kunstmatige intelligentie tot op het gebied van generatieve AI en agentic AI zijn hiermee mogelijk met verhoogde mate van controle en prestatie. Deze samenwerking stelt publieke en private organisaties in staat om veilig en innovatief te opereren met lokaal beheerde gevoelige informatie.

Jean Jacques Kroesbergen
Sales Lead
Dell Technologies Netherlands
0615629320

DELL
Technologies





Quirine van Eeden is onderzoeker bij het Rathenau Instituut waar zij onderzoek doet naar de maatschappelijke verantwoordelijkheid van technologiebedrijven. Van Eeden, die rechtsgeleerdheid studeerde, richt zich op de afhankelijkheid van de samenleving van Big Tech-bedrijven en de impact daarvan op maatschappelijke verhoudingen en onze democratische rechtsstaat. Ze was projectleider van het team bij het Rathenau Instituut dat recentelijk een drieluik heeft gepubliceerd, genaamd 'van digitale afhankelijkheid naar digitale autonomie'.¹ Met haar onderzoek wil ze bijdragen aan een digitale toekomst die werkt voor iedereen.

Digitale afhankelijkheid zet regie over publieke sectoren op het spel

In de zomer van 2024 werden in Nederland ziekenhuisactiviteiten teruggedroefd en duizenden vluchten geannuleerd door een wereldwijde storing. De reden? Een fout in een software-update van beveiligingsbedrijf CrowdStrike waardoor 8,5 miljoen Windows-computers het lieten afweten. Een ogenschijnlijk kleine fout heeft ontwrichtende gevolgen voor onze samenleving door de hoge concentratie van diensten bij een handjevol bedrijven. Daarom wint het feit dat overheden steeds meer leunen op de clouddiensten van (met name) Microsoft terecht aan aandacht in de Tweede Kamer.

Afhankelijkheid van Big Tech in de samenleving

Maar er is meer aan de hand. Niet alleen de overheid raakt steeds afhankelijker van een handjevol aanbieders. We raken als samenleving afhankelijk. Ook in het onderwijs, wetenschap, journalistiek en gezondheidszorg trekken experts en professionals aan de bel (Rathenau 2025). De docent, de huisarts, de bankmedewerker en de wetenschapper: geen van hen kan hun werk meer doen zonder

de diensten van grote Amerikaanse tech-bedrijven. Die afhankelijkheid van enkele grote tech-bedrijven beperkt zich bovendien niet tot clouddiensten: sectoren worden ook steeds afhankelijker van andere diensten van dezelfde bedrijven. Daarbij valt de denken aan sociale mediaplatformen, zoekmachines, smartwatches en laptops. Gemeenten gebruiken WhatsApp en Facebook om inwoners te bereiken, scholen maken gebruik van Chromebooks en ziekenhuizen zetten wearables in om de gezondheid van patiënten te monitoren.

Dreiging van acute problemen

De prijs van afhankelijkheid is hoog. In het politieke en publieke debat gaat het dan al snel over de risico's met acute gevolgen. Want door al je eieren in hetzelfde mandje te leggen, word je een aantrekkelijk doelwit voor kwaadwillenden en ben je kwetsbaar voor uitval. Een Rijksbrede risicoanalyse van de NCTV² achtte in 2022 al een aanval op een cloudprovider 'waarschijnlijk' en de consequenties daarvan als 'zeer ernstig'.

Ook kan de Amerikaanse overheid onder

voorwaarden inzage eisen in gegevens van personen buiten de Verenigde Staten. De grote aanbieders van clouddiensten waar veel publieke organisaties gebruik van maken, de zogeheten hyperscalers Amazon, Google en Microsoft, hebben zich namelijk te houden aan Amerikaanse wetgeving zoals de Amerikaanse CLOUD Act en sectie 702 van de Foreign Intelligence Surveillance Act (FISA). Daarbij maakt het niet uit waar ter wereld je data-center precies staat.

Dat laatste risico is in een nieuw licht komen te staan sinds het aantreden van de regering-Trump, die signalen afgeeft dat hij zich keert tegen de Europese aanpak om de macht van Big Tech in te dammen. Onze afhankelijkheid kan dus ook als geopolitiek drukmiddel worden gebruikt. De toenadering tussen de Amerikaanse president en een aantal Big Tech-bedrijven maakt afhankelijke partijen nog kwetsbaarder. Dat gemeenten onder tussen laten weten: "Er mag niets met Microsoft gebeuren,³ want dan hebben we een probleem", toont aan hoe riskant de huidige situatie is.

Maatschappelijke opdracht onder druk

De veiligheids- en privacyrisico's van afhankelijkheid worden inmiddels breed erkend. Maar er staat meer op het spel: wanneer publieke organisaties hun digitale processen uitbesteden aan Big Tech-bedrijven, geven ze geleidelijk de regie over kernprocessen uit handen aan deze bedrijven.

Veel publieke organisaties draaien op de diensten van Big Tech, maar weten vaak niet precies hoe de technologie van deze bedrijven werkt. De controle op het onderhoud en de beveiliging neemt af. Ook de technische kennis gaat achteruit. Afhankelijke partijen hebben bovendien steeds minder te kiezen tussen verschillende diensten, en de onderhandelingsruimte met deze bedrijven is beperkt. Daardoor krijgen deze bedrijven steeds meer invloed op de koers van publieke organisaties, zonder dat daar bewust voor is gekozen. Uiteindelijk kan hierdoor de maatschappelijke opdracht van deze organisaties onder druk komen te staan. Op grond van welke onderwijsprincipes richten platforms een digitaal klaslokaal in? Wie heeft controle over de data van patiënten? Hoe bepalen sociale media welk bereik journalisten krijgen?

Afhankelijkheid afbouwen

Om te voorkomen dat we de koers van onze digitale samenleving steeds meer laten bepalen door een aantal Big Tech-bedrijven, moeten we onze afhankelijkheid afbouwen. Afbouwen van afhankelijkheid betekent kiezen voor andere diensten dan die van de grote tech-bedrijven. Alleen zo kan de autonomie van publieke organisaties om hun maatschappelijke opdracht uit te voeren, behouden blijven.

Dat gaat niet over één nacht ijs, en eenvoudig wordt het evenmin. De kernprocessen van organisaties zijn immers vervlochten met de diensten van Big Tech. De overheid kan een leidende rol spelen: coördineer en bundel de vraag naar digitale oplossingen, wend als overheid je inkoopmacht aan om alternatieve aanbieders van de grond te laten komen, en benut de kennis van andere organisaties die zo'n overstap in gang hebben gezet.

Voorkom nieuwe afhankelijkheden door AI

Dat betekent natuurlijk ook dat we nieuwe afhankelijkheden moeten voorkomen.

Het gebruik van generatieve AI-diensten neemt een vlucht in publieke sectoren (Rathenau 2025). Volgens de Algemene Rekenkamer is de verwachting dat generatieve AI een grotere plek gaat krijgen in de bedrijfsvoering van de overheid. Ook in de Nederlandse Digitaliseringsstrategie (NDS) is aandacht voor het "versnellen" van de inzet van AI binnen de overheid. Deze diensten zijn grotendeels in handen van dezelfde bedrijven (Rathenau 2025).

Als we nu 'versnellen', raken we niet alleen afhankelijker, we snijden onszelf ook op een andere manier in de vingers: we vergroten op deze wijze ook het succes van huidige taalmodellen en daarmee uiteindelijk de voor-sprong van deze diensten op kleinere alternatieven. Doorgaan op dezelfde voet betekent dat Big Tech-bedrijven alsmaar machtiger worden en onze afhankelijkheden groter. De prijs daarvan is hoog: publieke actoren verliezen hun sturingsmogelijkheden. Zo raken publieke waarden uit het zicht en kan het functioneren van de democratische rechtsstaat onder druk komen te staan. Hoogste tijd dus om andere keuzes te maken. Daar kunnen we vandaag al mee beginnen, bijvoorbeeld met de indrukwekkende waslijst⁴ aan geschikte alternatieven

die Public Spaces voor ons op een rij gezet.

Overzicht van de risico's van digitale afhankelijkheid



¹ <https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/samenleving-kwetsbaar-digitale-afhankelijkheid-meer-dan-cloud-bij-de-overheid>

² <https://www.rijksoverheid.nl/documenten/rapporten/2022/07/31/rijksbrede-risicoanalyse-nationale-veiligheid-2022>

³ <https://www.binnenlandsbestuur.nl/digitaal/it-personeel/er-mag-niets-met-microsoft-gebeuren-want-dan-hebben-we>

⁴ <https://spoelekenen.publicspaces.net/tools>

Eddie van Marum is sinds 2 juli 2024 (inmiddels demissionair) staatssecretaris op het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) met als portefeuilles Herstel Groningen, Koninkrijksrelaties en Digitalisering. Van Marum was eerder Statenlid in Groningen namens de BBB.

Nederlandse Digitaliseringsstrategie: samen doen

Voor demissionair staatssecretaris Eddie van Marum draait digitalisering niet om systemen, maar om mensen. Zijn doel: één overheid die burgers en ondernemers digitaal ondersteunt én beschermt. Maar dat vraagt om stevige keuzes. “Als het volgende kabinet echt stappen wil zetten, moet er een substantieel budget komen. En wat mij betreft behoort digitalisering standaard aan tafel te zitten bij de ministerraad.”

“Digitale diensten worden steeds meer een publieke voorziening, net als energie, onderwijs en voedselvoorziening”, zegt Van Marum, zittend aan de grote tafel in zijn werkkamer op het ministerie van BZK. Naast hem ligt zijn iPad, waarmee hij beleidsdocumenten en Kamerbrieven aftekent. “De maatschappij digitaliseert in een razend tempo. Dat heeft veel voordelen, maar het brengt ook risico’s met zich mee. Want het is niet vanzelfsprekend dat alles blijft werken.” Storingen en digitale aanvallen zijn niet ondenkbaar in het huidige geopolitieke klimaat. Digitale weerbaarheid is dan ook een speerpunt in de Nederlandse Digitaliseringsstrategie (NDS), die de demissionair staatssecretaris vlak voor de zomer heeft gelanceerd. “Stel je voor dat je opeens geen toegang meer hebt tot je zorggegevens

of spaargeld, of dat je persoonlijke gegevens opeens op straat liggen. We weten inmiddels dat dat kan gebeuren. Dat kan zorgen voor een deuk in het vertrouwen dat mensen hebben in de overheid. En dat moeten we voorkomen.”

Vertrouwen

Het woord ‘vertrouwen’ gebruikt hij niet toevallig. Van Marum is ook demissionair staatssecretaris Herstel Groningen. Hij spant zich iedere dag in om het vertrouwen te herstellen bij mensen die te maken kregen met aardbevingsschade. “Ik zie in Groningen hoe belangrijk het is om bij het maken van beleid de mens niet uit het oog te verliezen. Dat gevaar ligt altijd op de loer, ook bij

digitalisering, misschien wel juist bij deze portefeuille. De digitale wereld verandert razendsnel. We maken als overheid gebruik van cloud, data en AI, en straks misschien wel quantumtechnologie. Maar de vraag die daarbij altijd leidend moet zijn is: wat hebben burgers en ondernemers nodig, en hoe kunnen we hen beschermen? Dat is de kern van de Nederlandse Digitaliseringsstrategie.”

Wat gaat de NDS precies veranderen?

“Door deze strategie werken gemeenten, provincies, waterschappen en het rijk echt intensief samen. Zo versterken we de digitale basis van Nederland. Dat is essentieel voor goede dienstverlening aan burgers en

centrale regie. Je ziet ook dat er door de NDS een sterke beweging is ontstaan bij alle overheden: iedereen wil meer dan ooit samenwerken, dat is echt een unicum.”

Beweging

De beweging begint bij de overheden zelf, stelt Van Marum. “Zij moeten samen tot een investeringsagenda komen. Er liggen veel goede plannen: voor systemen die beter op elkaar aansluiten, voor een soevereine cloud, en voor slimmer gebruik van data. Maar we kunnen niet alles tegelijk. Eerst is nu het programmateam van BZK aan zet, met medeoverheden en publieke dienstverleners als gelijkwaardige partners. Zij moeten gezamenlijk keuzes gaan maken: welke prioriteiten uit de NDS pakken ▶

“

Je moet het gevoel krijgen dat je met één overheid te maken hebt en meteen wordt geholpen

”

bedrijven. We willen mensen bijvoorbeeld zo veel mogelijk op één plek helpen, en niet van loket naar loket sturen.”

“Maar het gaat ook om veiligheid. Tot nu toe heeft iedere overheid zijn eigen systemen, clouds en standaarden. Dat lijkt handig, maar het maakt ons kwetsbaar. Als systemen niet op elkaar aansluiten, kun je ze ook niet samen verdedigen. En als de ene organisatie bijvoorbeeld een lek heeft, kan dat ook gevolgen hebben voor anderen. Mijn voorganger Zsolt Szabó zag dat scherp en zette de NDS in de steigers. Ik heb er alles aan gedaan om de lancering door te zetten, ook in een demissionair kabinet. Dit dossier was te belangrijk om op pauze te zetten.”

De risico's van digitalisering zijn al jaren bekend? Waarom dan nu pas een NDS?

“De zorgen zijn inderdaad niet nieuw. Maar elke overheid bestreed die risico's met eigen systemen en eigen beleid. Daardoor ontstond versnippering. Wat nu anders is: we kiezen er bewust voor om het samen te doen, met alle overheden: één koers en

we nu op, en welke later? Daarbij worden ze – gevraagd en ongevraagd - geadviseerd door de NDS-Raad met externe digitaliseringexperts. Je kunt hen zien als de aanjagers van het proces. Uiteindelijk moet er een investeringsagenda komen die glashelder maakt: wat moet er gebeuren, voor wie, en hoe gaan we dat doen?” Voor zichzelf ziet Van Marum daarbij vooral een politieke rol weggelegd. “Ik wil het belang van digitalisering nóg meer op de kaart te zetten in de Tweede Kamer, om ervoor te zorgen dat er nu al wordt nagedacht over wat er nodig is om Nederland digitaal weerbaarder te maken in de komende kabinetsperiodes. En misschien is dit onderwerp wel zo belangrijk dat er op termijn een minister van Digitalisering op deze plek moet komen te zitten.”

Wat betekent de NDS concreet voor burgers en ondernemers in Nederland?

“Burgers en ondernemers hebben recht op begrijpelijke en betrouwbare dienstverlening. De NDS moet dat waar maken: minder wachttijd, minder fouten, meer veiligheid. Je kunt het zo zien: we bouwen aan een veilig digitaal stopcontact. Alle overheden kunnen daar uiteindelijk hun diensten in prikken. Burgers krijgen dan wat ze nodig hebben, op één centrale plek. Denk bijvoorbeeld aan Overheid.nl als de wegwijzer waar je straks alle informatie kunt vinden. Daar lees je hoe je iets regelt bij een gemeente of bijvoorbeeld de Belastingdienst.” “We kijken ook naar het verantwoord inzetten van digitale assistenten. Gemeenten doen daar al ervaring mee op, met de OmgevingsChat in Leeuwarden en AI chatbot Guus in Goes. Uiteindelijk moet je als burger of ondernemer het gevoel krijgen dat je met één overheid te maken hebt en meteen wordt geholpen.”

Versnelling

Er wordt in de NDS veel gesproken over versnelling. Niet in plannen blijven steken maar echt bouwen, is het motto. “Dit is geen papieren strategie die in een la verdwijnt. We betrekken de uitvoeringsorganisaties er nadrukkelijk bij, bijvoorbeeld de Belastingdienst en gemeenten. Zij weten hoe de dienstverlening naar burgers in de praktijk werkt. Hun kennis bepaalt welke stappen we eerst zetten.” “Daarnaast zorgen we ervoor dat belemmeringen worden weggenomen. Zo gaan we werken met verplichte, overheidsbrede standaarden. Denk aan één manier van inloggen of één manier om gegevens te delen tussen organisaties. Dat voorkomt dat iedereen zelf het wiel uitvindt. Het scheelt tijd, het verkleint de kans op fouten en het maakt de dienstverlening overzichtelijker. Daardoor zien burgers en bedrijven ook sneller resultaat.”

Welke investeringen zijn nodig, waar komt het noodzakelijke geld vandaan?

“Daar kan ik duidelijk over zijn. Digitale voorzieningen vragen om structureel geld, nu én in de toekomst. We

moeten tegelijk brandjes blussen en bouwen aan een stevig fundament. Aan de ene kant zijn er maatregelen nodig om bestaande systemen draaiend te houden en risico's direct te beperken. Aan de andere kant moet de investeringsagenda ervoor zorgen dat we op de lange termijn digitaal weerbaar blijven.” “Maar de overheid kan dit niet alleen. Dit vraagt om gezamenlijke investeringen: publiek, privaat en misschien ook Europees. Kijk naar Defensie: Nederland heeft zich gecommitteerd aan de NAVO-norm van 5 procent van het bruto binnenlands product. Daarvan is 1,5 procent bedoeld voor bredere investeringen. Wat mij betreft moeten we bekijken of een deel daarvan ook kan worden ingezet voor digitale weerbaarheid en infrastructuur. Want die zijn net zo onmisbaar voor onze veiligheid.”

De NDS is op 4 juli in een brief aan de Tweede Kamer aangekondigd. Een dag eerder informeerde collega-de-missionair staatssecretaris Gijs Tuinman het parlement over de Digitale Transformatie Strategie Defensie. De NDS vormt samen met de Strategie Digitale Economie, Digitale Transformatie Strategie Defensie en de Nederlandse Cybersecurity Strategie (NLCS) het fundament van het digitaliseringsbeleid, aldus Van Marum. “We trekken in digitalisering nauw op met Defensie. Dat kan ook niet anders. De modernisering van de digitale overheid vraagt om samenwerking, niet meer ieder ministerie voor zich. Ik spreek regelmatig met Gijs Tuinman, we hebben het dan over digitale weerbaarheid, autonomie en het gebruik van de infrastructuur voor AI. We kijken hoe we elkaar kunnen versterken.”

Van Marum geeft aan dat het ook de bedoeling is van de NDS om minder afhankelijk te worden van Amerikaanse diensten zoals Google en Microsoft. “Maar dat gaat niet in één keer. Grote Amerikaanse cloudplatforms zijn nu vaak de standaard: schaalbaar, betrouwbaar en relatief goedkoop. Dat gemak heeft natuurlijk wel een keerzijde: je maakt je afhankelijk en er zijn terechte zorgen over de bescherming van gegevens. Daarom werken we aan alternatieven die onze digitale autonomie vergroten. Een voorbeeld is een overheidsbrede soevereine cloud. We onderzoeken nu of en hoe we de infrastructuur hiervoor in eigen beheer kunnen opbouwen, samen met publieke en private partijen in Nederland. Uiteindelijk kun je in zo'n cloud de data en processen opslaan die je niet in een publieke cloud wilt hebben, zoals persoonsgegevens of gevoelige overheidsgegevens. Zo houden we grip op onze eigen informatie en kunnen we beter samenwerken tussen overheden.”

Hoewel niet specifiek genoemd in de NDS, juicht Van Marum de plannen voor een AI-fabriek in Groningen

“
Digitalisering is
geen bijzaak meer,
het raakt de kern
van onze samenleving
”



van harte toe. “De AI-fabriek gaat verder dan alleen de digitale overheid. Het raakt ook aan werkgelegenheid en de economische positie van Nederland. Daarom staat het niet in de NDS. Maar er wordt wél hard aan gewerkt. Kabinet en regio investeren samen 200 miljoen euro. Hier komen mijn portefeuilles Herstel Groningen en Digitalisering mooi samen. Ik zou het fantastisch vinden als Groningen hiermee een voortrekkersrol krijgt. Dat biedt kansen voor de bewoners én laat zien dat Den Haag deze regio ook echt iets goeds te bieden heeft.”

Basisvoorziening

De NDS helpt ook in het perspectief van grotere cyber-aanvallen. “We zijn al beter voorbereid dan vroeger, maar we zijn ook zeker niet volledig veilig. Geen enkel land is dat. De NDS maakt ons weerbaarder, verkleint de risico's en helpt ons sneller reageren als er iets misgaat. En we kunnen niet alleen op techniek vertrouwen. Techniek kan uitvallen. Daarom werken we ook aan noodplannen en noodvoorzieningen. Want zoals ik bij het begin van dit interview al zei: digitalisering is een basisvoorziening geworden, net als water of stroom. Ook bij een crisis moeten burgers en bedrijven gewoon op de overheid kunnen rekenen.”

Tot slot: er wordt vaak gepleit voor een minister van Digitale Zaken. Moet uw opvolger geen staatssecretaris maar minister worden?

“Die discussie speelt al langer, en ik snap dat heel goed. Digitalisering is nu verspreid over allerlei ministeries. Het is belangrijk om het signaal af te geven dat dit onderwerp topprioriteit heeft. Digitalisering behoort wat mij betreft net als Defensie en Financiën standaard aan tafel bij de ministerraad. Of er een minister komt, is natuurlijk aan het volgende kabinet. Maar hoe meer centrale sturing, hoe beter. Want digitalisering is geen bijzaak meer, het raakt de kern van onze samenleving.”

Nederlandse Digitaliseringsstrategie (NDS)

De NDS is 1 van de pijlers van het kabinetsbeleid op digitalisering en definieert 6 prioriteiten voor 1 overheid.

Prioriteit 1 – Cloud

Prioriteit 2 – Data

Prioriteit 3 – Artificiële Intelligentie

Prioriteit 4 – De overheid stelt burgers en ondernemers centraal in (digitale) dienstverlening

Prioriteit 5 – Versterken digitale weerbaarheid en autonomie van de overheid

Prioriteit 6 – Digitaal vakmanschap en een moderne werkomgeving

Logius biedt de helpende hand

Wat de Nederlandse Digitaliseringsstrategie (NDS) bepleit – werk als één overheid samen – is voor Logius min of meer het organisatie-DNA. Door het beheer van producten als DigiD en MijnOverheid, staat het agentschap, achter de schermen weliswaar, namens de gehele overheid stevig in de samenleving waar het gaat om online dienstverlening aan burgers en bedrijven.

Dat werk blijft niet onopgemerkt. Zo brachten voormalig staatssecretaris Digitalisering Zsolt Szabó en ook de vaste Kamercommissie Digitale Zaken een bezoek aan Logius en schoof Bert Voorbraak recent aan bij een rondetafelconferentie van de Tweede Kamer over de NDS. “Een paar jaar geleden had niemand het erover en plaatsten we onze data allemaal gewoon in een public cloud maar in twee jaar tijd is de wereld enorm veranderd. We zien steeds meer verbinding tussen politiek, beleid en uitvoering, ik vind dat echt heel fijn.”

Weerbaarder worden

“Digitale autonomie, digitale soevereiniteit, weerbaarheid, dat zijn precies de termen die de afgelopen jaren heel nadrukkelijk op onze agenda zijn gekomen en die ook hun weerklank vinden in de NDS”, aldus Bert Voorbraak. Hij is blij met de NDS, “want daarmee zorgen we er samen voor dat er een aantal thema’s op de agenda komen, overheidsbreed, die tot nu toe wat moeilijker liepen. Alle partijen zeggen: dit is goed, dit moeten we gaan doen, dit helpt ons als overheid in de breedte om weerbaarder te worden.” “De uitgangspunten en prioriteiten van de NDS gelden al heel lang voor Logius. Wij werken zoals gezegd voor

Bert Voorbraak is sinds 26 februari 2024 algemeen directeur bij Logius, een agentschap van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Logius draagt mede zorg voor de digitale overheid met stelsels, standaarden en voorzieningen. Het beheert voornamelijk (en ontwikkelt via derden, zoals ICTU en diverse marktpartijen) cruciale digitale producten van de overheid zoals DigiD, MijnOverheid, Digipoort en Berichtenbox. Samen met diverse stakeholders werkt Logius aan de Generieke Digitale Infrastructuur (GDI).

de hele overheid, niet alleen voor de Rijksoverheid”, zegt Voorbraak. Hij noemt als voorbeeld MijnOverheid. “Wij kunnen op één plek alle gegevens publiceren die van een burger bij de overheid bekend zijn. Als je inlogt met je DigiD en informatie opvraagt, dan halen wij die gegevens

voor je op. Dat betekent niet dat wij al die gegevens hebben, we zijn niet de eigenaar van die informatie, wij publiceren die alleen maar wanneer die wordt opgevraagd, binnen de geldende protocollen uiteraard. DigiD is een authenticatiemodel waarvan alle overheidsorganisaties gebruik mogen maken: de Rijksoverheid, uitvoeringsorganisaties als de SVB en UWV, en ook de gemeenten. Sterker nog: we zien een sterke groei vanuit de zorg-

“
Waar het om
gaat is: ben
je weerbaar
tegen allerlei
invloeden?
”

sector – ziekenhuizen, zorgverzekeraars – die DigiD gebruiken. Dus het is een online inlogmiddel dat voor alle overheidspartijen geldt, en dat beeld van de NDS – werk als één overheid samen – dat is ons uit het hart gegrepen.”

In het kader van thema’s als versterking digitale weerbaarheid en autonomie van de overheid en gezamenlijke cloudtechnologie zijn onder de NDS zogenaamde aanjaagteams ➤



geformeerd om hier prioriteit aan te geven. Ook Logius maakt daarvan deel uit. Voorbraak erkent dat er tijdsdruk opzit. “Dat voelen we zeker ja, want we weten niet wat er geopolitiek gaat gebeuren.” Overigens: Logius maakt geen gebruik van *hyperscalers*, meldt Voorbraak. “Een deel van ons applicatielandschap staat gewoon bij een ODC (overheidsdatacentrum – red.) en een ander deel, via een aanbesteding, bij een Nederlandse provider.”

Is daarmee al voorgesorteerd op de discussie die gaande is?

“Dat zou te gemakkelijk zijn. Die aanbestedingen zijn jaren geleden al gedaan toen deze discussie helemaal nog niet speelde. Maar ik prijs me achteraf wel gelukkig dat toen die keuze is gemaakt. Het gaat me niet om die *hyperscalers*, waar het om gaat is: ben je weerbaar tegen allerlei invloeden?”

Heb je de indruk dat Logius meer weerbaar is dan anderen?

“Weet ik niet. Dat is de grote discussie natuurlijk. *Hyperscalers*, daar zitten ongelooflijk veel investeringen achter. Als je daar geen gebruik van maakt dan loop je in principe dat innovatievermogen ook mis. Het gaat om de balans. Ik wil echt niet pretenderen dat die *hyperscalers* geen waarde hebben, maar maak daarin gewoon bewuste keuzes en zeg: dit is data die zo gevoelig is, die wil ik niet bij een *hyperscaler* hebben terwijl je voor andere data prima met een *hyperscaler* uit de voeten kan.”

Helpende hand

Inmiddels bestaat DigiD al 20 jaar. Toch zijn er nog overheidsinstanties die geen gebruik maken van bijvoorbeeld DigiD, het is wat dat betreft geen verplichte winkelnering. “We zijn in gesprek met niet-gebruikers om te kijken wat daarvoor de reden is. Want DigiD is een middel dat we bedacht hebben met elkaar en voor elkaar, en we hebben het ook samen betaald. Dus als

je er geen gebruik van maakt is dat eigenlijk doodzonde. De slag die we nu aan het maken zijn is om meer de helpende hand toe te steken: hoe kunnen we ervoor zorgen dat je kunt aansluiten? Kunnen we dat met elkaar makkelijker maken?”

“Aan de andere kant, als ik kijk vanuit het burger perspectief: het is een beetje schrijnend, maar er is nog steeds een grote groep burgers die niet zodanig digitaal vaardig is dat ze DigiD of MijnOverheid makkelijk gebruiken, die vinden dat echt heel moeilijk.”

Het Sociaal Cultureel Planbureau (SCP) heeft hierover eerder gerapporteerd. Een actueel voorbeeld, waarvoor de Nationale ombudsman Reinier van Zutphen aandacht heeft gevraagd, betreft de Berichtenbox. Sommige gemeenten plaatsen daarin verkeersboetes, zonder dat

je daarover schriftelijk wordt geïnformeerd. Door alleen een elektronische melding bestaat de kans dat mensen niet in hun Berichtenbox kijken en boetes onnodig hoog oplopen. “Ik snap heel goed wat Van Zutphen zegt en ik ben het ook met hem eens dat we moeten nadenken over hoe dit soort effecten te voorkomen. Het is waar dat wij als overheid met dit soort complexe situaties te maken hebben, daar kun je niet voor weglopen.”

Voorbraak vertelt over een recent bezoek aan een Informatiepunt Digitale Overheid (IDO) bij de Bibliotheek Rotterdam. “Dan mag ik – na om toestemming te hebben gevraagd uiteraard – meeluisteren met gesprekken, en dan schrik ik van het feit dat veel mensen waarvan wij als overheid denken dat die wel in die digitale overheid

mee kunnen, daar heel veel moeite mee hebben.

Daar willen we als Logius graag een helpende hand bieden. Wij zijn niet in staat om 18 miljoen Nederlanders te helpen,

“We voelen zeker tijdsdruk, want we weten niet wat er geopolitiek gaat gebeuren”

daar zijn we niet op toegerust, maar we denken wel na over hoe we degenen die in de frontlinie staan - denk aan steunpunten, denk aan buurthuizen, denk aan balies van de Belastingdienst of SVB – of we hen niet meer kunnen equiperen om de vragen op te vangen voor de digitale overheid. We hebben daar inmiddels het programma ‘Help de Helper’ voor ingericht.”

‘Burgers en ondernemers centraal’

Ook in de NDS is ‘burgers en ondernemers centraal’ een thema. Bij het ontwikkelen van applicaties zet Logius UX designers in, vertelt Voorbraak. “Die gaan in gesprek met burgers, met representanten uit die groep digitaal minder vaardige mensen, met de vraag: als wij een nieuw systeem of een nieuwe applicatie of een nieuwe functionaliteit moeten maken, hoe zouden we dat dan zo moeten doen dat dit voor jullie begrijpelijk is? Dus er wordt nog niks geprogrammeerd, op een whiteboard wordt getekend hoe het eruit zou kunnen zien. Er bestaan natuurlijk al langer trajecten rond het gebruik van begrijpelijke taal, dus dat is op zich niet nieuw, maar dit helpt wel. Ik krijg nog wel eens de vraag: waarom kan dit bij het bedrijfsleven wel of waarom gaat dat bij de overheid moeilijker? Maar die vergelijking vind ik niet helemaal eerlijk. Het bedrijfsleven bedient vaak een bepaalde doelgroep en de overheid bedient alle burgers, dus dat is wat mij betreft toch wel een heel ander fenomeen. Wij moeten diensten bedenken, ontwikkelen en uitvoeren die voor een digitaal ontwikkelde burger misschien een beetje ouderwets aanvoelen terwijl het voor een niet digitaal vaardige burger heel ingewikkeld is. Dat is wel onze realiteit. Ik heb gedacht dat dit zich in de loop van

de tijd wel zou oplossen maar ik heb letterlijk gezien op een IDO dat ook jonge mensen om hulp vragen omdat ze het ingewikkeld vinden; terwijl ze toch bijna opgroeien met een telefoon in de hand.”

Een bruggetje naar iets anders dat ingewikkeld is, of in elk geval ingewikkelder dan vroeger: cyberdreiging. Begin dit jaar heeft Logius veel last gehad van DDoS-aanvallen, dit gaf wat zorgen met de NAVO-top in het verschiet. In het verleden waren dat relatief simpele aanvallen, op het internet kun je gewoon met je creditcard een DDoS-aanval kopen, dat is niet zo ingewikkeld. Maar nu kregen we te maken met een nieuw type aanvallen. Normaal gesproken is een aanval op één punt gericht, met veel verkeer. En daar zijn onze systemen op ingericht, die filters zien dat en zetten meteen de wasstraat aan en dan wordt dat verkeer eraf gehaald. Wij kennen dat als dagelijks werk, daar worden we niet koud of warm van. Maar nu waren het aanvallen die een heel breed spectrum bedienden met allemaal een klein beetje verkeer.”

Prijsschieten

Dit fenomeen staat bekend als *carpet bombing*. “Onze filters detecteerden dat niet omdat die onder de drempel bleven maar in hun optelling wel zorgden voor problemen. Daar moest onze infrastructuur op getuned worden en vervolgens zagen we dat de aanvallers zo intelligent waren dat zij zagen welke mitigerende maatregelen wij namen en daarop weer een antwoord hadden. We zeiden wel eens tegen elkaar: dit lijkt wel op prijsschieten op de overheid. Want als je DigiD weet plat te leggen dan werkt dat door, dan zie je ook problemen bij UWV en de Belastingdienst, want je raakt iedereen die met DigiD inlogt. Dat heeft veel impact omdat je veel andere organisaties raakt.”

“Het heeft een tijdje geduurd voordat wij het echt helemaal onder controle hadden. We signaleren het overigens nog steeds maar hebben er geen last meer van. In deze wereld is het altijd een soort ratrace - de aanvaller is altijd sneller dan jij als verdediger. Kun je alles voorkomen? Dat geloof ik niet. Dus waar wij op inzetten: weerbaarheid is ook wendbaarheid, dus zo snel mogelijk kunnen anticiperen op wat je ziet gebeuren. Dus we monitoren ons netwerk, onze applicaties, we hebben een calamiteitenorganisatie die 24/7 stand-by is en als directeur heb ik naast deze telefoon ook nog een rode telefoon en die heb ik 24 uur per dag in mijn nabijheid. Dat vindt het thuisfront misschien niet leuk, maar die gaat mee naar de slaapkamer.”

Hoe vaak gaat die rode telefoon af?

“Niet zo vaak, gelukkig niet. Die crisisorganisatie werkt in allerlei gelaagdheden. De eerste aanvallen worden gewoon operationeel afgevangen en pas later wordt opgeschaald.”

Werken aan weerbaarheid

Regelmatig duiken in het nieuws berichten op over 'hacks' bij onder meer de overheid, zoals recent het Openbaar Ministerie en Bevolkingsonderzoek Nederland. Dat heeft de nodige impact op de bedrijfsvoering maar zeker ook op het vertrouwen in de overheid. Het NCSC telt op tweederde al veel meldingen en verwacht naar schatting aan het einde van het jaar 50.000 meldingen van een kwetsbaarheid. Vorig jaar was dit nog 40.000. Kortom: *cybercrime is here to stay*.

Het NCSC maakt zich hard voor digitale weerbaarheid; het vermogen om digitale dreigingen, zoals malware, *phishing*, *quishing* en desinformatie, te weerstaan. De organisatie is zelf ook niet verschoond gebleven: uit naam van het NCSC zijn begin juni phishing mails verzonden. "Het feit dat het NCSC gebruikt wordt voor phishing campagnes, betekent dat we als organisatie zichtbaar zijn maar dan zijn dit wel de neveneffecten. Het is niet anders dan BN'ers die gebruikt worden voor allerlei fraude. De naam van NCSC werd gebruikt samen met de politie en Europol."

<< Digitale weerbaarheid moet een prioriteit worden in beleidsvorming en uitvoering, zelfs boven andere beleidspunten. Burgers moeten kunnen rekenen op een betrouwbare overheid. Het is de verantwoordelijkheid van de politiek, bewindspersonen en de ambtelijke top om overheden weerbaar te maken tegen langdurige uitval van ICT-diensten.>>

Ziehier een citaat uit het rapport 'Van kwetsbaar naar weerbaar', opgesteld door ABDTOPConsult van de Algemene Bestuursdienst, dat 12 september jl. werd aangeboden aan de ministerraad.

“

Het is niet de vraag of maar eerder de vraag wanneer je een keer slachtoffer wordt van cybercrime

”

Vertrouwen

Een jaar is voorbij gegaan sinds Van Amelsfort aantrad als directeur van het NCSC, "en in dat jaar is best wel een hoop veranderd in de wereld. De situatie bij het Internationaal Strafhof (ISH) is daarbij het mooiste voorbeeld als *eye-opener* in de zin van de risico's van digitale afhankelijkheid, ofwel waar kun je nog op vertrouwen in je systemen, hoe moet je risico's inschatten?"

"Dat kan gaan over vertrouwen in de opslag van de data en de beschikbaarheid, wat vaak speelt bij *ransomware* zaken en dat soort dreigingen. Maar ook als data naar buiten komt, wat doet dat met jouw vertrouwen in hoe je gegevens zijn opgeslagen? Vertrouwen en veiligheid kennen verschillende aspecten en dus ook verschillende invalshoeken van waaruit je ernaar moet kijken."

Van Amelsfort adresseert het onderwerp data aan de hand van verschillende fases. Hij gebruikt de termen *at rest* (opgeslagen), *in use* (actief gebruik) en *in transit* (de data bewegen tussen gebruikers en systemen). Voor al die verschillende fases zou je specifieke encryptie maatregelen moeten nemen.

"De omgeving is veel complexer geworden de laatste jaren", stelt Van Amelsfort, doelend op ontwikkelingen als BYOD (*Bring Your Own Device*) en het thuiswerken dat post-corona gemeengoed is geworden. "Veel systemen worden aan elkaar gekoppeld, zowel IT als OT, wat weer nieuwe risico's met zich meebrengt. Wat dat betreft hebben we te maken met een veelkoppig monster en 100 procent veiligheid is een illusie. Wel moet je bij je vitale infrastructuur echt inzetten op die 100%. Daar streven we natuurlijk wel naar en dat betekent enerzijds zorgen dat je de boel op orde hebt en anderzijds – en dat is

het tweede aspect van weerbaarheid – als je dan toch slachtoffer wordt: hoe organiseer je dan je business continuïteit? Wat heb je geregeld om te kunnen uitwijken, dat je niet in een *vendor-lock* terechtkomt, wat is je Plan B?"

De geopolitieke situatie voedt de behoefte aan strategische digitale soevereiniteit in de EU, wat betekent dat voor de positie van het NCSC daarin?

"Wij zijn altijd wel van het schetsen van het bredere plaatje. Dus als we praten over een soevereine data-cloud in Nederland of Europa, dan is het een feit dat heel veel apparatuur die daarbij wordt gebruikt, die komt van buiten Europa. Denk aan servers, aan routers, aan softwarepakketten. In de basis is de vraag: welke risico's loop je en welke risico's vind je acceptabel? En wat is de voorspelbaarheid van die risico's, vooral dat is de laatste tijd veranderd. Het is niet zo van 'we hebben straks die cloud in Europa en dan zijn we klaar'; veiligheid is een continu proces."

"Ook wij maken natuurlijk die afweging qua risico acceptatie ten aanzien van waar we onze data neerzetten. We hebben nu voor Nederland de registratieplicht bij het NCSC vanuit de Network and Information Security Directive (NIS2-richtlijn) die in de aanstaande Cyberbeveiligingswet is geïmplementeerd. Deze is gericht op de verbetering van de digitale en economische weerbaarheid van belangrijke en essentiële diensten en organisaties in Europa. Dat register is een van de kroonjuwelen van het NCSC en die beschermen we uiteraard maximaal."

Matthijs van Amelsfort is sinds 1 september 2024 directeur van het Nationaal Cyber Security Centrum (NCSC), dat bedrijven helpt om de digitale weerbaarheid te vergroten door middel van advies, onderzoek en het delen van kennis. Het NCSC ressorteert onder het ministerie van Justitie en Veiligheid. Van Amelsfort was eerder werkzaam bij de Nationale Politie, Landelijke Eenheid Opsporing en Interventies, Dienst Landelijke Recherche (DLR) - locatie Driebergen. Hij leidde daar het Team High Tech Crime met een focus op cybercrime en digitale opsporing.

Sleutelrol

Als het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland gaat het NCSC een sleutelrol spelen in het informeren van organisaties en bedrijven om hun cyberweerbaarheid te verhogen. Daarbij vindt er begin 2026 een integratie plaats met het Digital Trust Center (DTC), dat ressorteert onder het ministerie van EZ, en het Computer Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP). Hierbij vallen ruim 2,3 miljoen entiteiten onder het NCSC.

Van Amelsfort refereert aan “the best of three worlds”, want: “Het gaat absoluut helpen als uiteenlopende doelgroepen – van ZZP tot MKB tot multinational tot vitale bedrijven – kunnen bouwen op identieke adviezen. Om die reden hebben we ook vijf basisprincipes (zie kader – red.) vastgesteld om duidelijkheid en uniformiteit te creëren.”

Wat is de staat van cybersecurity in Nederland?

“Dat is moeilijk te meten. Het aantal meldingen van kwetsbaarheden wordt ongeveer 50.000 dit jaar. Dat is heel breed en heel divers, en ook de impact kan heel verschillend zijn. Het is gewoon lastig om vast te stellen wanneer hebben we ons weerbaar

getoond en wat hebben we kunnen voorkomen door alle adviezen die we uitdragen? Meet je zo'n staat af aan het aantal keren dat het is fout gegaan of het aantal keren dat het is goed gegaan? Maar natuurlijk genereren we uit die informatie ook trends en analyses, die we delen met de NCTV (Nationaal Coördinator Terrorismebestrijding en Veiligheid – red.).”

Is het dweilen met de kraan open?

Met een glimlach: “Ik heb een ‘Loesje spreuk’ die ik al vanaf het begin gebruik en die luidt: ‘Het is fijner dweilen als je weet dat iemand de kraan aan het repareren is. En die blijft actueel wat mij betreft. Dus dat doen we als het NCSC, wij zijn die kraan aan het repareren samen met onze publieke en private partners. Dat zie ik als een belangrijke taak als je het hebt over Nederland digitaal weerbaar maken: met elkaar die kraan repareren.”

Van Amelsfort spreekt van “een continu proces” rond de vraag wat een geaccepteerd risico is. Dat bedrijven in Nederland en Europa qua marktpositie achterop zijn geraakt het laatste decennium wijt hij niet aan een ge-

brek aan kennis of innovatie, integendeel. “Maar door de globalisering en keuzes die in het verleden zijn gemaakt, zit je nu in een hele andere werkelijkheid en die draai je niet zomaar terug. Helemaal onafhankelijk kun je niet zijn en ik denk dat we vooral moeten streven naar een wereld waarin we met elkaar kunnen leven, misschien is dat wel het grotere doel. Eigenlijk heb je een soort wederzijdse afhankelijkheid nodig om in die balans te komen. Als ik kijk naar de innovatiekracht in Nederland, en naar alle start-ups die voorbij komen, dan denk ik dat we echt wel wat kunnen en dat je dat ook moet blijven stimuleren.”

Successen delen

Het NCSC werkt samen met Europese partners waarbij Van Amelsfort aantekent dat de samenwerking onderling tussen EU-landen (hij spreekt van *member states*) anders is dan die met andere landen binnen de grenzen van Europa. “Ook tijdens ONE Conference zijn er veel ontmoetingen waarin met elkaar wordt overlegd over de geopolitieke situatie, maar ook over de uitdagingen die we gezamenlijk hebben, bijvoorbeeld als het gaat over implementatie van wetgeving. En we delen met elkaar ook successen. België heeft een Anti-Phishing Shield (BAPS) dat uitermate succesvol is. Wij zijn nu gestart, samen met KPN, om te kijken hoe we dat kunnen adopteren en implementeren in Nederland. Dat ziet er op het eerste gezicht al veelbelovend uit.” Die samenwerking over de grenzen is ook noodzakelijk bij het snel delen van informatie. “Een criminele actor kijkt niet snel naar landsgrenzen of een bepaalde sector als hij in de aanval gaat, die schiet met hagel en dan heeft-ie ergens raak en gaat daarop verder. Maar in de recente Citrix-lek, waardoor enkele organisaties, ook binnen de Rijksoverheid, konden worden gehackt, hebben we gezien dat het heel belangrijk is om internationaal informatie met elkaar te delen. De eerste signalen kregen wij toen vanuit een Europese instantie en daar konden wij weer op verder bouwen. We konden vrij snel reageren en proactief communiceren en scripts ter beschikking stellen binnen Europa zodat ook andere landen daarmee hun voordeel konden doen.”

Data gedreven werken is een drijfveer. “We maken gebruik van AI om te kijken in welke mate we data-analyses geautomatiseerd kunnen doen. Natuurlijk, de check kent nog altijd de menselijke factor: wat het systeem ons vertelt, is dat in overeenstemming met wat wij ook zien? Maar dat soort technieken helpt ons natuurlijk wel om snelheid in processen te brengen.” Dat geldt ook voor een ontwikkeling als quantumcomputing. “Wij hebben een proactieve houding waar het gaat om het onderzoeken van wat nieuwe risico's kunnen zijn, voorbij de horizon die we nu kennen. En toch, wat wij in de praktijk vooral zien: die vijf basisprincipes, dat is nog steeds waar het misgaat.”

Niet of maar wanneer

De dreiging is groot, de materie complex en het wordt met een steeds meer digitaliserende samenleving ook niet makkelijker, stelt Van Amelsfort. “Het is niet de vraag of maar eerder de vraag wanneer je een keer slachtoffer wordt van cybercrime of cyberaanvallen, in wat voor mate dan ook. Dat kan variëren van een DDoS-aanval tot een daadwerkelijk binnentreding van je systeem.” De boodschap: wees niet naïef, de wereld is veranderd. “Tegelijkertijd is bij mij het glas ook altijd wel weer halfvol. Dat is ook de reden geweest dat ik ben overgestapt na 25 jaar bij de politie naar hier om écht die kranen te gaan repareren, écht te gaan werken aan die weerbaarheid. Het is de taak van het NCSC om dat overkoepelende

beeld te hebben en informatie te delen om die weerbaarheid te kunnen garanderen. Bij ernstige security-incidenten zijn er directe contacten met de AIVD, MIVD en de Nationale Politie. En ik denk dat in 2026, met onze nieuwe organisatie en de context van de nieuwe Cyberbeveiligingswet, we vanuit die informatiepositie goed geëquipeerd zullen zijn om die dreigingen het hoofd te kunnen bieden, en te zien en te horen en te voelen wat er gebeurt in de wereld van cybersecurity.”

De 5 basisprincipes van weerbaarheid

- Basisprincipe 1: Breng je risico's in kaart
- Basisprincipe 2: Bevorder veilig gedrag
- Basisprincipe 3: Bescherm systemen, applicaties en apparaten
- Basisprincipe 4: Beheer toegang tot data en diensten
- Basisprincipe 5: Bereid je voor op incidenten





Peter Verkoulen is programmadirecteur van het Centre of Excellence for Data Sharing & Cloud (CoE-DSC). Hierin zijn sinds 2023 een aantal generieke Nederlandse initiatieven op het gebied van data delen en cloud gebundeld. Het CoE-DSC ondersteunt (federatieve) initiatieven op het gebied van data delen en cloud, werkt aan interoperabiliteit en geeft impulsen aan de markt. En dit in een internationale context. Het CoE-DSC vervult ook de rol van Gaia-X hub in Nederland, met als doel om digitale soevereiniteit te bevorderen, en daarmee maatschappelijke en economische waarde te helpen realiseren.

Gaia-X en de federatieve aanpak

Driekwart van de wereldwijde cloud-capaciteit is in beheer van drie zogenaamde *hyperscalers* te weten: Microsoft, Google en Amazon Web Services. In de discussie over de noodzaak van (meer) soevereiniteit is ook de roep om een Europees equivalent te horen. “Maar als je al daartoe zou besluiten, wat is dan de weg ernaar toe?”, stelt Peter Verkoulen.

Verkoulen weet zelf ook het antwoord niet, zegt hij er eerlijkheidshalve bij, maar wil er wel hardop over nadenken. “Ik veronderstel dat een Europese variant op Microsoft zich allicht anders zal gedragen dan de Amerikaanse Microsoft, maar het blijft een *hyperscaler* met de businessmodellen die daarmee samenhangen. Dan is de vraag: wat worden we daar beter van? Maar ook: waar moeten de miljarden, misschien wel 50 of 100, vandaan komen om die *hyperscaler* te bouwen? Want de huidige drie zijn over een periode van 20 jaar ontstaan en dan vooral uit de manier waarop wij ons met z’n allen als inkopende organisaties hebben gedragen.”

Federatieve aanpak

“Het probleem is: je zou minstens tien jaar nodig hebben om daar te komen en dan is de vraag: hoe kom je die jaren door? Je zou zo’n stap kunnen verdedigen door te stellen: uiteindelijk willen we gewoon helemaal onafhankelijk zijn. Maar bereik je dat dan door een Europese *hyperscaler* te bouwen – en eerlijk gezegd: van drie naar vier vervuimt ook niet echt de keuze – of door federatieve oplossingen mogelijk te maken?” Gaia-X is een van de Europese initiatieven die zo’n federatieve aanpak voorstaan. “Daarbij kan ik bijvoorbeeld met een kleinere cloud-provider werken omdat die toevallig om de hoek zit of heel specifieke diensten levert of waar-

van ik zeker weet dat mijn persoonlijke data in Nederland blijven. En dat kan ik combineren met een Duitse partij of een Franse partij, of een *hyperscaler*, het is maar net wat je wilt.”

Verkoulen gebruikt voor de federatieve oplossing de parabel van de lappendeken. “Jouw oplossing kun je helemaal met Europese lapjes aan elkaar knopen – en als iemand er een Japans, Indiaas of Amerikaans lapje in wil weven: prima. En in geval dat het blauwe lapje niet bevalt, moet je het ook los kunnen punniken en kunnen vervangen door een groen lapje.”

Gaia-X is in 2020 ontstaan op initiatief van elf Franse en elf Duitse bedrijven. Inmiddels zijn wereldwijd zo’n 250 bedrijven en instellingen aangehaakt. “Het is een initiatief dat in Europa is ontstaan, vanuit de Europese normen en waarden, maar wel met een breder internationaal perspectief. Want wat heb je in het huidige mondiale systeem aan een oplossing die het alleen maar in Europa doet? Dus er is al snel gezocht naar hoe dat uit te breiden en dat heeft geresulteerd in het opzetten van hubs in andere landen. Er is een hub in Amerika, er is een hub in Japan, er is een hub in Zuid-Korea, dus echt over de hele wereld verspreid. Economische Zaken heeft toen aan TNO gevraagd om dat in Nederland op te starten en TNO heeft aan mij gevraagd, vanuit mijn rol als zelfstandig adviseur, om dat voor hen te doen.”

In 2023 is de hub opgegaan in het Centre of Excellence for Data Sharing & Cloud, de Nederlandse hub voor alles wat met data delen en de onderliggende benodigde (federatieve) cloud infrastructuur te maken heeft.

Kernwaarden

Met als kernwaarden data soevereiniteit, interoperabiliteit, transparantie en open standaarden, is Gaia-X inmiddels vijf jaar onderweg. “Dat is een proces van veel praten en nadenken en stukken schrijven en sinds anderhalf jaar wordt er ook echt software ontwikkeld. De kern van Gaia-X is eigenlijk het zogenaamde Digital Clearing House, dat ervoor zorgt dat data delende partijen met elkaar worden verbonden en dat daar ook (cloud) diensten onder kunnen worden gehangen die je dan federatief kunt gebruiken. Er zijn inmiddels tien commerciële partijen in de wereld welke die Digital Clearing House functionaliteit leveren. Ook in Nederland zijn gesprekken met een paar kandidaten in een afrondende fase. Daarmee is ook een misverstand uit de wereld geholpen dat Gaia-X zelf diensten zou gaan leveren en een concurrent zou worden van IT-leveranciers. Nee, Gaia-X is geen commerciële partij, maar zorgt voor een standaard voor bijbehorende software specificaties en commerciële bedrijven gaan uiteindelijk die functionaliteit leveren.” Hij voegt eraan toe dat Airbus en ook Électricité de France (EDF) in hun tenders om Gaia-X ➤

“
Bij Europese
aanbestedingen
ook kijken naar
aspecten van
soevereiniteit
”

compliance vragen. “Dit zijn de eerste stapjes maar we staan aan de vooravond van een doorbraak.”

Een ander misverstand is dat Gaia-X gesubsidieerd zou worden door de Europese Commissie, geeft Verkoulen aan. De aangeslotenen betalen contributie en brengen op die manier werkbudget bij elkaar. “Er is wel een belangrijke rol weggelegd voor de overheid want die heeft een enorme marktmacht die ze kan inzetten bij Europese aanbestedingen. Daarbij wordt altijd gesproken over de ‘economisch meest voordelige inschrijving’, waarbij vroeger primair naar prijs werd gekeken en pas later naar functionaliteit. Maar je zou nu ook moeten kijken naar aspecten van soevereiniteit, beschikbaarheid. Kan ik makkelijk een Plan B organiseren als er iets gebeurt met mijn dienstverlener? Of als ik ineens niet meer bij data in Amerika kan, heb ik dan een alternatief? Daar moet je, vind ik, aandacht aan besteden en uiteindelijk moet je daar ook voor willen betalen. Dus de overheid heeft daar ook een heel belangrijke taak bij het aanschaffen van IT-oplossingen die ze toch al nodig heeft en dit als het ware on *the fly* kan stimuleren en regelen.”

Verkoulen vervolgt: “Dit geldt in z’n algemeenheid en bij de innovatieve toepassingen waar we het in deze context over hebben geldt dat nog sterker. Het is het bekende kip-ei probleem: als er geen vraag is, gaan leveranciers ook niks ontwikkelen. Dus de overheid kan daar een impuls geven. Dat gebeurt gelukkig ook al, er zijn in Nederland een aantal grote innovatieve data deel projecten, zoals Health-RI. Dat gaat over secundaire data in de gezondheidszorg, dus niet om het primaire proces te ondersteunen maar data gebruiken om innovatie te doen en beleidsvraagstukken te beantwoorden. Een ander goed voorbeeld is het Smart Connected Supplier Network (SCSN) in de Brainport regio. Hier is een federatieve datadeel oplossing geïmplementeerd waar meer dan 400 high tech bedrijven via meer dan tien service providers dagelijks gebruik van maken.”

Speerpunten en sturing

In de op 4 juli jl. aangekondigde Nederlandse Digitaliseringsstrategie (NDS) zijn data, cloud en weerbaarheid drie van de zes speerpunten. “Ergo: dat moet nu echt gaan leiden tot één aanpak van de overheid op die domeinen. In de voorbereidende workshops zei iemand: ‘We hebben een Rijksvastgoedbedrijf, moeten we niet ook naar een Rijkscloudbedrijf toe?’, en dan zie je mensen reageren en zeggen dat het een goed idee is en vervolgens beargumenteren waarom het voor hen toch niet past. Maar die NDS, die ademt nu wel uit: dit is geen keuze meer, we moeten dit samen gaan doen. Vanwege effectiviteit, kosten en functionaliteit. Maar ook omdat we op die manier sturing kunnen geven aan de markt en kunnen zorgen dat we een betere kant

“
Als er geen vraag is,
gaan leveranciers ook
niks ontwikkelen. Dus
de overheid kan daar
een impuls geven

”
ook een rol te spelen in de toekomst, maar wel op een manier waarop wij er nog controle over hebben. En dat zien we dus in die federatieve aanpak en lappendeken.”

Hoe zullen de hyperscalers hierop reageren denk je? Verlies van marktaandeel lijkt een logisch uitvloeisel...
“Ja, dat kan, maar als je naar meer soevereine oplossingen toewerkt, dan gaat er nog een veel grotere markt ontstaan. Als de markt viermaal zo groot wordt en je marktaandeel zou halveren, dan heb je in absolute zin nog je omzet verdubbeld. Dus van die groeiende markt kun je ook met een kleiner marktaandeel beter worden. Het is dus enerzijds gecontroleerd de schade beperken en anderzijds ontstaan ook gewoon nieuwe mogelijkheden en nieuwe kansen. In het huidige geopolitieke klimaat, dat vergeten we wel eens, hebben Amerikaanse klanten ook vragen over afhankelijkheid en continuïteit. In zijn algemeenheid is dit iets wat niet meer weggaat. Dus kun je er maar beter actief wat mee gaan doen, ook als *hyperscaler*.”

Een korte anekdote: “Als ik twee, drie jaar geleden met betrokkenen sprak over het onderwerp digitale autonomie, dan was mijn punchline altijd in de geest van: ‘door het faciliteren van digitale autonomie maken wij innovatie en economische groei mogelijk’; als je weet dat je je data veilig kunt delen met anderen, dan ga je dat ook doen. En dan was de response veelal dat er nog geen beleid was voor digitale autonomie, of soevereiniteit. Mede door de actuele geopolitieke ontwikkelingen – om het maar even neutraal te zeggen – is dat nu prioriteit één, twee en drie in de politiek en dus ook bij de top van de ministeries en de uitvoeringsorganisaties. En ook in het bedrijfsleven, want ook daar wil men dat data veilig zijn, al is het misschien meer vanuit concurrentiële – dan vanuit privacyoverwegingen. Dit zie je ook terug bij het eerder genoemde SCSN voorbeeld: bedrijven delen enerzijds data met elkaar en zijn anderzijds concurrenten. Ze willen dus controle hebben over wat ze delen en met welk doel.”

EuroStack

Ook in Europa zijn data delen en data soevereiniteit op dit moment ‘Chefsache’. Nadat de Europese Commissie (EC) eerder al een consortium van Europese bedrijven opdracht gaf voor het bouwen van Simpl (voor het ondersteunen van datatoegang en interoperabiliteit tussen Europese dataruimten) en het Europese Data

Spaces Support Centre oprichtte, is EuroStack het meest recente initiatief van de EC, samen met meer dan 250 bedrijven en organisaties, waaronder de Nederlandse organisaties RINIS en AMS-IX. EuroStack behelst het maken van een plan voor een soevereine digitale infrastructuur voor Europa over de hele (digitale) stack heen en is ontstaan vanuit een conferentie in 2024 waar DG CONNECT (het directoraat-generaal van de EC belast met digitalisering) en de top van het Europese bedrijfsleven met elkaar spraken over de noodzaak van meer soevereiniteit en hoe die handen en voeten te geven.

“Een soevereine digitale infrastructuur voor Europa over de hele stack heen: dat is van laten we zeggen de onderkant met de grondstoffen en de chips tot aan de bovenkant met de applicatie-laag, de AI-toepassingen, etcetera. Dus over die hele toren wordt nu nagedacht en gesproken over hoe Europa tot meer soevereiniteit en regievoering kan komen met betrekking tot de toepassingen die worden gebruikt. Gaia-X levert daaraan een kleine maar feitelijke bijdrage, en dan vooral over het cloud deel en over het data delen deel”, aldus Verkoulen. Waarbij hij aantekent: “Feit is wel dat je op alle lagen moet nadenken over welke controle je hebt en welke oplossingen van anderen je kunt gebruiken. Want je kunt wel soevereine cloudoplossingen bouwen als Europa, maar met welke hardware ga je dat dan doen? Met welke virtualisatiesoftware? Welke chips ga je gebruiken, enzovoorts.” Het principe van de lappendeken is op al die lagen toepasbaar.



Bouwen aan weerbaarheid van Europa door innovatie, investeringen en soevereiniteit

In 2030 zal elke twee seconden een bedrijf of organisatie slachtoffer worden van een ransomware-aanval; een dramatische versnelling ten opzichte van de voor 2025 voorspelde elf seconden.

Vrijwel wekelijks verschijnen berichten over door statelijke actoren gefinancierde cybercriminelen die zich schuldig maken aan spionage en sabotage, of zich richten op het beïnvloeden van de publieke opinie. “Cyberaanvallen kosten Europese bedrijven nu al miljarden euro’s per jaar. Zulke cijfers houden veel mensen ‘s nachts wakker”, zegt Christiane Kirketerp de Viron. “Vandaar onze focus op cybersecurity en het verbeteren van digitale weerbaarheid in Europa.”

Volgens Kirketerp de Viron wordt de Europese cyberspace voortdurend aangevallen. Het 1 oktober jl. gepubliceerde ENISA Threat Landscape Report¹ bevestigt deze pijnlijke realiteit. In dat rapport staat onder meer dat het afgelopen jaar 53,7 procent van het totaal aantal geregistreerde cyberincidenten de volgende top-5 sectoren binnen de EU trof: het openbaar bestuur (en daarmee de brug tussen overheid en de samenleving), de transport sector, digitale infrastructuur en diensten, de financiële sector en de maakindustrie.

Aanvallen

Kirketerp de Viron: “Het dagelijks leven in Europa wordt overschaduwd door aanvallen op onze vitale, kritieke infrastructuur – zoals die van ziekenhuizen, energienetwerken, transport- en vervoerssystemen en banken. Ter illustratie: een recente cyberaanval op een externe IT-dienstverlener van de check-in- en boardingsystemen heeft het vliegverkeer op meerdere Europese luchthavens verstoord. Bij onder meer Brussels Airport en Berlin Brandenburg kon daardoor alleen handmatig worden ingecheckt en geboard, wat leidde tot forse vertragingen. Daarmee werd pijnlijk zichtbaar hoe kwetsbaar onze systemen kunnen zijn.”

“**Cybersecurity never sleeps - het is voortdurend in ontwikkeling**”

Bovenal maakt deze casus ook het continuïteitsrisico zichtbaar van wat de strategische afhankelijkheid van één externe IT-aanbieder en acute uitval van zijn systemen met zich mee kan brengen, aldus Kirketerp de Viron. Ze waarschuwt: “Een dergelijke verstoring laat zich niet beperken tot de grens en kan er in het ergste geval er zelfs toe leiden dat het verstoringen op continentale schaal veroorzaakt. Cybersecurity gaat daarom niet alleen over het beveiligen van de eigen buitengrenzen, maar gaat juist steeds meer over het beveiligen van de ICT-toeleveringsketens (de digitale, software gestuurde netwerken), het hanteren van een proactieve aanpak voor wat betreft kwetsbaarheden en het beperken van de strategische risico’s en afhankelijkheden.”

Samenwerking

Europa heeft belangrijke fundamenten gelegd met regelgevingsinstrumenten zoals NIS2 en de wet inzake cyberweerbaarheid (Cyber Resilience Act), samen met gerichte maatregelen zoals de EU-Toolbox voor 5-G beveiliging en het Europees actieplan voor cyberbeveiliging in de gezondheidszorg. Maar regelgeving alleen is niet voldoende, stelt Kirketerp de Viron. “We hebben juist ook de behoefte aan een pragmatische uitvoering, en ook een leidraad met standaarden en toegankelijke instrumenten. Cybersecurity moet daarmee voor alle bedrijven, ongeacht hun omvang, laagdrempelig worden gemaakt.” En dat is niet alleen een taak voor de overheid, benadrukt Kirketerp de Viron. “Daarvoor is samenwerking nodig tussen overheidsinstellingen, de private sector, de academische wereld, het maatschappelijk middenveld en de Defensiesector.

Samen met beginnende, baanbrekende start-ups tot en met de meest succesvolle spelers op de wereldmarkt moeten we Europese oplossingen gaan ontwikkelen die onze collectieve veerkracht en digitale weerbaarheid kunnen garanderen en waarborgen.”

In het licht van de steeds veranderende en toenemende dreigingen, alsook de eisen die NIS2 aan bedrijven stelt om hun cyber-



Christiane Kirketerp de Viron is directeur Digital Society, Trust and Cybersecurity van het Directorate-General for Communications Networks, Content and Technology (DG CONNECT) van de Europese Commissie (EC) in Brussel dat verantwoordelijk is voor het cybersecuritybeleid van de Europese Unie (EU).

Kirketerp de Viron. “AI kan dreigingsdetectie en -patching automatiseren. Generatieve AI kan een code scannen op zwakke punten, oplossingen voorstellen en de veilige ontwikkeling versnellen. Maar, AI is slechts één kant van de medaille: quantumcomputing biedt enorme kansen, maar brengt ook evenveel uitdagingen met zich mee. Hoewel het nieuwe mogelijkheden op het gebied van versleuteling (encryptie) en communicatie opent, dreigt het ook de huidige cryptografische methoden achterhaald dan wel overbodig te maken. Europa moet daarom ‘nu’ investeren in quantumbestendige encryptie en veilige quantumcommunicatie.”

Strategisch ecosysteem

Door AI, quantumtechnologie, veilige architecturen en dual-use-capaciteiten (technologie, software of kennis die zowel voor civiele als voor militaire doeleinden kunnen worden gebruikt) te verweven in één uniforme Europese cyber-industriële strategie, is de afhankelijkheid van niet-EU-oplossingen te verminderen en onze technologische autonomie te versterken, meent Kirketerp de Viron. “Dual-use-technologieën bieden een vruchtbare bodem voor convergentie: denk aan AI op het gebied van Defensie en gezondheidszorg, veilige satellietcommunicatie, geavanceerde drones, quantumtechnologieën – dit zijn geen afzonderlijke silo’s, maar onderdelen van een gemeenschappelijk strategisch ecosysteem.”

“Als we Europese cybersecurity start-ups en scalers vragen wat ze nodig hebben, zeggen slechts enkelen dat ze overheidsfinanciering nodig hebben. Maar allemaal zeggen ze: overheidsopdrachten”, glimlacht Kirketerp de Viron. “Daarom mogen we de kracht van de Europese aanbestedingen, juist ook om de Europese cybersecuritysector te helpen groeien, niet onderschatten. Het geeft bedrijven geloofwaardigheid, want als de overheid het inkoopt, dan moet het wel goed en betrouwbaar zijn. En dat zorgt dan tegelijkertijd voor die noodzakelijke innovatie in de publieke sector.”

“*Cybersecurity never sleeps* – het is voortdurend in ontwikkeling”, zegt Kirketerp de Viron. “Als publieke sector moeten we daarin meegaan. Het betekent dat we moeten samenwerken met de industrie - anticiperen in plaats van reageren. Het betekent ook dat we moeten inzetten op een cultuur van vooruitkijken, proactief vormgeven in plaats van reactief verdedigen, investeren in innovatie voor onze veiligheid.”

security-positie te verbeteren, zullen de investeringen in cybersecurity binnen de Europese Unie explosief toenemen, zo voorspelt Kirketerp de Viron. Marktanalisten verwachten de komende tien jaar zelfs een verdubbeling van de groei. Dat terwijl op dit moment circa 75 procent van de Europese cyberbeveiligingsmarkt wordt gedomineerd door bedrijven van buiten de EU. “Die afhankelijkheid is niet alleen een economische kloof – het is ook een kwetsbaarheid van onze weerbaarheid”, zegt Kirketerp de Viron.

Deeptech-innovatie

Om de Europese samenleving veilig, digitaal weerbaar, open en concurrerend te houden, moeten we op drie aspecten voort bouwen volgens Kirketerp de Viron:

1. Deeptech-innovatie;
2. Strategische investeringen;
3. Overheidsopdrachten.

“De huidige Europese Security Operations Centers (SOC’s), die verbonden zijn met regionale cyberhubs, bieden real-time monitoring van dreigingen en geven een snelle, adequate respons door het delen van informatie en inlichtingen. Ze vormen daarmee een goed fundament voor het versterken van ons investeringsfonds en het gezamenlijk ontwikkelen en aanschaffen van cybersecurityoplossingen”. Deeptech-innovatie (en dan met name AI en quantumcomputing) moet centraal staan in onze strategie, stelt

¹ ENISA Threat Landscape 2025 | ENISA

Focus op de toekomst met herstel van groei

De wereld is fundamenteel veranderd. Nieuwe machtsverhoudingen tekenen zich af en er is sprake van een groeiend wantrouwen in instituties. De roep om soevereiniteit klinkt alom. Ook de rol van IT is, mede onder invloed van de opkomst van AI, fundamenteel veranderd. IT is niet langer een ondersteunende tool, maar de driver van vrijwel elke publieke en private organisatie. Ondertussen tornen cyberaanvallen aan de bedrijfscontinuïteit.

“In zo’n veranderende en onzekere wereld zoeken organisaties een veilige haven en partners die vertrouwen en zekerheid bieden. Dat is de rol die wij als Atos Nederland willen vervullen.”

Was getekend: Hans Koolen. Nu de rust binnen de Atos groep is weergekeerd, de financiële situatie is gestabiliseerd en geborgd, en de propositie en het portfolio stevig is gestoeld op vier pijlers (Cybersecurity, Digitale Soevereiniteit, Cloud en Data & AI), kan alle aandacht weer worden gericht op waarde-creatie voor de opdrachtgevers.

“Onze strategische koers bouwt voort op drie kernwaarden: betrouwbaarheid, autonomie en veiligheid”, aldus Koolen. “Betrouwbaarheid betekent dat klanten er altijd op kunnen vertrouwen dat je doet wat je zegt en zegt wat je doet. Autonomie betekent dat organisaties zelf de regie houden over hun IT-infrastructuur en technologie, zonder ongewenste afhankelijkheid van buitenlandse platforms en netwerken. Veiligheid betekent technologie inzetten waar het er écht toe doet om de grote uitdagingen van deze tijd het hoofd te bieden: van desinformatie tot cyberdreigingen en van de energietransitie tot de bescherming van de ‘kroonjuwelen’ van de instituties en de veiligheid in Nederland.”

BV Nederland

“De IT van nu is niet meer de IT van vijf jaar geleden”, gaat Koolen verder. “De hele markt moet gaan inzien dat IT

niet is: ik wil een kilo service of een kilo SAP of een kilo Smart Cloud. De vraag van de klant spitst zich toe op: ‘Ik wil dat je met ons meedenkt in waar onze business staat en kom mij daarin bij de hand houden’. Het makkelijkste voorbeeld dat ik daarin heb: ons Bruto Nationaal Product (BNP) is voor meer dan de helft afhankelijk van niet-grootbedrijven. Bijna de helft van onze economie draait daarop. Net als voor onze grootste klanten geldt ook voor hen: ze moeten mee in de digitale transformatie. Dus de opgave voor de BV Nederland is: hoe gaan we dat bereiken met elkaar? Ik wil aangeven dat de verandering die plaatsvindt in Nederland, die vindt niet vanzelfsprekend plaats. Willen wij als land voortvarend blijven dan zullen we overal, op alle niveaus, moeten nadenken over: wat ben je aan het maken? Hoe kun je geld verdienen met data?”

Anders gezegd: hoe blijf je relevant, hoe blijf je in business? De afhankelijkheid van IT is groot, er speelt geopolitiek van alles, disruptie ligt op de loer. Dat maakt kwetsbaar. Het is ook de strekking van het ABDTOPConsult rapport ‘Van kwetsbaar naar weerbaar’¹ dat 12 september jl. aan de ministerraad is aangeboden. Het rapport kaart ook aan hoe afhankelijkheid van één leverancier in de keten voor kwetsbaarheid kan zorgen. Wat is je Plan B? En zonder dat Atos als een van die partijen wordt genoemd, is dat wel tussen de regels door te lezen.

“Dat is natuurlijk wel de impact geweest van de storm waar we als Atos in terecht waren gekomen”, bevestigt Jitka Beukenkamp. “We zijn door een transformatie gegaan en dat heeft ons tot een expert gemaakt in weerbaarheid. Eerlijk gezegd denk ik dat dat een invalshoek is waar veel organisaties die wij voorzien van onze dienstverlening heel erg geïnteresseerd in zijn, want *‘we have been there, we have done it and we got through it’*. We zijn ervaringsdeskundigen als het gaat over weerbaarheid, over kwetsbaarheid. Het gaat erom dat je ervoor zorgt dat de continuïteit van je business gegarandeerd wordt; en dat is iets waar wij alles van afweten en ook proposities rond hebben.”

Koolen benadrukt dat Atos Nederland - ondanks de crisis waarin de groep zich de afgelopen periode bevond - ➤



Hans Koolen is sinds 9 april 2025 CEO van Atos Nederland en brengt meer dan 30 jaar ervaring mee in leidinggevende functies binnen de IT-sector bij Fortune 500-bedrijven.

Jitka Beukenkamp is 'Head of Growth' Belux, Nederland en Nordics van Atos en daarmee verantwoordelijk voor de commercie binnen deze regio's. Ze stoelt op ruim 25 jaar leidinggevende en sales ervaring.

altijd een financieel gezond en stabiel bedrijf is gebleven. “Vorig jaar was de piek van ons dal, maar geen van onze klanten heeft afscheid van ons genomen; de *customer loyalty* en *customer scores* stegen alleen maar. Atos levert een groot deel van de kritische IT-diensten waarop de Nederlandse samenleving draait. Daar blijven we ons voor inzetten. In het licht van de veranderingen is het eerlijke verhaal aan klanten wel: *sourcing maturity* vereist ook *leadership maturity*. Als je meerdere leveranciers hebt, zul je ook de regierol moeten pakken. Daar ligt in publieke functies wel een uitdaging.”

Europese #1 in cybersecurity

Zichtbaar trots spreekt Jitka Beukenkamp over het recente nieuws dat een omvangrijk meerjarig contract (326 miljoen Euro) voor cybersecuritydiensten is getekend met de Europese Commissie. “Als leidende partner in een consortium gaan we de EU-instellingen beschermen door middel van een reeks van diensten, waaronder incidentrespons, digitale forensische analyse, dreigingsinformatie en offensieve beveiliging. We voelen ons erkend als de Europese nummer één op het gebied van cybersecurity”, glimlacht Beukenkamp. “En als de Europese Unie je vertrouwt, ja, wie dan niet?” Ze wijst ook op Atos' lange staat van dienst bij het Internationaal Olympisch Comité (IOC) en het Internationaal Paralympisch Comité (IPC), eerst als system integrator later als officieel IT-partner. “Vanaf 1989 tot en met de Zomerspelen van Parijs in 2024 hebben we 35 jaar lang aangetoond het grootste sportevenement ter wereld veilig te kunnen laten verlopen, juist op een actueel thema als digitale weerbaarheid. De Olympische Spelen staan voor een complexe combinatie van technologie, processen en mensen. De ogen van de hele wereld zijn erop gericht. Als het op de kleinste details aankomt, mag er echt niets misgaan. Met die laatste editie in Parijs behaalden wij een mijlpaal op het gebied van IT-levering: ze staan bekend als ‘de meest digitale en veilige in de geschiedenis’” Bewezen ervaring waarvan ook de UEFA gebruik van maakt. Zo is Atos sinds 2022 de officiële technologiepartner van UEFA National Team Football. De samenwerking is gericht op het beheren en verbeteren van de technologie voor UEFA's nationale voetbalcompetities tot minstens 2030, inclusief grote competities zoals de UEFA Nations League Finals en de UEFA EURO-toernooien. Atos levert hiervoor IT-diensten, evenementen- en diffusiesystemen en cybersecurity, en ondersteunt het optimaliseren van de hybride cloud-omgeving.

Betrouwbare partner

Bij de wedstrijden van Oranje speelt Atos dus mee als betrouwbare partner. Net zoals zij dat is voor een grote

Gesprek over business continuïteit is de kapstok voor iedere discussie over soevereiniteit

schare aan opdrachtgevers in alle sectoren van de Nederlandse samenleving: overheden, banken, verzekeraars, industrie en zorginstellingen. Beukenkamp: “Met Rijks-overheidsovereenkomsten voor kritieke diensten als SAP-bedrijfsvoering, hosting AOW en Kinderbijslag en een nieuw systeem voor de zorgindicatie hebben wij ook de morele verplichting om hierin te voorzien met passende, mitigerende maatregelen en uitwijkvoorzieningen. Wij geven de digitale transformatie vorm.” “Analisten zeggen dat er in Europa op dit moment twee maximaal drie partijen zijn die echt Europese diensten in de breedte kunnen aanbieden, *at scale*. Atos is er daar een van”, zegt Koolen. “Dat is een cruciaal gegeven in de context dat Europa zich strategisch en autonoom wil positioneren om haar afhankelijkheid van andere regio's te verkleinen in een wereld waarin machtsblokken verschuiven. Zeker nu blijkt dat de Verenigde Staten niet meer de betrouwbare bondgenoot uit het verleden zijn en Europa op allerlei niveaus waarborgen probeert in te bouwen om minder afhankelijk te worden.” Zeker in een open en exportgerichte economie als Nederland is deze autonomie ontzettend belangrijk. Door zijn geografische ligging en kenniseconomie heeft Nederland een belangrijke strategische, fysieke en digitale koploperspositie in de wereld. Er lopen bijvoorbeeld ondergrondse leidingen voor de energievoorziening en er ligt een hoog ontwikkelde digitale infrastructuur waar virtuele snelwegen van over de hele wereld elkaar kruisen. Voor de economische veiligheid van Nederland zijn volgens de Nationaal Coördinator Terrorismebeveiliging en Veiligheid (NCTV) drie zaken van essentieel belang: de continuïteit van vitale processen, het verkleinen van risicovolle strategische afhankelijkheden en het voorkomen van de ongewenste overdracht van kennis en technologie.²

‘Your Data, Your Rules’ is de belofte van Atos Nederland en die onderstreept de focus op het bieden van digitale oplossingen die relevant zijn; voor klanten en samenleving. “We zetten technologie in om alles wat van waarde is te beschermen en te versterken”, aldus Koolen. Het weerspiegelt de ambitie van Atos om haar digitale expertise in te zetten om een positieve impact te realiseren, voor uiteenlopende sectoren en op thema's als veiligheid en duurzaamheid. De herijking van Atos' strategie is gebaseerd op vier pijlers: Cybersecurity, Digitale Soevereiniteit, Cloud, Data & AI.

Cybersecurity

Cyberaanvallen worden steeds geraffineerder en kunnen leiden tot operationele verstoringen, financiële verliezen en het verlies van gevoelige data, maar ook



tot reputatieschade. Nieuwe dreigingen - mede door de inzet van generatieve AI en *deepfakes* - maken het speelveld nog complexer. Als gevolg van hybride oorlogsvoering door onder meer Rusland en China nemen ook geopolitiek gemotiveerde cyberaanvallen toe; statelijke actoren vallen via zwakke schakels in de keten steeds vaker specifieke doelwitten in vitale sectoren aan. Zo was het Internationaal Strafhof tijdens de NAVO-top in juni 2025 nog doelwit van een cyberaanval. Het aantal cyberaanvallen is sinds het uitbreken van de Coronapandemie ruim verdubbeld. In combinatie met de steeds verdergaande digitalisering, de opkomst van AI en geavanceerde technologieën en toenemende geopolitieke spanningen wereldwijd, vormt dit een ernstige bedreiging voor de (financiële) stabiliteit. De economische schade door cyberaanvallen zal wereldwijd volgens Cybersecurity Ventures en het World Economic Forum in 2025 naar verwachting 10,5 biljoen dollar bedragen. Als cybercrime als ‘land’ zou worden beschouwd, zou dit de op twee na grootste economie ter wereld vertegenwoordigen, na de VS en China.

“Ik wil niemand op de tenen trappen maar ik denk dat het bewustzijn hierover en daarmee het gevaar voor de business

“We zetten technologie in om alles wat van waarde is te beschermen en te versterken”

continuïteit nog onvoldoende is”, zegt Beukenkamp. Ze wordt daarin bevestigd door een onderzoek van ABN AMRO³ waaruit blijkt dat de weerbaarheid van Nederlandse bedrijven tegen cyberaanvallen achterblijft. Cybersecurity wordt nog te vaak beschouwd als sluitstuk en niet als wezenlijk onderdeel van de bedrijfsstrategie, stelt Koolen. Het is daarom van wezenlijk belang dat de Chief Information Security Officer (CISO) een plaats in de boardroom krijgt en op strategisch niveau meedenkt over de beveiliging van kritische IT-infrastructuur, data en bedrijfsprocessen.

Koolen: “Security is niet langer alleen een technologisch vraagstuk, maar moet worden ingebed in de strategie om te kunnen fungeren als motor voor veilige en beheersbare (digitale) groei. Het hoort bovenaan de agenda in de bestuurskamer. Dit gaat ook gepaard met het creëren van bewustwording over de risico's die er zijn. Sommige

politici pleiten ervoor om een spreekwoordelijke ‘muur’ om Nederland te zetten om ons land af te sluiten van dreigingen van buitenaf. Zo zou je ook de digitale grens kunnen sluiten. Maar stel je voor wat er zou gebeuren als we dat doen? Dat betekent dat je geen buitenlandse websites meer kunt raadplegen, geen pin-transacties, het luchtverkeer platgelegd wordt en je mobiele devices niet langer kunt gebruiken.”

Met de invoering van Europese regelgeving als de NIS2-richtlijn en de Cyber Resilience Act wil Brussel de digitale weerbaarheid van essentiële (vitale) sectoren versterken. De NIS2-richtlijn - de nieuwste versie van de Europese richtlijn voor netwerk- en informatiebeveiliging - heeft als doel de cyberbeveiliging in de Europese Unie te versterken. De regelgeving helpt organisaties zich te beschermen tegen cyberdreigingen en zorgt ervoor dat de digitale infrastructuur van de EU veiliger en robuuster wordt. Zo verplicht NIS2 bedrijven onder meer tot risicobeheersing, het melden van incidenten en ketenverantwoordelijkheid. Het is cruciaal dat Nederlandse bedrijven voorbereidingen treffen om aan deze Europese verplichtingen te voldoen, aangezien deze regelgeving vanaf nu, het derde kwartaal van 2025, van kracht wordt. ➤

Om bedrijven hierbij te ondersteunen, lanceerde Atos in mei al de SecureHorizons NIS2 Compliance Manager. Deze draait op het ServiceNow-platform en biedt klanten één technologisch platform dat handmatige processen vervangt door efficiënte, gestandaardiseerde en geautomatiseerde workflows, waarmee organisaties kunnen voldoen aan de vereisten van de NIS2-richtlijn.

Digitale soevereiniteit

Digitale soevereiniteit is de tweede pijler in de herijkte strategie van Atos. Cloud is hierin fundamenteel. Europa kan zich, vooral vanwege geopolitieke ontwikkelingen, niet langer veroorloven om zo afhankelijk te zijn van Amerikaanse *hyperscalers* als Microsoft, AWS en Google. Het roept ongemakkelijke vragen op: wat als de Amerikaanse cloud door een politiek besluit 'op slot' gaat? Wat als cruciale data van de ene op de andere dag ontoegankelijk zijn?

Koolen: “Er is door de *hyperscalers* inmiddels zo'n 800 miljard geïnvesteerd in waar ze nu staan. Het is een illusie om te denken dat we dit in Europa zonder overheidssteun kunnen doen; we komen niet eens in de buurt. Daarbij merk ik wel op: er is al een vierde of een vijfde (semi-)publieke cloud en dat is de private cloud. Denk aan oplossingen als OpenShift en OpenStack. Daarmee worden de meest belangrijke functionaliteiten van onze klanten in een public cloud afgedekt in een private cloud. Het is belangrijk voor ons om daar met klanten een eerlijk gesprek over te hebben. Als je CEO bent van een private partij ben je geneigd te denken dat als je uit de publieke cloud gaat, je time-to-market lager is. Maar dat is te betwijfelen.”

Beukenkamp: “Het gesprek over business continuïteit, is wat mij betreft de kapstok voor iedere discussie over soevereiniteit. Hoe ga ik om met welke vorm van data? Is dat publieke data, dan is er niks aan de hand om het in de public cloud te hebben staan in de VS. Maar is het *highly confidential* of business *disruptive* als het door de Amerikanen wordt stopgezet, of door de Chinezen, of door wie dan ook, dan heb je die Europese of private cloud nodig. Het betekent dat we eigenlijk teruggaan naar een discussie die ik eerder heb gehad met klanten, namelijk: ga je alles in de publieke cloud zetten, of blijft een hybride cloud eigenlijk de norm? Als je mij dit drie jaar geleden had gevraagd dan had ik waarschijnlijk gezegd: ik denk dat iedereen op den duur wel naar de publieke cloud gaat want de investeringen daarin zijn zo veel hoger en dus krijg je veel meer *return on investment*. Maar als je me nu die vraag stelt, met alle geopolitieke druk, denk ik dat ik dat antwoord niet op die manier zou geven. Dan is een hybride cloud, waarbij een deel in een private omgeving of op een Europese cloud draait

en een ander deel - dat sneller en beter je business kan ondersteunen - in de publieke cloud draait, een beter alternatief. Dat zijn allemaal oplossingen waarover we in gesprek kunnen. Want voor een overheid brengt dat natuurlijk weer een heel andere dynamiek dan voor een commercieel bedrijf.”

Koolen refereert aan een recent onderzoek van White-lane Research onder 300 relaties. “Op de vraag wat zij gaan doen met *hyperscaler* gebruik geeft een derde (!) aan bezig te zijn met repatriëring, dus het terugbrengen van public naar iets anders. Nog een derde, zegt dat binnen nu en twee jaar te gaan doen. In totaal dus tweederde, dat is nogal wat.”

En wat is de rol van Atos hierin?

“Het repatriëren zelf – het beheren daarvan. De Atos cloud is de vierde public provider; wij bieden de services die een AWS biedt, maar dan in een soevereine Europese omgeving. Niet alles, ik denk 80 procent. Dat doen we niet alleen, maar met partners. Je kunt naar cloud kijken in z'n meest primaire vorm en dan is het *'just someone else's computer'*. Maar het zijn pas de services die je daar bovenop aanbiedt, die differentiërend werken. Wat het interessant maakt is dat ik als klant kan zeggen: van die computer wil ik dat de helft SAP doet en de andere helft Office, ik noem maar wat. En ik hoef maar een balkje aan te zetten op m'n dashboard en 't werkt. Dat is de *value add*. Die klant kan besluiten: ik ga m'n eigen software schrijven, in *serverless* code – dus je hebt geen operating system meer nodig, het platform zelf kiest wel waar het wat neerzet. Dat kan allemaal.”

Zo kiezen organisaties in de gezondheidszorg, Defensie, de overheid en de financiële sector steeds vaker voor een hybride IT-strategie, waarin publieke cloudoplossingen worden gecombineerd met soevereine alternatieven. Soevereiniteit betekent ook geen afhankelijkheid van buitenlandse AI-modellen, geen ondoorzichtige data-uitwisseling en geen 'lock-in' situaties die innovatie belemmeren. Zodat bedrijven het eigenaarschap en de controle over hun IT-infrastructuur kunnen behouden. Mei 2024 was de lancering van 'Atos Sovereign AI' - een aanbod van Dell Technologies voor de productie en het onderhoud van generatieve AI-modellen - om tegemoet te komen aan de groeiende behoefte aan datasoevereiniteit en dataprivacy. En mei 2025 opende Atos Belux, Netherlands and Nordics in Amstelveen de deuren van het 'Sovereign Innovation Center' (SIC). Dit is bedoeld om samen met partners te innoveren, op basis van Europese regelgeving, met volledige controle over de eigen data en technologie. Het SIC ondersteunt organisaties bij hun



digitale transformatie en waarborgt datasoevereiniteit en technologische onafhankelijkheid. “Op deze manier helpen wij organisaties niet alleen zich voor te bereiden op potentiële bedreigingen, maar óók om nieuwe kansen te benutten”, aldus Beukenkamp. Europa moet op eigen benen kunnen staan. Niet alleen als het gaat om de energietransitie of de winning van zeldzame aardmetalen voor de productie van accu's, windmolens of zonnepanelen, maar ook op het gebied van herbewapening. In 2025 heeft de EU een grootschalig programma hiervoor aangekondigd: *ReArm Europe Plan/Readiness 2030*. “Daarvoor ligt 800 miljard klaar. Dit biedt kansen om de economie in Europa en Nederland te versterken.”

AI & Data

Over de kansen en bedreigingen van kunstmatige intelligentie (AI) wordt veel gezegd en geschreven. Het gebruik van AI in openbare diensten kan de kosten verlagen en nieuwe mogelijkheden bieden voor openbaar vervoer, onderwijs, energie- en afvalbeheer en de duurzaamheid van producten verbeteren. Voor bedrijven kan AI de ontwikkeling mogelijk maken van een nieuwe generatie producten en diensten, inclusief in sectoren waar Europese bedrijven al sterk aanwezig zijn: groene en circulaire economie, machines, landbouw, gezondheidszorg, mode

en toerisme. Criticasters en sceptici daarentegen wijzen op het gebrek aan transparantie, op de gevolgen voor privacy en gegevensbescherming, op misbruik door criminelen, op statelijke actoren die het toepassen voor het verspreiden van nepnieuws of het manipuleren van verkiezingen, op de impact op het milieu, en op het risico dat de technologie in handen is van een relatief kleine groep grote bedrijven. “Allemaal waar”, zegt Koolen. “AI is een exponent van de vierde industriële revolutie en een revolutie heeft per definitie disruptieve kenmerken. De Europese Commissie heeft vorig jaar de AI Act aangenomen, de eerste en zeer uitgebreide wetgeving ter wereld op het gebied van AI, om te borgen dat systemen die in Europa worden gebruikt veilig zijn en de grondrechten respecteren. Duidelijk is dat AI een onomkeerbare ontwikkeling is.”

Hij legt uit dat Atos autonome AI-oplossingen biedt die volledig binnen een Europese infrastructuur draaien. “In samenwerking met partners als Dell Technologies en Red Hat hebben wij sectorspecifieke AI-modellen ontwikkeld die getraind zijn op lokale data, met volledige transparantie en controle. Deze modellen draaien op eigen servers, in eigen datacenters - zonder afhankelijk te zijn van Amerikaanse cloud-providers - en voldoen aan de strengste eisen voor dataveiligheid en privacy.”

Beukenkamp: “We hebben afgelopen juli 'Atos Polaris AI' geïntroduceerd. Dit is een platform van AI-agents en gecreëerd voor het ontwikkelen, testen en uitvoeren van IT-operaties. Het ondersteunt engineers in alle fasen van het ontwikkelproces. Dit helpt organisaties om hun digitale transformatie te versnellen. De AI-agents die zijn ontwikkeld met dit AI-platform helpen bedrijfsresultaten te verbeteren door ingebouwde functionaliteiten, die zijn gericht op autonoom plannen, samenwerken, handelen en leren. Het platform biedt daarnaast een 'Agent Ops'-functionaliteit om prestaties af te stemmen op business KPI's.” “Dit gaat bijdragen aan een versnelling in de digitale transformatie van onze klanten naar AI-oplossingen, zodat zij maximale waarde uit hun cloud-investeringen kunnen halen.”

¹ <https://www.rijksoverheid.nl/documenten/rapporten/2025/09/12/rapport-van-kwetsbaar-naar-weerbaar>

² <https://www.aivd.nl/actueel/nieuws/2022/11/28/andere-landen-bedreigen-nederlandse-veiligheid-steeds-meer>

³ <https://www.abnamro.nl/nl/zakelijk/insights/sectoren-en-trends/alle-sectoren/cyberweerbaarheid-ondernemers-blijft-achter-bij-realiteit.html>



Martijn Lucassen is sinds 1 april 2025 directeur Digitale Economie bij het ministerie van Economische Zaken en lid van het managementteam van het directoraat-generaal Economie en Digitalisering. Hiervoor was hij adviseur Europese Zaken bij het Kabinet Minister-President van Mark Rutte (ministerie van Algemene Zaken) en vervulde vanuit het ministerie van Buitenlandse Zaken verschillende diplomatieke posities op onder meer posten in Ramallah en Skopje.



Maaïke Okano-Heijmans is senior onderzoeker en hoofd van het programma 'Geopolitiek van Technologie en Digitalisering' op Instituut Clingendael in Den Haag. Ze is tevens gastdocent aan de Universiteit Leiden. Met haar team doet zij beleidsgeschiedonderzoek over de digitale autonomie, economische veiligheid en technologische concurrentiekracht van Nederland en de EU in een snel veranderende wereld.

Zoeken naar handelingsperspectief

Geopolitieke ontwikkelingen zetten druk op het Europese streven naar meer digitale soevereiniteit en technische zelfredzaamheid. Ook in ons land geldt in toenemende mate een *sense of urgency*. Het ministerie van Economische Zaken heeft kennisinstellingen TNO, HCSS (The Hague Centre for Strategic Studies) en Clingendael gevraagd om vanuit technologisch en geopolitiek perspectief te onderzoeken waar in het digitale domein de meest strategische afhankelijkheden zitten en wat manieren zijn om die waar nodig en gewenst te adresseren. Dat heeft geresulteerd in een Agenda Digitale Open Strategische Autonomie, kortweg DOSA [zie kader].

November 2022 was er al het beleidsdocument Strategie Digitale Economie (met als ondertitel: Werken aan een weerbare en welvarende digitale economie), “en daar staat alles in”, zegt Martijn Lucassen, “maar de actuele boodschap is: het moet meer begrepen en gevoeld worden op het politiek bestuurlijke niveau. Het is natuurlijk heel abstract, het digitale domein, maar we hebben in een diagram het lagen model proberen te verduidelijken. En dan zie je - of je het nu hebt over 5G, over chips, over AI, over smartphone apps, over grondstoffen, infrastructuur, satellieten, datacenters, zeekabels, noem maar op -, dat het allemaal met elkaar samenhangt en elkaar beïnvloedt.” Ergo: het is belangrijk om de samenhang der dingen te begrijpen, stelt Lucassen, vervolgens zaken te prioriteren en te zoeken naar handelingsperspectief. Want ja: de tijd tikt door natuurlijk. En dan is er de geopolitieke context van vandaag de dag. Lucassen: “Wat gebeurt er op technologiegebied in de VS, in China, en tussen die twee onderling, en hoe

verhoudt Nederland - en Europa - zich op dat wereldtoneel tot die twee grote actoren en de tech-bedrijven die daarbij horen?”

Driehoek

Maaïke Okano-Heijmans reageert en geeft duiding: “Vergeet ook India niet. Dat is ook een grootmacht en zit er net weer even anders in. India brengt nuance aan in wat de EU voorstaat met een focus op *Human Centred* (de burger, de consument) en regulering, investeren in het borgen van privacy van burgers, dat er ethische overwegingen zijn, dat er een vertrouwensbasis moet zijn en transparantie. Als je dat stelt naast het Amerikaanse uitgangspunt dat vooral bedrijven hun ding moeten doen - ik noem dat *Cowboy Capitalism* - en China dat vindt dat de staat het recht heeft op toegang tot jouw data en dat het hen vrij staat om daarmee te doen wat zij willen, daar staan we in Europa ver vanaf. India zegt: ‘wij willen graag ontwikkelen en dan is toegang tot data nodig. We laten ons inspireren door de EU waar het gaat om privacy wetgeving, maar wij zijn wel India dus ga niet zeuren als we het anders invullen’. Dus dat is belangrijk om voor ogen te houden als we naar het bredere plaatje kijken. Wat we ook aan de rest van de wereld willen en kunnen brengen, het gaat om het handelingsperspectief uiteindelijk. Prima als je je boodschap wilt overbrengen van *Human Centred*, maar je moet ook ruimte laten voor de business optiek van de Amerikanen, want die

doen ook heel veel zinnigs en verdienen er heel veel geld mee. Dus die driehoek van prioriteit op burgers-bedrijven -staat vind ik heel belangrijk als een soort van raamwerk voor het denken; en tegelijkertijd moet je er niet in vast zitten.”

Wil Europa verdere stappen zetten ter versterking van de digitale economie (met een markt van 500 miljoen bewoners) en vergroting van haar digitale soevereiniteit, dan is samenwerking noodzakelijk. Op het gebied van privacywetgeving (in ons land bekend als de AVG: Algemene verordening gegevensbescherming) is dat gelukt. Wat is er nodig?

Okano-Heijmans: “De totstandkoming van die Digital Services Act (DSA) en Digital Markets Act (DMA) was een testcase, ook in de zin van hoe kunnen we daarop leveren? De wetgeving is mooi, maar helaas blijft de implementatie achter. Waar zijn de bedrijven die helpen om dit goed te implementeren op een manier die voor de gebruiker fijn is? Daar is geld mee te verdienen. Vorig jaar is ook de AI Act vastgesteld voor de regulering van artificiële intelligentie en dat is ‘s werelds eerste wetgeving die bindend is op AI. Dus op dat vlak zijn we wel een inspiratie voor anderen. Ik hoor ook van sommige Amerikaanse bedrijven ‘go for it!’ want van onze eigen overheid kunnen we niks verwachten’. Dus behalve kritiek oogsten we ook veel waardering en zien bedrijven het als een mogelijkheid om te voldoen aan een *golden standard* waarmee ➤

ze wereldwijd kunnen aankomen. Maar ik denk dat we moeten oppassen dat we straks niet alleen op regulering de inspiratie zijn voor andere landen en dat landen die graag een beetje 'staatssurveillance' willen, gaan shoppen bij de Chinezen en dat landen die een business first model willen, vooral doen wat de Amerikanen doen. Dan eindigen we in een polaire wereld die niet zo zinnig is."

Durfmentaliteit

Lucassen knikt instemmend: "Iets meer een durfmentaliteit, een *can do*-mentaliteit, in de economie en samenleving rond digitale technologie is denk ik waar we nood aan hebben. Het vraagstuk van onze afhankelijkheid op digitale technologie is een vraagstuk van schaal en van kapitaal. We hadden het daarnet over wet- en regelgeving en hoe lastig het soms is om het geïmplementeerd te krijgen. Maar bedrijven hebben niet alleen met digitale wet- en regelgeving van doen, maar ook met fiscale wet- en regelgeving en met arbeidsrecht. We hebben in de EU 27 lidstaten en vele verschillende wettelijke kaders waaraan bedrijven moeten voldoen. Als je dat vergelijkt met de VS: als je daar een bedrijf hebt, kun je direct die markt van 340 miljoen consumenten op. Dus het zit niet eens sec op digitale wet- en regelgeving, maar ook op de schaal van het ondernemersklimaat in Europa."

"Ik denk dat wij een fantastisch ecosysteem hebben voor fundamenteel onderzoek en innovatie. En dat hebben ze in de VS ook rond hun topuniversiteiten en Silicon Valley. Maar de vervolgstap van een *start-up* naar een *scale-up*, daar gaat het hier vaak mis. Er is nu wel consensus over – en ik vat dat dan maar even samen als 'schaal en kapitaal' – dat het groeien als bedrijf en het geld om die groei te kunnen financieren, dat we in algemene zin in Europa minder bereid zijn om risicodragende investeringen te doen. Pensioenfondsen en durfkapitaal zouden meer in die technologieën van de toekomst moeten investeren. Je ziet op dit moment dat *start-ups* en *scale-ups* merendeels Amerikaans gefinancierd zijn en dat ze vervolgens na die eerste stap de échte stap maken door naar de VS te gaan. Dus maak het eenvoudiger, door wet- en regelgeving, om te ondernemen op de interne markt en zorg ervoor – en dat is bijna een cultuurvraag – dat er meer *appetite* komt om durfinvesteringen te doen. Er is genoeg geld in Europa, dat is het punt niet."

Okano-Heijmans haakt in: "Ik zou ook nog inkoopmacht van de overheid willen noemen. Daar zit een echte kans om een markt te creëren voor Europese bedrijven. Dat betekent als de overheid inkopen gaat doen voor bijvoorbeeld software, dat de inkoopprocedure niet aanstuurt op Microsoft, zoals nu feitelijk een beetje het geval is, maar aanstuurt op een Europese oplossing. Daar-



mee zwengel je die markt aan, je geeft een stempel van goedkeuring: als de overheid zo groot inkoopt, dan moet het wel goed en betrouwbaar zijn. Dus die markt kun je als overheid helpen ontwikkelen. Die markt moet ook substantieel zijn, een bepaalde omvang hebben. Want als de gemiddelde winkel op de hoek hier overstapt op Europese software, ja dat is fijn natuurlijk, maar dat gaat het verschil niet maken. Maar, de overheid kan dat verschil maken. En daar zijn we heel terughoudend in geweest, om allerlei redenen. Ik wil er geen anti-Amerikaans verhaal van maken, dat is het ook niet, maar ik geloof wel in een pro-Europees verhaal."

Maar is er al voldoende aanbod aan Europese technologie en producten?

Lucassen: "Dat verschilt en moet je ook per technologie bekijken. We spraken zojuist over de geopolitiek en de urgentie die we in het verhaal willen brengen. Ik denk dat er consensus aan het ontstaan is, ook politiek, op die probleemanalyse dat we écht uit een ander vaatje moeten tappen. We hebben heel lang gedacht dat we - vanuit de langjarige samenwerkingen en de diepe interdependentie die we met name trans-Atlantisch hebben, dat we prima kunnen vertrouwen op technologie en infrastructuur die je van buiten betreft. Terwijl we daar vroeger ook zelf een heel grote speler in waren, hè, dus dat is ook iets waar we langzaam maar zeker onze eigen marktpositie hebben verloren. In 2010 kwam ongeveer een kwart van de digitale economie vanuit Europese bedrijven en in 2022 was dat gedaald naar 11 procent en ik denk dat we nu misschien wel onder de 10 procent zitten. Dat kachelt dus hard achteruit."

Hij vervolgt: "Dat vonden we een tijd lang niet erg maar door de actuele geopolitieke ontwikkelingen ervaren we dat nu wel zo. En hoe ga je daar vervolgens mee om?



Ik denk met een aantal maatregelen. Het belang van wetten en dus effectieve stevige regelgeving is en blijft belangrijk. Dat hoort bij ons Europees model, dat is om een concurrerende economie te hebben, dat is om veilig te zijn. Het heeft te maken met wat voor samenleving we willen zijn. Dit gaat om bedrijven die over onze data gaan. Dit gaat over wat er op onze schermen komt; wat heel erg bepalend is voor de publieke opinie. Het gaat om nieuws, het gaat om democratie, het gaat over verkiezingen, dus het is een heel wezenlijk onderdeel van onze economie en samenleving." Lucassen stelt dat in die context van krimpende capaciteit je wel aan wet- en regelgeving kunt bouwen (en daarmee veiligheidsperspectief), "maar als er geen alternatieven zijn, dan ben je toch kwetsbaar. Ook ik ben niet anti-Amerikaans, ik geloof heel erg in dat partnership, die interdependentie en strategische samenwerking. Overigens niet alleen in die driehoek, maar juist ook met Japan, Korea, India, de hele wereld. En zeker ook trans-Atlantisch, want dat is gewoon een bondgenoot van ons. Maar naast wet- en regelgeving – die je ook effectief moet uitvoeren zodat bedrijven daarmee uit de voeten kunnen – waarmee we spelregels in het digitale domein hebben gebracht, denk ik dat we ook moeten focussen op spelregels voor innoveren en investeren."

Spelregels

Gevraagd naar hoe die spelregels er dan uit zouden kunnen zien, spelen Okano-Heijmans en Lucassen de bal over en weer, inherent aan de constructieve wijze waarop al langer door hen wordt samengewerkt. Ze refereren aan een investeringsagenda, want: "Als overheid kun je dat niet allemaal zelf financieren en zeker niet ontwerpen, maar je kunt wel proberen daar een ecosysteem voor te creëren waarbij je zorgt dat het kapitaal gaat stromen, dat die markt gaat groeien. Je kunt als overheid ook *launching customer* zijn en dat betekent ook dat je bewuster gaat inkopen. Het moet dan ook mogelijk worden gemaakt dat de overheid dat kan doen. We kennen een aanbestedingswet, en die is eigenlijk primair



gericht op prijs en kwaliteit. Je moet geen industriepolitiek gericht protectionistisch systeem willen, maar je kunt je wel voorstellen dat gezien de huidige, strategische afhankelijkheden, dat je de ruimte moet hebben om in bepaalde gevallen extra gewicht toe te kennen aan een Europees alternatief." Bij een Europees alternatief gaan de gedachten niet perse uit naar een nieuwe *hyperscaler*, maar eerder naar bedrijven met aan elkaar complementaire technologie en producten.

Hoe kansrijk is dit?

"Nou, ik ben wel een optimist. Op het gebied van AI lopen we achter, maar die race is nog niet gelopen. De infrastructuur die wordt nu gigantisch hard opgebouwd in de VS, China en het Midden-Oosten, dus dat is lastig voor ons, maar voor het ontwikkelen van AI-modellen en toepassingen liggen er volop mogelijkheden. De Europese Commissie heeft de bouw van gigantische fabrieken aangekondigd, ook Nederland wil daar aan meedoen via onder andere een AI fabriek in Groningen. Dus als we ons focussen op die onderdelen van AI-technologie waar wij denken dat we een kans hebben, nationaal en Europees, waar onze uitgangspositie goed is, dan zijn we zeker kansrijk. Ik denk ook aan quantum en 6G." Okano-Heijmans deelt het optimistische gevoel maar tekent aan: "Waar regulering in de begroting is verwerkt – en met alle respect voor iedereen die daaraan keihard werkt, het is ook de core business van de overheid – gaat hierin investeren geld kosten dat niet in de begroting staat. Dit is van een totaal andere orde dan we gewend zijn de afgelopen decennia en ook niks in vergelijking met wat eerder is gedaan ten aanzien van de topsectoren."

Is er iets te zeggen voor een consortium waarin de overheid participeert als hoeder van noemt 't maar 'de maatschappelijke kaders en principes'?

Lucassen: "Ik kan me heel goed voorstellen – en dat zie je nu ook wel op allerlei *communities* rondgaan – dat er een ►



soort Deltaplan op AI nodig is. Dit is een disruptieve systeemtechnologie die van grote invloed gaat zijn op alle andere topsectoren. Met AI gaan we straks de biotechnologie van de toekomst ontwikkelen, de precisielandbouw, denk aan *life sciences* en *health issues*, gewoon alles wat in de zorg gebeurt, robotica, dat wordt straks allemaal door AI-technologie en rekenkracht aangedreven. Dat is de grote disruptie die zich aandient. Dus als we nou één ding moeten doen - en dat is ook mijn hartenkreet - we moeten durven kiezen. We zijn notoir slecht gebleken in het durven kiezen en natuurlijk komen we nooit uit op één technologie, maar als we er één zouden mogen doen, dan zou dat AI moeten zijn.” Hij voegt eraan toe: “In Nederland is het vertrouwen in AI als technologie best wel laag in vergelijking met andere landen, dus daar hebben we nog een wereld te winnen, ook als overheid. Het is denk ik onze dure plicht om daar heel zorgvuldig in te zijn en de juiste keuzes in te maken. Want het gaat namelijk wel gebeuren. Dus pak dan je rol en doe dat verantwoordelijk en wees daar transparant over.”

Economische veiligheid

Okano-Heijmans: “We hebben een survey gedaan onder bedrijven: hoe zien jullie nou geopolitieke ontwikkeling, staat dat op de agenda? Wat de overheid verstaat onder economische veiligheid, kennen jullie dat überhaupt? Nou... slechts de helft van de bedrijven in onze survey is daarmee bekend. Dat komt ook doordat wij geen wetgeving voor economische veiligheid hebben. Pas als het een wet wordt, dan gaan we ernaar kijken. Dat gat tussen die twee is de reden dat ik blijf zeggen: je moet veel meer het gesprek gaan voeren zodat je misschien minder aan regelgeving hoeft te doen en bedrijven toch ergens mee aan de slag gaan. En dan kom je misschien ook tot oplossingen waarbij je snapt hoe je bedrijven het best in hun kracht kan zetten, in

plaats van dat je ze met regels iets oplegt. Want in de huidige situatie zouden vooral die Europese bedrijven in een achterstand kunnen komen ten opzichte van niet Europese bedrijven. Dus regels, daar help je niet altijd mee. Wel als je dan een *golden standard* kan creëren, maar bedrijven in hun kracht zetten, wat hebben ze daarvoor nodig, weten we dat eigenlijk? Op basis van onze survey zou ik wel durven zeggen dat er nog heel veel ruimte te winnen is in bedrijven aanmoedigen om te doen wat de overheid hoopt dat ze doen: een soort van geopolitieke verantwoordelijkheid nemen, dat ze goed divers zijn, dat ze niet enorm afhankelijk zijn van landen die we eigenlijk niet vertrouwen of die al veel te veel aan ons verdienen. Daarover kan je het gesprek voeren maar dan willen zij natuurlijk ook weten hoe ze daarin kunnen worden geholpen.” Ze vervolgt: “Als we praten over wat haalbaar is, dan kunnen we denken in hele grote mooie dromen - en die moeten we ook hebben - maar mijn realistische stip aan de horizon is vaak net iets kleiner. Maar, die kan groter worden als we het echt Europees afstemmen en kijken: waar zijn wij heel sterk? Bedrijven als ASML, Nokia, Ericsson - en ook minder bekende, kleinere sterren in andere tech sectoren - laat ze *shinen* en de wereld veroveren, moedig ze aan, help ze om binnen te komen bij landen die voor ons strategisch belangrijk zijn. Daar kan je wat winnen.”

Okano-Heijmans richt zich tot Lucassen en vraagt: “Moeten we dan ook de rol van de toezichthouders een beetje oprekken? Moeten we hen een soort van kanarie in de kolenmijn laten zijn? Want zij zien dingen langskomen natuurlijk... ik denk aan zonnepanelen, die met staatshulp uit China hier zijn gekomen en die hebben de hele Europese markt verziekt eigenlijk, dat hebben we niet kunnen voorkomen. Je ziet dat nu weer gebeuren met humanoïde robots, of hoe noem je dat in goed Nederlands? Als zij zoiets signaleren, kunnen we zo'n golf dan weerstaan?”

Lucassen: “Dat vind ik wel een lastige vraag. Toezichthouders moeten vanuit wettelijke kaders hun taken uitoefenen en toezien of de wet wordt gerespecteerd en als dat niet zo is daarop handhaven. Tegelijkertijd evalueren we natuurlijk ook wetten en kijken we ook naar ontwikkelingen. We zijn niet toondoof voor dingen die je net schetst rond de markt die is overspoeld door zonnepanelen. Daar is vanuit verschillende toezichthoudende rollen naar te kijken. De Autoriteit Consument & Markt kijkt vanuit mededinging, dus de facto naar monopolies die ontstaan; de Rijksinspectie Digitale Infrastructuur kan meekijken vanuit bijvoorbeeld een cybersecurityperspectief. Denk aan digitaal verbonden producten, is dat allemaal wel veilig en volgens de wetten die we op dit moment aan het implementeren zijn? Dat is allemaal *work in progress*. Maar ik zie wel op termijn dat we meer en meer, ook vanuit de wet, handelingsperspectieven zien, om daarop bij te kunnen sturen.”

Taai en saai

“De nieuwe Cyber Resilience Act bijvoorbeeld is cybersecuritywetgeving die je ook kunt zien als productregulering, want die stelt voorwaarden aan producten om in Europa op de markt toegelaten te mogen worden. Dat is in de jaren '70 '80 '90 ook gedaan voor bananen, voor keukentrapjes, voor boormachines, dat moet vertrouwd zijn en dat wil je ook voor digitale producten. Die maatregel wordt nu uitgewerkt. Dat is taai en saai, het is complex want er moeten standaarden voor worden ontwikkeld, dus die implementatie is best hardnekkig. Maar ik geef je op een briefje: een groot deel van de wereld gaat dit overnemen. Het creëert duidelijkheid en veel landen zullen zeggen: als het een Europees keurmerk heeft, dan mag het ook onze markt op.”

Agenda Digitale Open Strategische Autonomie (DOSA)

Uitgangspunten

Meer regie over onze veiligheid en onze maatschappelijke en economische positie;
Een **samenhangende blik** op digitale technologie ('whole-of-stack'-benadering);
Ongewenste strategische **afhankelijkheden mitigeren** en **gericht investeren** in digitale sleuteltechnologieën.
Dat wij onze open maatschappij en economie moeten entameren met **meer (internationale) partnerschappen**; meer partners in plaats van een *single point of failure* helpt ook onze kwetsbaarheid verminderen;
Dat we een krachtig speelveld moeten bevorderen met **innovatie**.

Prioriteiten

1. Netwerktechnologie is een randvoorwaarde voor veilige, betrouwbare en hoogwaardige communicatie en vormt een belangrijk fundament voor het goed functioneren van vitale sectoren en overheden;
2. Cloud maakt het mogelijk om op een efficiënte manier gegevens op te slaan, te verwerken en daarmee te benutten voor allerlei doeleinden;
3. Artificiële Intelligentie verandert als systeemtechnologie onze wereld fundamenteel;
4. Het realiseren en onderhouden van hoogwaardige cybersecurity is cruciaal voor onze veiligheid en het functioneren van onze digitale economie;
5. Halfgeleiders staan aan de basis van het digitale domein. In het bijzonder heeft de technologische leiderschapspositie van Nederland een groot positief effect op de Nederlandse economie. Het draagt fors bij aan het verdienvermogen en creëert hoogwaardige technische werkgelegenheid.
6. Quantumtechnologie raakt aan grote publieke belangen. Quantumcomputers zullen in staat zijn een groot deel van de huidige cryptografische protocollen te kraken, waarmee het raakt aan de vertrouwelijkheid, beschikbaarheid en integriteit van onze communicatie en gevoelige data.
7. Het versterken van het concurrentievermogen is essentieel voor de Europese welvaart en verdienvermogen. Een groot deel van de digitale technologie komt uit bedrijven van buiten de EU. Van de twintig meest waardevolle digitale technologiebedrijven zijn er slechts twee (!!) Europees.

Digitaliseren wat we kunnen digitaliseren

De opdracht voor Rijkswaterstaat is zorgen dat Nederland veilig, leefbaar en bereikbaar blijft. 'Doelgericht digitaliseren' is daarbij het credo. Digitaliseren moet helpen om grote onderhoudswerken en nieuwe projecten te kunnen realiseren. "We hebben veel meer werk voor de deur liggen dan we fysiek aankunnen", zegt Ron Kolkman. "Eén van de oplossingen die we hebben bedacht is: digitaliseren wat er te digitaliseren valt."

Want de interne opgave is zonneklaar: met hetzelfde aantal medewerkers 25 procent meer output genereren. "Dus we gaan digitalisering vooral inzetten om de efficiency van onze mensen te vergroten", legt Kolkman uit. "We gaan echt vol inzetten op digitalisering die ons moet helpen om een aantal grote ingrepen te doen. Veel objecten zijn in de jaren '50 en '60 gebouwd. Met een technische levensduur van 80 jaar zijn deze nu toe aan vervanging en grondige vernieuwing. Dus dat is een grote zorg voor Rijkswaterstaat en ook voor Nederland, want het verkeer ondervindt steeds vaker hinder. Met instandhouding zorgen we dat ze veilig en betrouw-

baar blijven, zodat Nederland kan blijven bewegen." "Digitalisering helpt ons daarbij enorm. Dankzij data, sensoren en digitale tweelingen weten we precies wanneer onderhoud nodig is. Dat maakt ons werk slimmer, duurzamer en efficiënter: minder storingen, minder hinder en beter gebruik van mensen en middelen."

Visiedocument

In het visiedocument 'Doelgericht digitaliseren' is sprake van nieuwe technologie als 'Digital Twins' en AI, die ook mede reden zijn om naar een private cloud te gaan. "We

zijn momenteel bezig met soevereine AI-toepassingen, dat is minstens net zo belangrijk als soevereine cloud, maar het hoort ook technisch bij elkaar. Wat wij belangrijk vinden, is dat we AI kunnen toepassen die ondersteunend is aan de medewerker."

Ook data gedreven assetmanagement speelt daarbij een belangrijke rol. "Simpel gezegd: we hangen een object vol met sensoren waaruit data komen rollen. Zo kun je vanaf je bureau een object goed beoordelen. Hoe kun je de mate van slijtage interpreteren? Hoe kun je de technische levensduur bepalen? Hoe kun je met scenario's werken? Dat is niet alleen heel relevant voor het werk dat we doen, maar het maakt 't ook erg leuk."

"We hebben hier een areaal met kunstwerken: tunnels, bruggen, sluisen. Daarin zitten veel PLC-systemen (*programmable logic controller* - red.), we hebben er laatst eentje vervangen, uit 1978. Die OT gaan we samenbrengen met IT."

“
De wereld van
IT verandert
heel snel nu
”

"Het is een open deur, maar ik loop al een tijdje rond in de wondere wereld van IT en het verandert wel heel snel nu. Het perspectief is totaal veranderd: vroeger hadden we het over werkplekken, nu gaat het over soevereiniteit en over kwetsbaarheid. Dat is echt een andere wereld en ik heb daarop zelf ook moeten schakelen in de zin van: wat betekent dit voor ons? Als ik dat kort samenvat dan is het punt: hebben we die continuïteit nu echt gegarandeerd? Daar spelen twee dingen naar mijn idee. Ten eerste de geopolitieke verhoudingen en alle commotie rond de Big Tech-bedrijven. Daar zijn we wel wakker door geschud, dat heeft ons aan het denken gezet. En het tweede is, dat we ook gewoon in onze dienstverlening altijd alert moeten zijn op mogelijke kwetsbaarheden zowel bij Rijkswaterstaat maar ook Rijksbreed. Zaken die vandaag prima werken, kunnen morgen een kwetsbaarheid zijn en daar moeten we snel op kunnen inspelen."

Continuïteit

Dit is ook van invloed geweest op de bestaande sourcing strategie, zegt Kolkman, vanuit zijn betrokkenheid in het CIO-Beraad bij het programma sourcing strategie van het Rijk. "De sourcing strategie loopt al een tijdje, en die moesten we herijken, maar toen kwam dit allemaal langs en beseften we dat het toch echt wel ergens anders om gaat. Feitelijk niet zo ingewikkeld, want om die continuïteit te waarborgen heb ik een goede exitstrategie nodig in de sourcingcontracten. Want we kunnen het met leverancier X wel goed geregeld hebben bij RWS, maar als die leverancier bij de hele overheid aan het werk is, dan heb

Ron Kolkman is sinds 15 februari 2022 hoofdingenieur-directeur (HID) van het landelijke organisatieonderdeel Centrale Informatievoorziening (CIV) en CIO van Rijkswaterstaat (RWS). Hij was eerder directeur van het JIVC van Defensie, directeur ICTRO en later directeur Spir-it (het huidige IVO Rechtspraak) en CIO van het Kadaster. Kolkman maakt deel uit van het programma sourcing strategie Rijk, is deelnemer aan het CIO-beraad én lid van de Nederlandse Digitaliseringsstrategie-raad.

je een heel andere context. Dus als CIO-Beraad kijk je dan hoe je dat landelijk kunt organiseren. De vraag die dan speelt is: gaan we het allemaal centraal regelen, hebben we het dan in een keer overheidsbreed voor elkaar? Daar geloof ik persoonlijk niet in. We moeten het volgens mij zo regelen dat de uitvoerder voldoende kracht krijgt om in de uitvoering te komen en dat we landelijk met elkaar het bestuurlijk comfort goed geregeld hebben. Ergo: dat je je uitwijk voor elkaar hebt, dat je een exitstrategie hebt met leveranciers en dat je een *competence center* hebt voor IT-sourcing waar je centraal advies kunt krijgen. Dan doen we het goed met betrekking tot continuïteit.” Overigens is Kolkman’s enthousiasme over en participatie in de Nederlandse Digitaliseringsstrategie (NDS) ook gebaseerd op het principe ‘de kracht van de uitvoering gebruiken en niet *top down* aansturen’. “We hebben vaak genoeg ervaren dat dit niet werkt, de overheid is te

groot om dat allemaal te doen. Dus ja, ik vind de aanpak van de NDS charmant.”

Bedrijfscontinuïteit – en de daarmee samenhangende dienstverlening – staat ook onder druk van toenemende cyberdreiging. Er wordt in dat verband wel gesproken over het uitvallen van elektriciteitscentrales, maar als we kijken naar RWS: bruggen, sluizen, dijken... We hebben hoog water, we hebben storm en de Russen hacken de Deltawerken. Hoe pak je dat aan?

“We zijn ons zeer bewust van het feit dat er iets kan gebeuren. Ik heb hier ook echt wel het gevoel bij: het is niet óf je wordt gehackt maar wanneer. Dat is the *worst nightmare* die je kan hebben als CIO. Maar we hebben het nog niet meegemaakt, gelukkig. Iedereen in Nederland kan rustig blijven slapen.” Overigens is het bij wet geregeld dat RWS op bijvoorbeeld

de keringen en bruggen de faalkansen zoveel mogelijk dient te beperken in het licht van miljarden aan maatschappelijke schade. “We doen er echt alles aan om die continuïteit te garanderen en uiteindelijk kunnen we dingen met de hand bewegen. Want je moet een laatste fall back scenario hebben om te zorgen dat Nederland droge voeten houdt, of veilig en bereikbaar blijft. We zijn vanuit ons eigen Security Operations Center (SOC) elke dag bezig met cyberbeveiliging. Niettemin blijft er kans op verstoringen door cyberaanvallen zonder dat Rijkswaterstaat dit zelf in de hand heeft’. Dat hoort ook bij deze tijd, cyberschaamte heet dat meen ik, dat je dit niet durft te vertellen, maar het is wel de realiteit van vandaag. Zo’n wereldwijde Sharepoint kwetsbaarheid heeft ons ook weer extra alert gemaakt.” Kolkman zegt dat er ook regelmatig crisismanagement-oefeningen worden gehouden om te anticiperen op mogelijke uitval van IT door bijvoorbeeld DDoS-aanvallen.

Nederland veilig, leefbaar, weerbaar en bereikbaar te houden, die bevindt zich in een andere laag.”

Spannend aan de NDS vindt Kolkman nog wel hoe de besluitvorming zal gaan, en de regievoering, met Rijksoverheid, provincies, gemeenten en waterschappen aan tafel. Het besef is wel alom dat dit iets is om samen in op te trekken, de noodzaak en urgentie wordt overheidsbreed gevoeld. Al, het moet gezegd, is hier en daar, overheid eigen, ook nog sprake van het *not invented here* syndroom. Kolkman glimlacht: “We gaan mensen verleiden om in te stappen, we gaan met *best practices* werken, we gaan een marktplaats maken. Er komt geen dwang als in ‘je mot over twee jaar’ in de overheidscloud zitten.”

Zonder negatief te willen zijn is de ervaring dat het tussen intentie en implementatie nog weleens spaak loopt...

Overheidscloud

Rijkswaterstaat investeert fors in z’n soevereiniteit en dat verklaart ook dat Kolkman lid is van de NDS-raad. De aan hem toegewezen prioriteit is cloud. Hij spreekt in dit verband van de overheidscloud, “omdat het de gehele overheid betreft: Rijksoverheid, provincies, gemeenten en waterschappen. Het is echt *huge*, ik heb dat nog niet eerder zo meegemaakt.” Zijn beeld van de overheidscloud is “dat die straks uit een aantal lagen bestaat, waarin ook de laag *hyperscaler* voorkomt. Ik denk niet dat we als Rijkswaterstaat van de Big Tech-partijen zoals de Microsofts van deze wereld af willen als we er niet al te spannend over doen. Ze zijn er en als ze er nu mee stoppen, dan hebben we met z’n allen ook een probleem. Denk aan de gemiddelde werkplek: die is een en al Microsoft. Maar die soevereiniteit op de data die er echt toe doen, de kroonjuwelen zoals die wel worden genoemd, in het geval van RWS dus de evidente data die we nodig hebben om

“Ja, eens. Maar waarom denk ik dat dit wel lukt? Dat is natuurlijk vooral omdat de urgentie heel hoog is. En ik denk dat als we echt een mooie overheidscloud hebben, waardoor we ook meer onafhankelijkheid hebben, waar je gewoon gebruik van kunt maken, en kunt opschalen en afschalen, dat iedereen daar beter van wordt. Dan kun je maximaal inzetten op continuïteitswaarborging.”

En wanneer is-ie er dan, die overheidscloud?

“Als je nu zegt we gaan een nieuwe cloudstrategie maken, dan moet je er rekening mee houden dat je over vijf jaar verplicht naar de overheidscloud gaat. Dat lijkt me een mooie ambitie. En dan hoop ik wel dat we binnen nu en twee jaar met elkaar wat laten zien, die energie moeten we wel zien vast te houden met elkaar.”

Next level

Kolkman wijst op de rol van de overheidsdatacenters (ODC’s) en neemt de consolidatie van ooit 64 naar thans 4 overheidsdatacenters als voorbeeld. “Die ODC’s zijn goed bezig met onder meer ‘OpenShift’. Ze hebben allemaal dezelfde technologie gekozen, waarbij je feitelijk al kunt doorgroeien naar een natuurlijke Rijkscloud. We beginnen dus niet met een blanco sheet. We moeten gaan inventariseren welke bewegingen er zijn, we moeten kijken hoe je dingen aanbestedingstechnisch zou kunnen doen. Dus ja, we hebben nog wat hobbels te nemen. Maar de aanpak is niet: huppakee, we gaan iets bouwen en over vier jaar is het klaar. Ook hier kijken we naar *best practices* en dan zou het best zo kunnen zijn dat we de komende twee jaar die vier, vijf ODC’s langzaam naar elkaar toe migreren. Ik weet zeker dat het geen *big bang* scenario zal worden, maar wel een heel logische stap naar de next level en dat is dan de overheidscloud.”

“
Soevereiniteit op data
gaat over evidente data
die we nodig hebben
om Nederland veilig,
leefbaar en bereikbaar
te houden
”

DATA

als basis voor inspirerend verkeersmanagement

CASE

Nederland staat voor grote mobiliteitsuitdagingen: files nemen toe, doorgaande verkeersstromen staan onder druk, en de samenleving verlangt tegelijk naar bereikbaarheid én duurzaamheid. Waar doorgaans naar asfalt wordt gegrepen, kijkt een studententeam van Maastricht University juist naar data als nieuw fundament voor slim verkeersmanagement.

In deze verkenning van de Maastricht University onderzochten studenten, begeleid door experts vanuit Rijkswaterstaat en Atos, inspirerende toekomstscenario's voor gepersonaliseerd verkeersmanagement. Geen strategie of blauwdruk van Rijkswaterstaat, maar een gedachte-experiment: hoe zou het 'reisadvies van de toekomst' eruit kunnen zien? Centraal staat het idee dat elke weggebruiker op basis van zijn persoonlijke reispatroon intelligente route-informatie ontvangt, mogelijk gemaakt door een 'route learning'-systeem en spelelementen.

Gepersonaliseerde reisadviezen

Het gepresenteerde scenario draait om het optimaliseren van bestaande verkeersinformatie, waarbij gebruikers geholpen worden slimme keuzes te maken om files en vertragingen te voorkomen. Het systeem leert van de dagelijkse routes van de gebruiker en biedt onderweg persoonlijke reisadviezen, vooral wanneer wegwerkzaamheden of incidenten impact kunnen hebben.

Een belangrijk element is de inzet van gamification: gebruikers worden uitgedaagd en beloond voor gewenst reisgedrag, zoals reizen buiten de spits of kiezen voor het openbaar vervoer. Denk aan (bonus)punten, badges of voordelen bij mobiliteitspartners. Zo wordt het veranderen van reisgedrag laagdrempelig, nuttig én ook leuk gemaakt.



Voor het verzamelen van mobiliteitsdata wordt in het scenario uitgegaan van dezelfde techniek als in het bekende Spitsmijden-project. Hierbij registreert slimme technologie – uiteraard alleen met expliciete toestemming van de gebruiker – anoniem het reispatroon, zonder privacygevoelige gegevens centraal op te slaan. GPS en connectiviteit van voertuigen spelen een rol, aangevuld met data uit vrijwillig gedeelde apps zoals Google Maps.

De autonomie van de weggebruiker is essentieel. Deelname aan het systeem is altijd vrijwillig, en de gebruiker blijft volledig eigenaar van zijn of haar data. Het concept respecteert alle uitgangspunten uit de AVG en is ontworpen vanuit het principe 'privacy by design'.

Inspiratie voor de sector

Met deze scenarioverkenning beoogt het studententeam discussies binnen de sector te stimuleren: kun je met gepersonaliseerde, speelse benaderingen duurzame gedragsverandering bereiken? En wat vraagt dit qua samenwerking, techniek en maatschappelijke acceptatie? De geschetste casus is nadrukkelijk niet bedoeld als voorgestelde beleidsrichting, maar als inspiratiebron voor innovatie.

Deze studie is uitgevoerd binnen het Premium-programma van Maastricht University. Mocht u interesse hebben in het gedachte-experiment, of in een bredere dialoog over de toekomst van verkeersmanagement, neem dan gerust contact op met de projectbegeleiders:

Joris van der Horst van Rijkswaterstaat,
joris.vander.horst@rws.nl
Wilbert van der Kruk van Atos,
wilbert.vanderkruk@atos.net



DISCLAIMER

GOV is een magazine dat informeert over ontwikkelingen op het gebied van de digitale overheid. GOV verschijnt in controlled circulation onder beslissers en beïnvloeders binnen de (de)centrale overheid, SUWI en het zorgdomein. Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht. Wilt u een gratis gedrukt of uitsluitend digitaal abonnement op GOV magazine of wenst u GOV magazine niet meer van ons te ontvangen, dan kunt u dit aangeven via willem.beelen@atos.net

Atos

**Your Data.
Your Rules.
Your Move.**

**Are you
ready?**

**Scan the QR code to download the full guide:
6 questions every IT leader must ask.**

