



Digitalisering in 2031: wendbaarheid of Achilleshiel?

Wat zien we?

Het essay en podcast *Europa 2031*¹ schetsen een toekomst waarin de geopolitiek rond generatieve AI (GenAI) Europa fataal wordt. Het scenario analyseert de afgelopen paar jaar en gaat halverwege 2026 over in fictie: de LLM-bubbel knapt niet en de technologie werkt. Wel mist Europa de boot: het EuroStack-initiatief² komt "Europees traag" van de grond en is "too little, too late". Europese gebruikers die inzetten op "Europees soevereine" (maar schromelijk achterlopende) technologie worden massaal gehackt en leeggezogen door ransomware. Europese gebruikers die toch in zee gingen met de internationale big tech worden afgesloten – en daarna massaal gehackt – wanneer rekenvermogen wereldwijd een knelpunt wordt (en door gebrekkige investering heeft Europa zelf te weinig datacenters). In 2030 is Europa afgegleden naar massawerkeloosheid, schulden, een ontbonden Euro, rellen en vooral: geen toegang meer tot digitale diensten. In 2031 worden Europa's laatste digitale mogelijkheden genadeloos weggevaagd wanneer zowel China als de U.S.A. met "nucleaire dringendheid" Europa's laatste relevante bedrijf (ASML) voor zichzelf op komen eisen...

Wat zit hierachter?

Het scenario is een synthese van drie trends die de auteurs herhaaldelijk benadrukken: de verdeeldheid en traagheid van Europese besluitvorming; een moeilijk voor te stellen snelheid waarmee GenAI groeit in transformatief vermogen; en de recent hernieuwde nadruk op een geopolitiek van competitie en pressiemiddelen. Het resultaat van de interactie tussen deze componenten is een geopolitisch kantelpunt³ (de omwenteling heeft een beangstigend korte doorlooptijd) dat lijkt te leiden tot de ineenstorting⁴ van de Europa's welvaart, relevantie en autonomie.

De auteurs – een GenAI-positieve denktank uit Brussel – roepen Europa op om doortastender⁵ voor big tech te kiezen. Uit het handelingsperspectief dat ze schetsen blijkt een sterk neoliberaal, americentrisch perspectief: generatieve AI leidt tot groei en groei staat centraal; Europa's heil ligt in het bouwen van infrastructuur voor Amerikaanse big tech; Europese sociale, ecologische en regulerende waarden worden meermaals als decadent en onhoudbaar neergezet; met China valt niet te praten. Dit scenario is niet neutraal, maar het bevat wel lessen.

Waarom is dit interessant?

Mocht Europa de adviezen van de auteurs opvolgen, dan zouden investeringen in big tech en datacenters in een stroomversnelling komen, ten koste van mens en milieu. Het zou de beschikbaarheid en verdeling van zoetwater, ruimte, energie, grondstoffen en menskracht verder onder druk zetten: knelpunten die de waterschappen en drinkwaterbedrijven nu al veel zorgen baren.

Waarom is dit echt interessant?

Interessanter is de vraag: wat als het doembeeld van de auteurs wel werkelijkheid wordt en digitale technologie in Europa nagenoeg onbruikbaar wordt? De watersector heeft de afgelopen 30 jaar een eerste digitale laag van procesautomatisering en communicatie opgezet en is juist begonnen met het aanbrengen van een tweede laag van aansturing op afstand en automatische beslissingen op basis van data en modellen. Belangrijke motivaties voor verdere digitalisering zijn kennisbehoud, efficiëntie, serviceniveau en systeeminzicht. We verwachten dat we met digitalisering de veerkracht en wendbaarheid van de sector kunnen vergroten. In dit scenario zet digitalisering de deur echter wagenwijd open voor kwaadwillenden.



Drinkwaterbedrijven en waterschappen houden in hun verstoringsrisicoanalyses natuurlijk al lang in het achterhoofd dat het wijs is om terug te kunnen blijven vallen op een “handmatig gestuurde” watervoorziening. Ook is er aandacht voor cybersecurity⁶ en het landschap van externe afhankelijkheden en bedreigingen⁷. Dit scenario kaart aan dat het desondanks voorstelbaar is dat pogingen om digitale veiligheid en autonomie te behouden⁸ plotsklaps tenietgedaan kunnen worden. In het bijzonder kan de schaal hiervan problematisch zijn. Ondersteund door GenAI hebben hackers potentieel voldoende reikwijdte om niet één, maar alle afsluiters in digitale watermeters over te nemen (of alle zuiveringslocaties). De enkelingen die nu weten hoe handmatige besturing in elkaar zit, zijn dan met te weinig om dat op te vangen; zeker als het lesmateriaal of protocol om anderen in te leren alleen in de cloud stond.

Strategische vragen voor de watersector

De snelheid van dit scenario gaat het tempo waarmee waterinfrastructuur wordt aangepast en onderhouden sterk te boven. Over vijf jaar is hooguit 5% van het leidingnet aangepast, zijn er misschien een paar nieuwe bronnen ontwikkeld, zijn de digitale watermeters nog lang niet uitgerold en is er nog heel veel ontwikkelruimte voor digitale tweelingen. De tijd en moeite die we besteden aan het aanpassen van onze systemen en processen zijn beperkt. Dit roept de volgende vragen op:

- Het geschetste scenario is extreem. Het is verleidelijk om te stellen “dat de huidige cyberveiligheid goed genoeg doordacht is” of “dat het zo’n vaart niet zal lopen met AI”, maar het scenario is voorstelbaar, de impact is hoog, en de waarschijnlijkheid is onmogelijk te voorspellen. Verdient het scenario actie of kunnen we het expliciet naast ons neerleggen?
- Hoe kunnen signalen in de richting van dit scenario worden herkend en geïnterpreteerd?
- Als vandaag alle digitale technologie voor onbepaalde tijd wegvalt (van informatiesysteem tot mobiele telefoon, van procesautomatisering tot de systemen van externe leveranciers), wat moet er dan geregeld zijn en klaar staan om de watervoorziening doorgang te kunnen laten vinden? Is het al geregeld?
- Kunnen we het mogelijk maken om onze systemen *grootschalig, snel en eenvoudig* los te koppelen van alle digitale besturing? Hoe kan de sector weerbaar worden gemaakt tegen digitale afhankelijkheid en chantage?
- Welke problemen kunnen worden veroorzaakt wanneer alle digitale verbindingen (portals, sensoren, digitale meters, automatische afsluiters, regelsystemen, procesaansturing) worden overgenomen door kwaadwillenden? Welke verbindingen hadden we dan eigenlijk

- liever niet aangelegd? Welke zijn we op dit moment aan het aanleggen? Wat zijn betrouwbare alternatieven?
- Is dit scenario dusdanig ontwrichtend dat het het handelingsperspectief van waterschappen en drinkwaterbedrijven te boven gaat? Welke verantwoordelijkheid willen en kunnen zij in dit scenario nemen voor waterveiligheid en sanitatie en op welke vlakken zijn ze aangewezen op de overheid?
 - Hoe kan de watersector blijven functioneren (van toeleveringsketens tot financiële houdbaarheid) onder de in het scenario geschetste economische omstandigheden? Als de sector slechts op beperkte kracht kan blijven functioneren, hoe wordt dan de triage?

Duiding

	Laag	Middel	Hoog
Impact			
Zekerheid	Diep onzeker		

Actie ondernemen:

Dat digitale technologie beveiligingsrisico’s kent is niks nieuws en dat “de ontwikkelingen snel gaan” is abstract wel bekend. Dat alle digitale technologie binnen vijf jaar simultaan en voor onbepaalde tijd weggevaagd zou kunnen worden, waarbij externe actoren doelbewust uit zijn op ontwrichting, vraagt om een oprechte evaluatie van de noodzaak tot het tijdig inbouwen van meer analoge uitvalsroutes.



Meer lezen

- Jujin, D.; van Baarsen, S.; Dada, J.; Negele, M.; Stelling, L.; Fox, P.; Petropoulos, A.; Bakker, M.; en Chivers, T. (2026, 11 juni). *Europe 31 – What getting AI wrong means for us*. <https://europe2031.ai>
- Eurostack (2026, 6 augustus). *Building a European alternative for technological sovereignty*. <https://www.euro-stack.info>
- KWR (2021, 20 november). *Trend alert – Klimaatscenario's, -kantelpunten en -extremen*. BTO 2023.083, KWR. <https://kwrwater.sharepoint.com/:b:/r/sites/Waterwijs/Shared%20Documents/Rapporten/BTO%202023.083%20Trendalert%20Klimaatscenario's,%20kantelpunten%20en%20extremen.pdf?d=w848d92140f9a400db2d174becc600c34&csf=1&web=1&e=AQkNOF>
- KWR (2021, 16 december). *Trend alert – Collapsologie en diepe adaptatie*. BTO 2021.071, KWR. <https://kwrwater.sharepoint.com/:b:/r/sites/Waterwijs/Shared%20Documents/Rapporten/BTO%202021.071%20Trendalert%20Collapsologie%20en%20diepe%20adaptatie.pdf?d=w214311ddc0c64e93904858204673084f&csf=1&web=1&e=GQH8wh>
- KWR (2026, 18 mei). *Trend alert – bestuurlijke moed*. KWR 2026.023, KWR. <https://kwrwater.sharepoint.com/:b:/r/sites/Waterwijs/Shared%20Documents/Rapporten/KWRW%202026.023%20Trendalert%20-%20Bestuurlijke%20moed.pdf?d=w23a8948a37cf4c59859cf65f87edaf96&csf=1&web=1&e=6HsP7O>
- KWR (2026, 24 april). *Trend alert – ICT aan de macht*. KWR 2026.018, KWR. <https://kwrwater.sharepoint.com/:b:/r/sites/Waterwijs/Shared%20Documents/Rapporten/KWRW%202026.018%20Trendalert%20-%20ICT%20aan%20de%20macht.pdf?d=w9fecbf57779146c69d11c4c20fda5b11&csf=1&web=1&e=3M8IUc>
- Vewin. (2026, 5 augustus). *Weerbaarheid van drinkwaterbedrijven*. Vewin. <https://www.vewin.nl/thema/weerbaarheid-van-drinkwaterbedrijven-a/>
- Nationaal coördinator terrorismebestrijding en veiligheid. (2025, 24 juli). *Dreigingslandschap vitale infrastructuur*. Ministerie van Justitie en Veiligheid. <https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur>

Groningenhaven 7 / PO Box 1072 3430 BB Nieuwegein The Netherlands
Contactpersoon: Karel van Laarhoven Karel.van.laarhoven@kwrwater.nl
+31 (0)30 60 69 697
www.kwrwater.nl
www.dws.nl
© KWR Water Research Institute