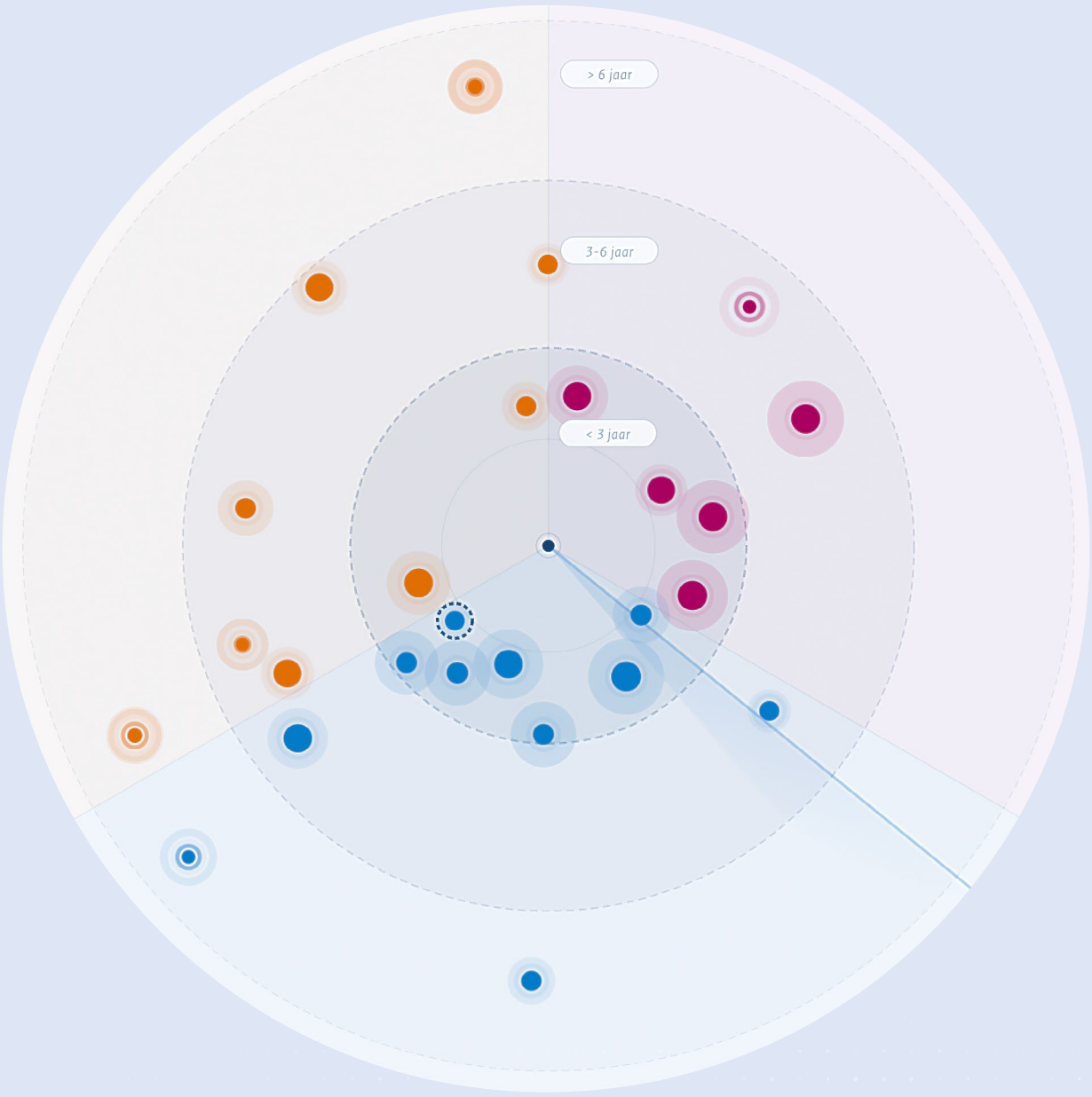
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat



Trendradar 2026

Rijksinspectie Digitale Infrastructuur
Voor een **veilig verbonden** Nederland

Inhoud

De digitale infrastructuur van morgen, vandaag op de radar 3

Technologische ontwikkelingen 4

Meer vraag naar frequentiespectrum vergroot schaarste en kwetsbaarheid 5
Agentic AI neemt de teugels uit handen 6
Driedimensionalisering netwerken 7
Quantumtechnologie stelt nieuwe eisen aan digitale weerbaarheid 8
Opkomst van sensing-technologie 9
AI neemt fysieke vorm aan 10
AI versnelt wetenschapsbeoefening 11
Fotonische chips 12
Dataopslag in DNA veelbelovend, voorlopig buiten bereik 13

Geopolitieke ontwikkelingen 14

Digitale infrastructuur als geopolitiek machtsinstrument 15
Cyberaanvallen worden onzichtbaarder en indirecter 16
Toenemende inzet AI voor cyberaanvallen en -verdediging 17
Digitale autonomie hoog op politieke agenda 18
Groeiende focus op strategische autonomie van grondstoffen en halffabricaten 19
Buitenlandse inmenging verzwakt verdienvermogen Nederland 20

Maatschappelijke ontwikkelingen 21

Wetgeving in spagaat tussen risicobeheersing en digitale innovatie 22
Alle aspecten van ons leven doordrongen van digitale infrastructuur 23
Synthetische identiteiten verhogen druk op digitale vertrouwensstelsels 24
Toenemend beslag op energie en water 25
Instroom niet-conforme apparatuur vergroot veiligheidsrisico's 26
Digitale weerbaarheidskloof tussen mkb en grootbedrijf 27
De vicieuze cirkel van AI en desinformatie 28
Beschikbaarheid digitale infrastructuur onder druk 29
Tekort professionals zet beschikbaarheid en innovatie onder druk 30
Extremer weer vergroot kwetsbaarheid digitale infrastructuur 31
Nieuwe mens-machine interfaces 32

Tot slot 33

Bronnen 34

De digitale infrastructuur van morgen, vandaag op de radar

Een beschikbare, betrouwbare en continu werkende digitale infrastructuur is onmisbaar voor het functioneren van onze samenleving. Dat is een vaststaand gegeven, maar de digitale infrastructuur zelf is dat allerminst. Technologische doorbraken, maatschappelijke verschuivingen en geopolitieke spanningen zorgen voor voortdurende veranderingen en maken de infrastructuur complexer en kwetsbaarder.

Met de Trendradar signaleert en duidt de Rijksinspectie Digitale Infrastructuur (RDI) welke ontwikkelingen de komende tien jaar onze digitale infrastructuur zullen raken. Voor de RDI is de radar een hulpmiddel om ons toezicht te prioriteren, tijdig te anticiperen en waar nodig maatregelen te nemen. Daarnaast ondersteunt dit rapport beleidsmakers, bedrijven en andere professionals in de digitale infrastructuur om risico's te beheersen en kansen te benutten.

Onze collega's kwamen samen met 30 experts uit bedrijfsleven, kennisinstellingen en overheden tot de 26 belangrijkste trends. Van doorbraken in quantumtechnologie en AI tot de groeiende druk op de energievoorziening en de gevolgen van extreem weer. De trends laten zien hoe breed het palet aan maatschappelijke uitdagingen is waar we als RDI en als samenleving voor staan.
De trends zijn verdeeld over drie thema's: technologie, geopolitiek en maatschappij. Elke trend op de radar heeft een score (hoog, midden en laag) waarmee de verwachte impact op de digitale infrastructuur wordt aangegeven. Ook staat de termijn genoemd waarop de trend naar verwachting op het hoogtepunt is.

We nodigen u uit om de trends te verkennen en met ons mee te denken over wat ze betekenen voor de digitale infrastructuur van morgen. Want zien welke ontwikkelingen op ons afkomen is één ding, de vertaling naar beleid, investeringen en samenwerking is aan ons allemaal.

Wat betekenen de impactscores?

hoog Groot effect op de (vaak gehele) digitale infrastructuur. Een groot deel van de samenleving ervaart de gevolgen.

middel Middelgroot effect op (onderdelen van) de digitale infrastructuur. Een middelgroot deel van de samenleving ervaart de gevolgen.

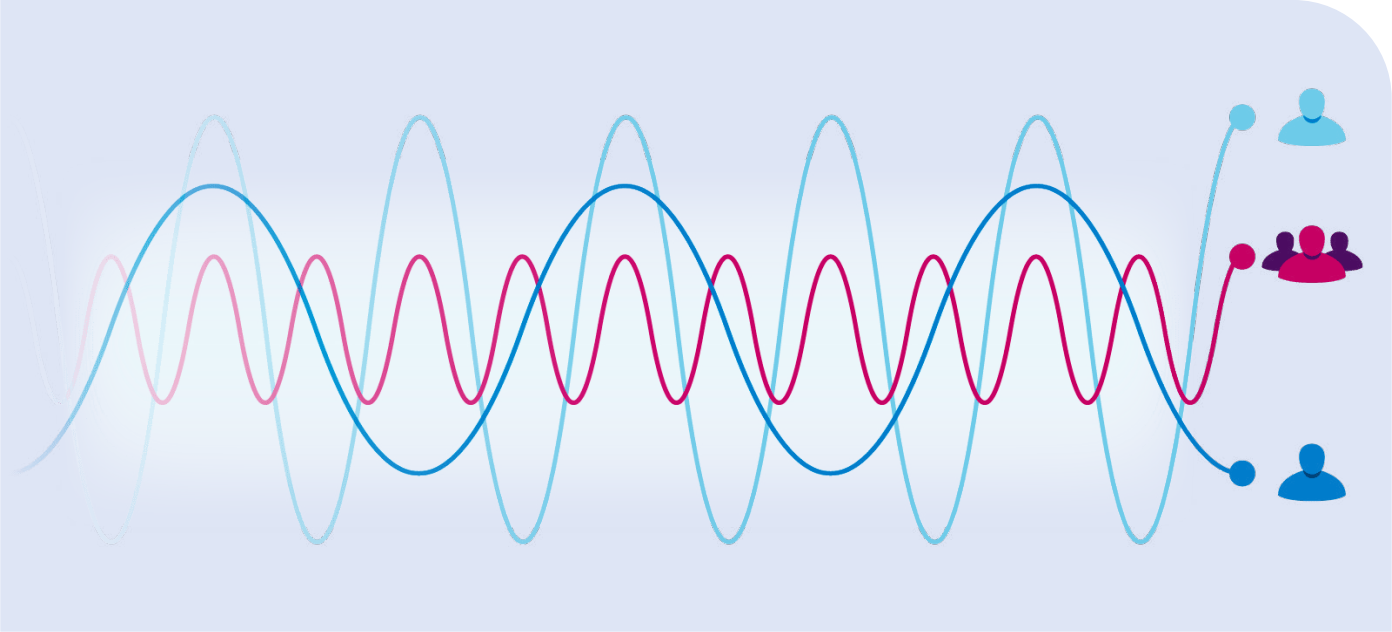
laag Beperkt effect op (kleine onderdelen van) de digitale infrastructuur. Een klein deel van de samenleving ervaart de gevolgen.

Technologische ontwikkelingen

Technologische doorbraken volgen elkaar snel op en hebben een grote en directe impact op de digitale infrastructuur en de sectoren die daarvan afhankelijk zijn. Ze brengen nieuwe mogelijkheden, maar ook risico's met zich mee. Ontwikkelingen die op de radar verschijnen zijn bijvoorbeeld sleuteltechnologieën als (vormen van) AI en quantumtechnologie, maar ook veranderingen in satelliettechnologie hebben een grote impact op de digitale infrastructuur.

Meer vraag naar frequentiespectrum vergroot schaarste en kwetsbaarheid

Impact **hoog** Termijn **<3 jaar**



De toenemende vraag naar radiospectrum zorgt in specifieke frequentiebanden voor schaarste. Deze ontwikkeling speelt bijvoorbeeld door de snelgroeiende vraag naar meer spectrum in hogere banden (Q/V/E en hoger) voor satelliettoepassingen.

Gezamenlijk gebruik van frequentieruimte ('spectrum sharing') vermindert de schaarste. De interesse hierin neemt gestaag toe. Technologische ontwikkelingen om spectrum sharing op grotere schaal te realiseren, zijn in volle gang. Bijvoorbeeld in de vorm van 'cognitive radio'. Bij die technologie kunnen apparaten in toenemende mate zelf, onderling én met het netwerk afstemmen welke frequentie ze gebruiken en met welk vermogen.

Impact

De toenemende druk op het frequentiespectrum kan leiden tot storingen in vergunningsvrije banden, waarin het gebruik van toepassingen als satellietcommunicatie, WiFi, Bluetooth en 'Longe Range' (LoRa)-apparaten intensiever wordt. Deze storingen vormen met name een risico voor kritieke toepassingen zoals medische apparatuur. Toenemende drukte brengt ook radioastronomie in de knel, omdat de banden die zij uitluisteren steeds vaker in gebruik zijn voor aardse toepassingen.

Het efficiënter benutten van spectrum door ontwikkelingen zoals cognitive radio verhogen de efficiëntie van het spectrumgebruik, maar vereist ook nieuwe regelgeving. Zo gaan vergunningen vaak nog uit van het toewijzen van gebruiksrechten voor een specifiek gedeelte van het spectrum aan een specifieke gebruiker, terwijl cognitive radio tussen meerdere gebruikers over een groter deel van het spectrum moet kunnen afstemmen. Cognitive radio is door de hoge complexiteit ook kwetsbaarder voor uitval.

Daarnaast wordt het frequentiespectrum, net als de bredere digitale infrastructuur, steeds meer een geopolitiek-strategisch terrein. Hybride dreigingen zoals opzettelijke verstoring ('jamming'), misleiding ('spoofing') en de inzet van drones hebben door de drukte in het spectrum nog meer impact. Impact is met name groot bij toepassingen die afhankelijk zijn van betrouwbare radiocommunicatie, zoals GPS/GNSS, noodhulpdiensten (C2000/P2000), de medische sector, defensie en luchtvaart.

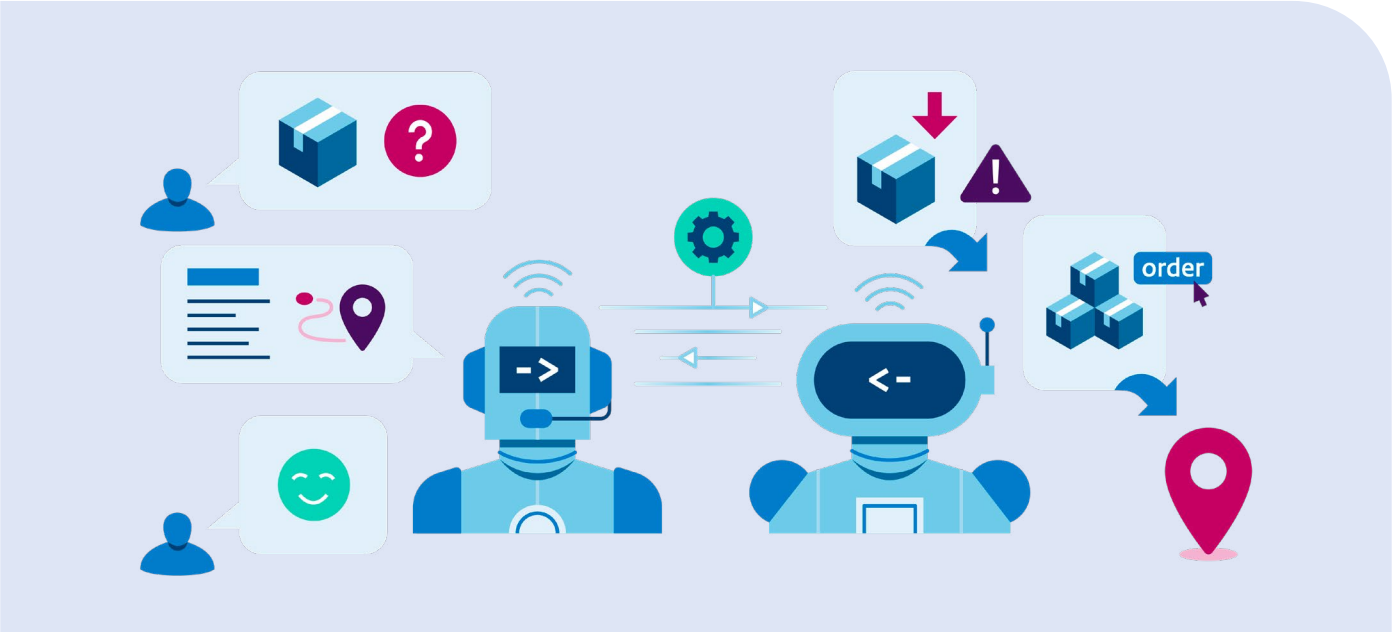
Zie ook

22 Wetgeving in spagaat tussen risicobeheersing en digitale innovatie

29 Beschikbaarheid digitale infrastructuur onder druk

Agentic AI neemt de teugels uit handen

Impact **hoog** Termijn **0-3 jaar**



AI-modellen zijn in staat om in hoog tempo enorme hoeveelheden informatie te verwerken en analyseren, variërend van videobeelden en audiogesprekken tot onderzoeksrapporten en ongestructureerde databronnen. Sinds 2025 worden uiteenlopende AI-systemen steeds vaker aan elkaar gekoppeld en van een doel voorzien dat (grotendeels) zelfstandig bereikt wordt. Dit staat bekend als agentic AI.

De toepassingsmogelijkheden zijn breed. Zo kan een autonome digitale assistent zelfstandig besluiten boodschappen te bestellen op basis van eerdere gesprekken, agenda-informatie en de hoeveelheid eten in de voorraad. Maar agentic AI kan ook worden ingezet voor geavanceerde, autonoom uitgevoerde ransomware-aanvallen, of zelfstandig veiligheidslekken vinden en misbruiken. Door de groeiende hoeveelheid gekoppelde gegevensbronnen – zoals consumenten- en verkeerscamera's, slimme apparaten, administratieve systemen en gezondheidsmonitoring – krijgen agents toegang tot steeds meer ongestructureerde informatie die zij kunnen combineren en benutten voor besluitvorming.

Doordat deze systemen leren van nieuwe gegevens en eerdere resultaten, worden hun analyses, beslissingen en autonoom uitgevoerde acties steeds geavanceerder, nauwkeuriger en doelgerichter.

Impact

Mits voorzien van de juiste autorisaties en authenticaties, kunnen autonome agents zelfstandig transacties uitvoeren, systemen aansturen en beslissingen nemen namens gebruikers. Daarmee verschuift de rol van AI fundamenteel: AI ondersteunt niet langer uitsluitend bij het nemen van beslissingen, maar kan ook zelfstandig regie voeren over digitale én fysieke processen om vooraf gedefinieerde doelen te bereiken.

Zie ook

11 AI versnelt wetenschapsbeoefening

16 Cyberaanvallen worden onzichtbaarder en indirecter

17 Toenemende inzet AI voor cyberaanvallen en -verdediging

Driedimensionalisering netwerken

Impact **hoog** Termijn **3-6 jaar**



Door verbeterde satelliettechnologie worden driedimensionale netwerken mogelijk, die zich niet alleen tweedimensionaal uitstrekken over het oppervlak maar ook verticaal, in hoogte. Allerlei typen satellieten kunnen onderdeel zijn van zo'n netwerk: satellieten in lage banen ('Low Earth Orbit', of LEO), in geostationaire banen, maar ook 'High-Altitude Platform Systems' (HAPS), zoals drones en ballonnen. Satellieten communiceren daarbij steeds vaker direct met apparaten van gebruikers ('Direct-to-Device', D2D), in plaats van dat ze een schakel zijn in de netwerkinfrastructuur.

Impact

3D-netwerken hebben door redundantie in verbindingstypen en dimensionering een hogere beschikbaarheid en betere dekking. Verbeterde beschikbaarheid komt doordat de verbinding bij uitval of gebrekkige dekking automatisch overschakelt naar de techniek die nog wel werkt. Ook is dynamische capaciteitsallocatie mogelijk: bij een (plotselinge) piek, zoals een grootschalig evenement of rampgebied, kunnen HAPS-systemen of satellietbundels extra capaciteit naar specifieke coördinaten sturen.

3D-netwerken zijn ook geschikt voor gebieden met minder dekking, zoals voor autonome landbouwvoertuigen, maritieme logistiek en ecologische monitoring. In Europees Nederland is de impact van deze toepassingen waarschijnlijk beperkt, omdat hier al een goede mobiele dekking beschikbaar is via bestaande netwerken. Op de BES-eilanden is de toegevoegde waarde groter.

Standaardisering en borging van interoperabiliteit in 3D-netwerken zijn belangrijke eerste stappen. Interoperabiliteit zal leiden tot netwerkonafhankelijke verbindingen. Daardoor kunnen klanten een connectiviteitscontract afsluiten zonder te hoeven kiezen tussen kabel, glasvezel, mobiel of satelliet.

3D-netwerken leiden tot nieuwe vragen bij overheden rond regulering. Wetgeving voor de ruimte is complex. Bestaande regelgeving is vaak gericht op afzonderlijke technologieën, terwijl 3D-netwerken verschillende soorten verbindingen combineren. Dat leidt tot nieuwe vraagstukken over verantwoordelijkheden en verplichtingen van netwerkoperators, zoals het oplossen van storingen in 3D-netwerken en aftapverplichtingen. Daarnaast wordt de ruimte door de toegenomen hoeveelheid satellieten steeds voller, met risico op botsingen en ruimtepuin.

Driedimensionalisering kan ertoe leiden dat nieuwe aanbieders toetreden tot de markt. Daarnaast bestaat het risico dat samenvoeging van netwerken leidt tot minder aanbieders en concentratie van macht. Europa onderkent dit risico en investeert in een eigen Europees alternatief voor een satellietconstellatie, in de vorm van IRIS2.

Zie ook

5 Meer vraag naar frequentiespectrum vergroot schaarste en kwetsbaarheid

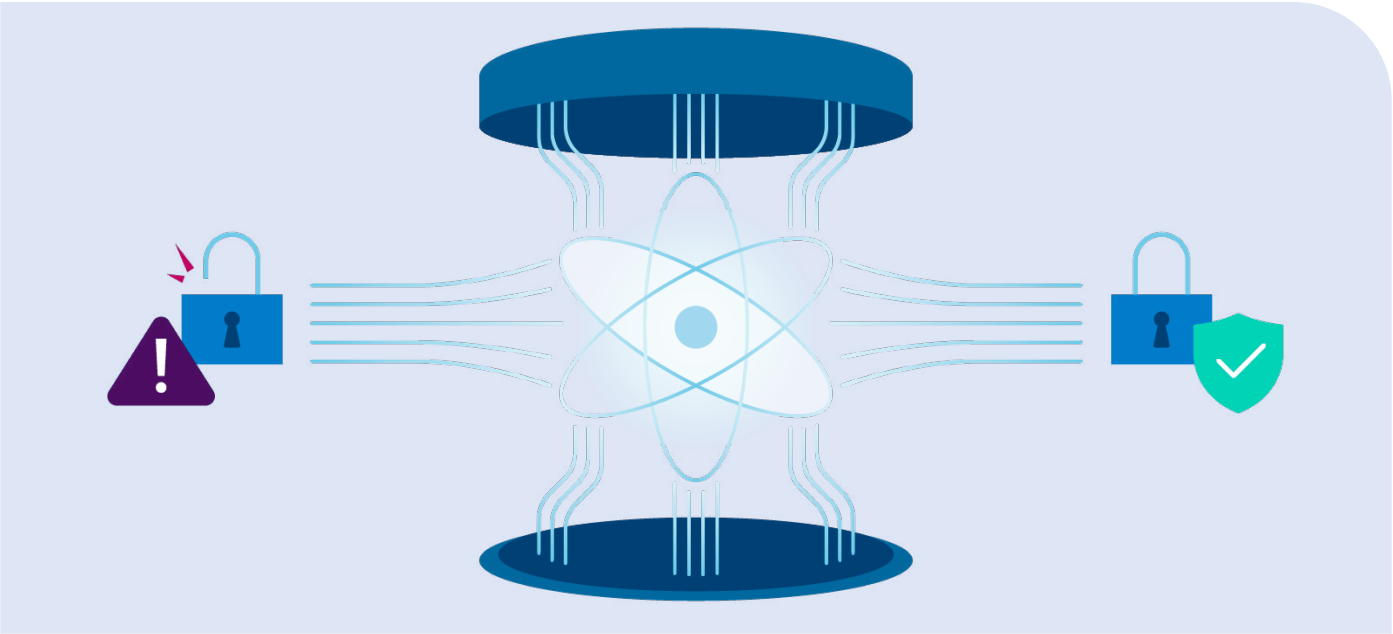
22 Wetgeving in spagaat tussen risicobeheersing en digitale innovatie

23 Alle aspecten van ons leven doordrongen van digitale infrastructuur

29 Beschikbaarheid digitale infrastructuur onder druk

Quantumtechnologie stelt nieuwe eisen aan digitale weerbaarheid

Impact **hoog** Termijn **3-6 jaar**



Quantumcomputers kunnen de beveiliging van digitale systemen fundamenteel veranderen. Er bestaan quantumalgoritmen waarmee een voldoende krachtige quantumcomputer veel huidige vormen van versleuteling kan doorbreken. Daarmee kan het vertrouwelijke informatie leesbaar maken.
Volwaardige quantumcomputers bestaan waarschijnlijk pas over enkele jaren. Toch gaat er nu al een reële dreiging van uit. Statelijke actoren kunnen versleutelde communicatie nu opslaan, in de verwachting dat zij die later alsnog kunnen ontcijferen ('harvest now, decrypt later'). Quantumtechnologie wordt dus gezien als een strategisch wapen.
Er zijn twee oplossingen in ontwikkeling: post-quantum cryptografie (PQC) en quantum key distribution (QKD).
QKD is een techniek om veilig sleutels te genereren en uit te wisselen. De uitgewisselde sleutel wordt vervolgens gebruikt voor traditionele encryptie die niet door quantumcomputers te ontcijferen is, of voor post-quantum cryptografie. PQC bestaat uit nieuwe vormen van encryptie die – voor zover bekend – niet door quantumcomputers te kraken zijn.
Voor QKD zijn quantumnetwerken nodig die, in plaats van digitale informatie, quantuminformatie kunnen sturen. Vooral over lange afstanden is dit nog een grote uitdaging.
Op termijn zal de toegang tot quantumcomputers waarschijnlijk vergemakkelijkt worden doordat deze ook als clouddienst beschikbaar komen.

Impact

Zonder ingrijpen is al onze vertrouwelijke financiële, medische en bedrijfsvertrouwelijke informatie over enkele jaren inzichtelijk voor kwaadwillende (statelijke) actoren. Het is dus nodig dat organisaties nú de transitie starten naar quantumveilige beveiliging, ook zonder een wettelijke verplichting.
De overstap van klassieke encryptie naar PQC vereist aandacht en tijd. Niet alle organisaties zijn zich voldoende bewust van de noodzaak en urgentie. Daarnaast vereist het soms nieuwe hardware of protocollen. Veel sectoren werken met assets met een lange levensduur, die niet tussentijds softwarematig te upgraden zijn naar PQC.
De maatschappelijke impact wordt bepaald door de techbedrijven en hun ontwerpkeuzes, niet door wensen en verwachtingen van gebruikers en de maatschappij. Grote techbedrijven kunnen uitgroeien tot 'gatekeepers'. Niet alleen omdat zij de hardware beheren maar ook vanwege de software, die een essentieel onderdeel is van het kunnen inzetten van quantumtechnologie.
Deze impact is minder zichtbaar dan die van de eerste generatie quantumtechnologie, die bestond uit halfgeleiders, chips en lasers.
Terugvalopties en klassieke alternatieven voor digitale communicatie (zoals koeriersdiensten) raken uit beeld, terwijl de (quantum)dreigingen toenemen.

Zie ook

16 Cyberaanvallen worden onzichtbaarder en indirecter

18 Digitale autonomie hoog op politieke agenda

19 Groeiende focus op strategische autonomie van grondstoffen en halffabrikaten

27 Digitale weerbaarheidskloof tussen mkb en grootbedrijf

Opkomst van sensing-technologie

Impact **middel** Termijn **3-6 jaar**



Bij sensing-technologie gebruiken systemen meerdere typen sensoren die verzamelde sensordata combineren en in samenhang analyseren. Vaak met behulp van kunstmatige intelligentie (AI). Hierdoor ontstaan nieuwe toepassingen waarin systemen hun omgeving steeds nauwkeuriger waarnemen, begrijpen en hierop reageren. Twee belangrijke ontwikkelingen binnen sensing zijn 'Integrated Sensing and Communication' (ISAC) in 6G-mobiele netwerken en de opkomst van quantumsensoren.
ISAC combineert communicatie en waarneming door de radiogolven van 5G- en 6G-antennes niet alleen voor datatransmissie, maar ook voor detectie en metingen te gebruiken. Op een kruispunt kan het systeem bijvoorbeeld de aanwezigheid, positie en beweging van personen en voertuigen waarnemen en zo de verkeersveiligheid verbeteren.

Quantumsensoren maken extreem nauwkeurige metingen mogelijk door gebruik te maken van quantummechanische eigenschappen. Een veelbelovende doorbraak zijn nieuwe (quantum)sensoren die nauwkeurige plaatsbepaling mogelijk maken, zonder afhankelijkheid van GNSS-systemen. Algemeen geldt dat de mogelijkheden van quantumsensoren nog verder toenemen wanneer sensoren via een quantumnetwerk met elkaar worden verbonden, in plaats van via traditionele digitale netwerken.

Impact

Een positieve ontwikkeling voor de digitale infrastructuur is dat sensing netwerkoperators in staat stelt om kwetsbaarheden, storingen en prestatievermindering vroegtijdig te detecteren. Hiermee kunnen operators de continuïteit en beschikbaarheid van digitale infrastructuur verbeteren. Ook voor andere sectoren biedt de technologie nieuwe mogelijkheden. In industriële omgevingen draagt de ontwikkeling van sensing bij aan de opkomst van autonome productielijnen en ondersteunen sensoren - waaronder quantumsensoren - toepassingen zoals preventief onderhoud. Het is ook mogelijk de veiligheid van personeel te verbeteren, bijvoorbeeld door automatische valdetectie voor onderhoudsmedewerkers.
De keerzijde is dat toenemende verwerking van sensorgegevens leidt tot een sterke groei van dataverkeer, die vervolgens drukt op het schaarse frequentiespectrum. Omdat communicatie- en detectiefuncties hetzelfde frequentiespectrum delen, wordt frequentiebeheer complexer en minder voorspelbaar. Daarnaast maakt de analyse van sensordata steeds vaker gebruik van AI. Waar eerder vooral specifieke AI-systemen per toepassing werden ingezet, verschuift de ontwikkeling steeds vaker naar generatieve AI-systemen die verschillende soorten gegevens combineren en interpreteren. Dit roept vragen op over het eigenaarschap, beheer en gebruik van sensorgegevens. Ook zijn er toenemende zorgen over privacy, bijvoorbeeld omdat sensing (ongewenste) surveillance mogelijk maakt.

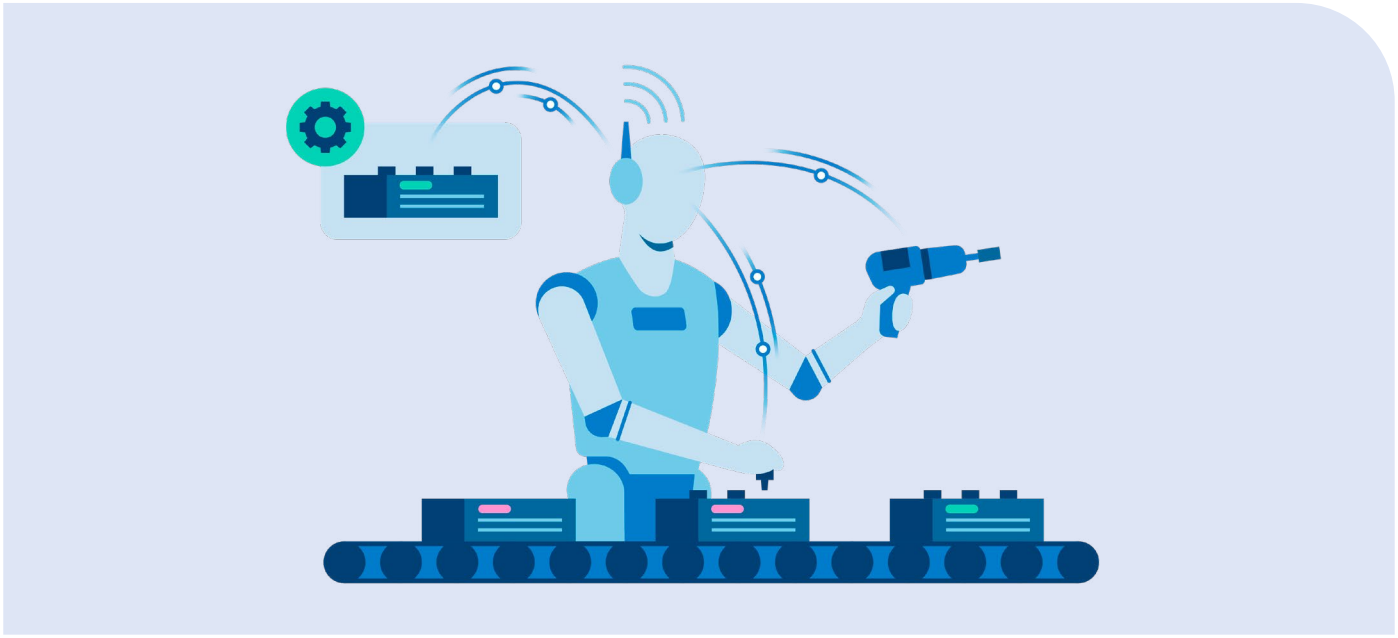
Geopolitieke ontwikkelingen stimuleren de ontwikkeling van nieuwe sensortechnologieën nog verder. Bijvoorbeeld voor drone-detectie en -identificatie, zowel voor civiele als militaire toepassingen. Hier speelt ook een bredere strategische vraag: zal Europa erin slagen een leidende positie te verwerven in de ontwikkeling van quantum- en 6G-standaarden en -hardwareproductie? Of zullen deze domeinen opnieuw voornamelijk worden bepaald door spelers uit China en de Verenigde Staten?

Zie ook

10 AI neemt fysieke vorm aan

AI neemt fysieke vorm aan

Impact **middel** Termijn **0-3 jaar**



Embodied AI combineert sensoren, verwerking van visuele data (‘computer vision’) en lerende algoritmen om robots, drones en voertuigen uit te rusten met de intelligentie om hun omgeving waar te nemen, beslissingen te nemen en doelgericht te handelen. De kracht van embodied AI zit in de wisselwerking tussen waarnemen, interpreteren en aansturen. AI verwerkt gegevens uit de omgeving en gebruikt deze om fysieke systemen direct aan te sturen.

Een embodied AI-systeem creëert nieuwe vormen van automatisering voor de samenleving. In gecontroleerde omgevingen zoals een fabriek met magazijnrobots, zal de impact anders zijn dan in de publieke ruimte. In een omgeving waar machines op hoge snelheid bewegen en nauw samenwerken met mensen, zijn low latency verbindingen cruciaal voor zowel de prestaties als de veiligheid.

Impact

Waar in beginstadia van AI de gevolgen vooral in de digitale wereld te zien waren, stapt Embodied AI met beide benen in de fysieke wereld, met mogelijk risico’s voor de fysieke veiligheid van mensen en goederen.

De grootschalige adoptie van embodied AI in drones en voertuigen blijft achter doordat systemen nog onvoldoende zorgvuldig en adaptief werken. Hierdoor zal de werkelijke impact van deze technologie pas op langere termijn volledig zichtbaar worden. Wanneer deze systemen echter op volle schaal worden uitgerold, zal het intensieve beroep op low-latency netwerken mogelijk leiden tot aanzienlijke netwerkcongestie.

AI versnelt wetenschapsbeoefening

Impact **laag** Termijn **>6 jaar**



De inzet van AI-technologieën leidt tot grote wetenschappelijke doorbraken, zoals het ontrafelen van het menselijk genoom, verbetering van klimaatmodellen dankzij verwerking van enorme hoeveelheden data, of het voorspellen van eiwitstructuren voor medicijnontwikkeling.

Aan de andere kant kent het gebruik van AI in de wetenschap ook een aantal nadelen. Er zijn zorgen over vooroordelen in algoritmen, de toename van hallucinaties, spookreferenties, en verzonnen gegevens. Ook is het mogelijk dat het gebruik van AI het kritisch denkvermogen doet afnemen.

De verwachting is dat de aanwas aan wetenschappelijke kennis enorm versnelt wanneer AI-research-bots zelf onderzoek gaan doen en dit combineren met en afzetten tegen het onderzoek van andere bots. Zo ontstaat er een netwerk van bots die met elkaar kennis opbouwen, zoals dit ook in de ‘menselijke’ wetenschapsgemeenschap gebeurt.

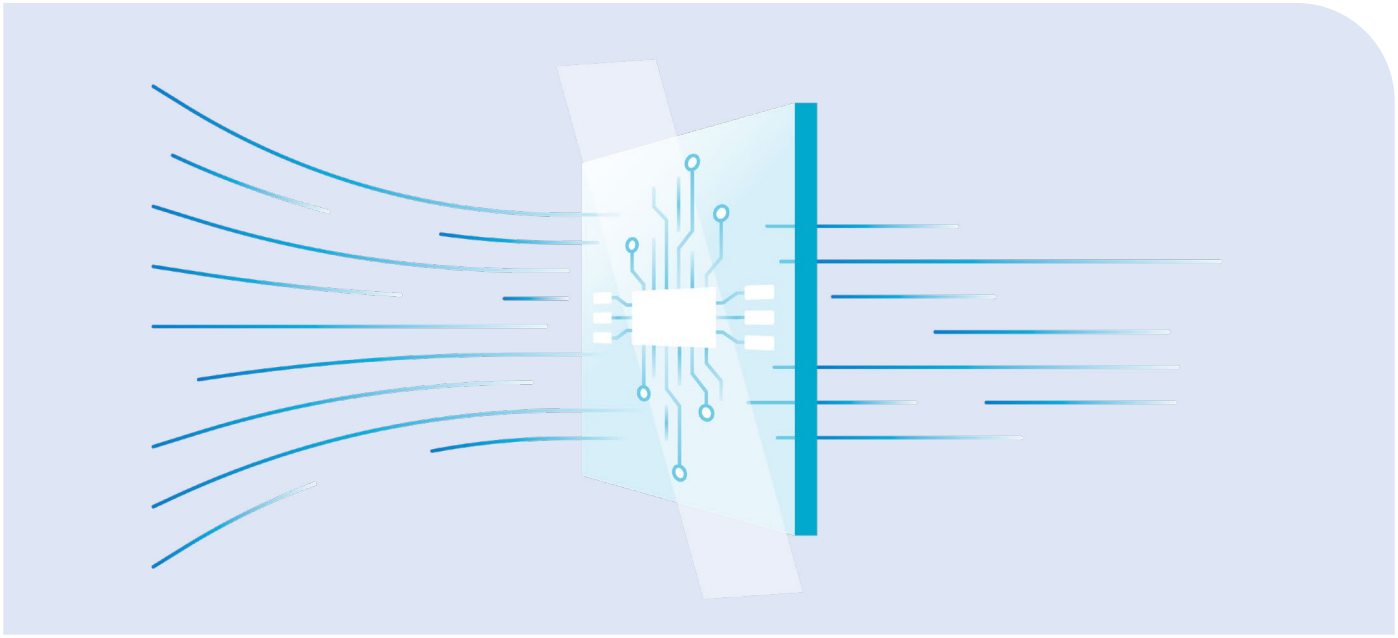
Impact

Net als andere vormen van AI zullen de research-bots om effectief te kunnen zijn een beroep doen op beschikbare dataruimte, bandbreedte, en rekenkracht.

Hier bovenop vraagt het om goede samenwerking tussen onderwijs- en onderzoeksinstellingen om datasets toegankelijk te maken, te koppelen en investeringen in (super)computers gezamenlijk te dragen.

Fotonische chips

Impact **laag** Termijn **>6 jaar**



Fotonische chips gebruiken licht in plaats van elektriciteit om informatie te vervoeren. Ze dragen bij aan een efficiëntere digitale infrastructuur door het transport van grote hoeveelheden data sneller en energiezuiniger te maken, omdat licht minder warmte genereert dan elektronen in koper. Momenteel vormen de chips vooral een aanvulling op traditionele elektronische chips voor datatransport op (ultra)korte afstand, met name interessant voor datacenters. Op de lange termijn is de verwachting dat fotonische chips ook zelf gaan rekenen, maar dit bevindt zich nog in de experimentele onderzoeksfase.

Impact

De grootste verwachte impact ligt in de verdere integratie van fotonische en elektronische chips. Hoe dichter de optische verbindingen bij processors worden toegepast, hoe sneller de gegevensoverdracht. Dit kan leiden tot hogere datasnelheden, een lager energieverbruik en minder warmteontwikkeling, waardoor datacenters efficiënter en duurzamer kunnen functioneren. Grootschalige adoptie wordt vooral verwacht door datacenters die zich focussen op AI, vanwege de enorme hoeveelheid data die zij verwerken.

Dataopslag in DNA veelbelovend, voorlopig buiten bereik

Impact **laag** Termijn **>6 jaar**



Bij synthetische DNA-opslag wordt informatie opgeslagen in kunstmatig geproduceerd DNA, in plaats van op traditionele opslagmedia, zoals harde schijven of SSD's. Digitale gegevens worden omgezet in een DNA-streng, die later kan worden uitgelezen met DNA-sequencing om de oorspronkelijke digitale informatie terug te vertalen.

DNA is geschikt voor het langdurig bewaren van grote hoeveelheden data, omdat het een hoge informatiedichtheid heeft en onder de juiste omstandigheden duizenden jaren stabiel blijft. Daadwerkelijk gebruik ligt in de verre toekomst, omdat DNA-synthese en DNA-sequencing momenteel nog duur en tijdrovend zijn. De verwachting is dat synthetische DNA-opslag in de toekomst vooral wordt ingezet voor archivering van gegevens die jarenlang of zelfs eeuwenlang bewaard moeten blijven.

Impact

De huidige impact van synthetische DNA-opslag op de digitale infrastructuur is beperkt, omdat de technologie nog te langzaam en te kostbaar is voor dagelijks gebruik. Op langere termijn kan DNA-opslag de digitale infrastructuur ingrijpend veranderen doordat het een alternatief biedt voor conventionele datacenters.
De opslagdichtheid van DNA is miljoenen keren groter dan die van huidige opslagmedia, waardoor enorme hoeveelheden data in een zeer klein volume kunnen worden opgeslagen. Voor de digitale infrastructuur betekent dit dat toekomstige datacenters mogelijk minder fysieke opslagruimte nodig hebben voor langetermijnarchieven.

Tegelijkertijd ontstaan nieuwe eisen aan de infrastructuur, zoals gespecialiseerde apparatuur voor DNA-synthese en DNA-sequencing, geautomatiseerde laboratoria en software die digitale bestanden betrouwbaar omzet naar DNA-codes en weer terug.

Geopolitieke ontwikkelingen

De digitale infrastructuur is steeds nadrukkelijker onderdeel van de geopolitiek: als middel én als doelwit. Allerlei vormen van cyberaanvallen, sabotage, of spionage worden ingezet om invloed uit te oefenen, informatie te verkrijgen of vitale systemen te ontwrichten. Dit vraagt om vooruitzien naar de impact van deze dreigingen en maatregelen om de impact te beperken. De digitale infrastructuur is veranderd van stil bezit in een geopolitiek machtsinstrument. Tegelijkertijd krijgt digitale autonomie nu steeds meer vorm.

Digitale infrastructuur als geopolitiek machtsinstrument

Impact **hoog** Termijn **0-3 jaar**



Recent zijn grootschalige, heimelijke aanvallen door statelijke actoren op de digitale infrastructuur sterk toegenomen. Deze zogenaamde hybride aanvallen nemen toe in aantal, intensiteit en diversiteit. Voorbeelden zijn hacking van vitale diensten, het verstoren van communicatiesignalen, desinformatiecampagnes vanuit vijandige staten en sabotage van fysieke infrastructuur.

De afgelopen jaren is de hybride dreiging continu toegenomen en de verwachting is dat dit verhoogde dreigingsniveau structureel wordt. Nederland bevindt zich in een 'grijze fase': we zijn niet openlijk in oorlog, maar het is ook geen vrede.

Impact

Cyberaanvallen kunnen leiden tot grootschalige uitval van essentiële diensten, zoals internet, betalingsverkeer of energievoorziening. Dergelijke verstoringen kunnen resulteren in maatschappelijke ontwrichting.

Bovendien is Nederland voor vitale onderdelen van de digitale infrastructuur afhankelijk van andere landen. Deze afhankelijkheid wordt nu en in de toekomst mogelijk nog vaker als drukmiddel benut in de geopolitiek.

De onvoorspelbaarheid van de ontwikkelingen vergroot de impact, omdat dit een goede voorbereiding bemoeilijkt.

Zie ook

16 Cyberaanvallen worden onzichtbaarder en indirecter

17 Toenemende inzet AI voor cyberaanvallen en -verdediging

18 Digitale autonomie hoog op politieke agenda

19 Groeiende focus op strategische autonomie van grondstoffen en halffabrikaten

Cyberaanvallen worden onzichtbaarder en indirecter

Impact **hoog** Termijn **0-3 jaar**



Hoewel de digitale infrastructuur steeds nadrukkelijker aanwezig is op het geopolitieke toneel, zijn de uitvoerders en betrokkenen bij cyberaanvallen op deze infrastructuur juist steeds moeilijker te identificeren.

Statelijke actoren vallen niet zelf aan, maar gebruiken proxy's (derde partijen, zoals criminele groepen) om aanvallen uit te voeren. Hiermee is de verantwoordelijkheid moeilijker terug te voeren tot de opdrachtgever. Ook zijn aanvallen indirecter, door leveranciers of onderaannemers in de toeleveringsketen als doelwit te gebruiken. Voorbeelden zijn de aanval op SolarWinds in 2020, de inbraak in bestandsoverdracht-programma Cleo in 2024 en misbruik van Citrix-kwetsbaarden in 2025.

Impact

Deze ontwikkeling verhoogt de kwetsbaarheid van de digitale infrastructuur doordat aanvallen en aanvallers moeilijker te traceren zijn. Ook worden steeds vaker minder zichtbare onderdelen van de digitale infrastructuur aangevallen. Dit betekent dat aanvallen nog moeilijker in kaart te brengen zijn en te bestrijden door autoriteiten.

De aanvallen vallen ook minder op doordat het midden- en kleinbedrijf vaker doelwit is dan grote bedrijven. Meerdere aanvallen op verschillende kleine bedrijven zijn minder zichtbaar dan één aanval op een groot bedrijf.

Zie ook

27 Digitale weerbaarheidskloof tussen mkb en grootbedrijf

Toenemende inzet AI voor cyberaanvallen en -verdediging

Impact **hoog** Termijn **0-3 jaar**



Aanvallers zetten slimme algoritmen in om kwetsbaarheden te identificeren, analyseren en uit te buiten. Traditionele cyberaanvallen, zoals ransomwa re, virussen en DDoS, worden in combinatie met AI-technieken sneller, grootschaliger en moeilijker te detecteren. AI verlaagt ook de benodigde technische kennis en vaardigheden om cybercriminaliteit te plegen. Met bijvoorbeeld 'Large Language Models' (LLM's) is het mogelijk om code voor het plegen van cybermisdrijven te genereren en aanvallen te automatiseren.

Vaak is effectieve verdediging alleen mogelijk door ook hier AI-technologie voor in te zetten. Bijvoorbeeld AI-methoden die deze aanvallen zelfstandig kunnen afweren en/of kwetsbaarheden vroegtijdig in kaart kunnen brengen en repareren.

Impact

Er zijn al voorbeelden bekend van door AI-systemen verbeterde adaptieve malware en cyberspionage, zoals de inzet van LAMEHUG in 2025 door een aan Rusland gelieerde hackersgroep, APT28. Grote impact wordt verwacht zodra AI-technieken nog meer (of volledig) autonoom kunnen opereren, en op grote schaal kritieke sectoren zoals telecom en energie kunnen ontwrichten. Door de complexiteit en adaptiviteit van AI-aanvallen, hebben organisaties minder tijd om kwetsbaarheden te repareren. Daardoor zijn traditionele cybersecuritymaatregelen sneller achterhaald.

Wanneer AI-systemen zelfstandig aanvallen gaan uitvoeren, wordt het nog moeilijker om de verantwoordelijkheid van een aanval aan een opdrachtgever toe te schrijven. De verwevenheid van AI met andere technologieën zoals quantum, satelliet en 6G zit nu nog in de onderzoeksfase, maar zal op termijn ook grote impact krijgen, omdat het de mogelijkheden en snelheid van aanvallen vergroot.

Positief is dat er in Nederland en de EU rekenkracht en expertise beschikbaar is, onder meer in (toekomstige) AI-fabrieken, onderzoeksinstituten en bij universiteiten. Deze wordt alleen nog beperkt ingezet voor weerbaarheid.

Zie ook

15 Digitale infrastructuur als geopolitiek machtsinstrument

18 Digitale autonomie hoog op politieke agenda

19 Groeiende focus op strategische autonomie van grondstoffen en halffabrikaten

29 Beschikbaarheid digitale infrastructuur onder druk

Digitale autonomie hoog op politieke agenda

Impact **hoog** Termijn **0-3 jaar**



De huidige geopolitieke spanningen vragen om maatregelen waarmee Europa meer grip krijgt op strategische afhankelijkheden binnen de digitale infrastructuur. Deze opgave wordt urgenter doordat de Verenigde Staten en China voorlopen op Europa als het gaat om de ontwikkeling van digitale sleuteltechnologieën, zoals AI en quantumtechnologie.

Verder komen digitale standaarden steeds vaker uit Azië, met name uit China en India. De standaarden uit deze landen zijn veelal gericht op het bevorderen van de eigen industrie. Dit leidt tot een afname van Europese en Nederlandse invloed en kan Europese bedrijven op een achterstand zetten.

Om minder afhankelijk van niet-Europese technologie te worden, wordt, met een stevige Europese en Nederlandse politieke agenda, meer digitale autonomie door Europese overheden en bedrijfsleven nagestreefd.

Deze nieuwe focus brengt ook kansen met zich mee om nationale en Europese initiatieven te ontplooien en het investeringsklimaat te verbeteren. Een voorbeeld hiervan is Gaia-X. Dit is een Europees initiatief om een federatieve data-en cloudinfrastructuur te ontwikkelen.

Impact

Ongewenste afhankelijkheden van (niet-)statelijke actoren op de digitale infrastructuur kunnen zorgen voor inmenging, en verhogen de kans op uitval, verstoringen of sabotage. Volledige onafhankelijkheid van niet-Europese landen is echter haalbaar noch wenselijk. Productie van eigen middelen die buiten Europa erg gewild zijn is daarentegen wel een belangrijke strategische optie.

De Europese digitale autonomie agenda leidt tot een bewustere afweging van risico's en tot actieve inzet op de eigen weerbaarheid van de systemen.

Groeiende focus op strategische autonomie van grondstoffen en halffabricaten

Impact **hoog** Termijn **3-6 jaar**



Voor strategische grondstoffen en vitale technologie, zoals zeldzame metalen die nodig zijn voor de productie van glasvezel of chips, en de geproduceerde chips zelf zijn we afhankelijk van lange, complexe en mondiale ketens. In deze ketens zijn specifieke schakels in handen van bepaalde landen. Taiwan is bijvoorbeeld dominant in de productie van chips (TSMC), en China heeft veel kritieke grondstoffen voor het produceren van chips en batterijen.

Het kabinet heeft in juni 2026 de 'Kritieke grondstoffenlijst' gepubliceerd. Dit initiatief benadrukt het belang van strategische autonomie voor deze grondstoffen.

Om autonomer te worden wordt ingezet op Europese alternatieven daar waar mogelijk, diversifiëren en versterken van de eigen voorsprong, en het recyclen van materialen en circulariteit.

Impact

De afhankelijkheid van een klein aantal landen en bedrijven maakt de digitale infrastructuur gevoelig voor geopolitieke spanningen, handelsbeperkingen en verstoringen in de toeleveringsketen. Hierdoor kunnen de beschikbaarheid en het onderhoud van netwerken, datacenters en telecomvoorzieningen onder druk komen te staan.

Tekorten aan halfgeleiders, glasvezelcomponenten of andere essentiële onderdelen kunnen leiden tot vertragingen bij de aanleg, vervanging en doorontwikkeling van digitale infrastructuur. Dit vergroot de risico's voor de continuïteit van vitale digitale diensten.

Buitenlandse inmenging verzwakt verdienvermogen Nederland

Impact **middel** Termijn **3-6 jaar**



Met economische veiligheid wordt de weerbaarheid van onze economie tegen ongewenste beïnvloeding en het misbruik van economische activiteiten voor geopolitiek e doeleinden bedoeld. Dergelijke activiteiten kunnen een risico vormen voor de nationale veiligheid. Zo kunnen buitenlandse bedrijven of investeerders die handelen vanuit geopolitieke belangen toegang verkrijgen tot gevoelige informatie, technologie, innovaties en bedrijfsprocessen. Dit kan plaatsvinden via spionage, maar ook via overnames van of investeringen in ondernemingen met strategische kennis of technologie, of een cruciale positie in de vitale infrastructuur. Dit gebeurt zowel in Europees als Caraïbisch Nederland. We kunnen strategische kennis en concurrentievermogen verliezen en afhankelijker worden van buitenlandse partijen en toeleveringsketens. Op de langere termijn kan dit leiden tot zowel economische als politieke afhankelijkheid.

Impact

Strategische afhankelijkheden kunnen ertoe leiden dat de digitale infrastructuur achterblijft in innovatie en kennisontwikkeling. Dit is moeilijk in te halen, en op termijn misschien helemaal niet meer.

Zie ook

18 Digitale autonomie hoog op politieke agenda

19 Groeiende focus op strategische autonomie van grondstoffen en halffabrikaten

22 Wetgeving in spagaat tussen risicobeheersing en digitale innovatie

Maatschappelijke ontwikkelingen

Maatschappelijke ontwikkelingen zijn politieke, economische, sociale, ecologische en juridische veranderingen die impact hebben op de inrichting van onze samenleving en ons dagelijks leven. Door de lens van de digitale infrastructuur zien we hier een grote verscheidenheid aan ontwikkelingen. We benoemen bijvoorbeeld de onmisbaarheid van de digitale infrastructuur voor het functioneren van de samenleving, terwijl andersom veranderingen in regeldruk, klimaatverandering en tekorten op de arbeidsmarkt nieuwe uitdagingen voor de digitale infrastructuur met zich meebrengen.

Wetgeving in spagaat tussen risicobeheersing en digitale innovatie

Impact **hoog** Termijn **0-3 jaar**



De opeenstapeling van Europese wetgeving, zoals de GDPR, NIS2, DORA, de Data Act en de AI-verordening, maakt naleving steeds complexer en kostbaarder. Dit verslechtert de concurrentiepositie en zorgt voor scheve verhoudingen in de markt. Want waar grotere, kapitaalkrachtige bedrijven makkelijker compliance-kosten opbrengen, worden kleinere organisaties hierdoor zwaar belast. Het bedrijfsleven pleit daarom voor minder regeldruk. Overheden nemen deze signalen over en de Europese Unie zet in op vereenvoudiging van regelgeving.

Tegelijkertijd is deze regelgeving essentieel voor een veilige en betrouwbare digitale samenleving. Wettelijke eisen rond cybersecurity, privacy en grondrechten dragen bij aan vertrouwen in digitale systemen en vormen een belangrijke randvoorwaarde voor verantwoorde innovatie.

Impact

Vereenvoudiging van regels kan ertoe leiden dat risico's in de toepassing van digitale technologieën minder goed zijn afgedekt.

Daarnaast maakt een wispelturige wetgever het voor bedrijven minder voorspelbaar waar zij aan moeten voldoen en hoe wetgeving zich inhoudelijk verder ontwikkelt.

In Caribisch Nederland is er niet altijd een directe doorvertaling van bovengenoemde Europese wetgeving waardoor de verandering in regeldruk minder van toepassing kan zijn.

Zie ook

5 Meer vraag naar frequentiespectrum vergroot schaarste en kwetsbaarheid

11 AI versnelt wetenschapsbeoefening

15 Digitale infrastructuur als geopolitiek machtsinstrument

20 Buitenlandse inmenging verzwakt verdienvermogen Nederland

27 Digitale weerbaarheidskloof tussen mkb en grootbedrijf

Alle aspecten van ons leven doordrongen van digitale infrastructuur

Impact **hoog** Termijn **0-3 jaar**



De afhankelijkheid van digitale infrastructuur neemt toe doordat steeds meer systemen, processen en apparaten zijn aangesloten op de digitale infrastructuur. Denk bijvoorbeeld aan energie- en watervoorziening, betalingsverkeer of communicatie. Deze trend is al jaren aan de gang. Met name de steeds verdergaande vervlechting met het persoonlijke, dagelijkse leven is opzienbarend.

Hoe om te gaan met de groeiende afhankelijkheid van de digitale infrastructuur is één van de grootste vraagstukken van nu en de nabije toekomst. Er zijn veel verschillende toekomstscenario's mogelijk, van verdere stimulering van digitale groei door overheid en bedrijfsleven tot meer fragmentatie van het digitale landschap door geopolitieke ontwikkelingen en maatschappelijke weerstand.

Er zijn nu maatschappelijke bewegingen zichtbaar die bewust nadenken over (meer) onafhankelijkheid van de digitale infrastructuur. Dit uit zich in meer aandacht voor autonomie, zelfredzaamheid en het zoeken naar technologische alternatieven. Recente geopolitieke en culturele ontwikkelingen laten op kleine schaal zien dat de interesse groeit in alternatieven die analoog of zelfstandig opereren, zoals decentrale en lokale netwerken, microgrids en thuisbatterijen.

Ook zien we dat de maatschappelijke afhankelijkheid van de digitale infrastructuur op andere manieren tegen de grenzen aanloopt, door ruimte-, water- of energiegebrek.

Impact

De sterke verwevenheid van digitale infrastructuur met maatschappelijke en economische processen vergroot de gevolgen van verstoringen, die tot diep in het persoonlijke leven reiken. Uitval van één onderdeel kan leiden tot keteneffecten in andere sectoren en processen.

Zie ook

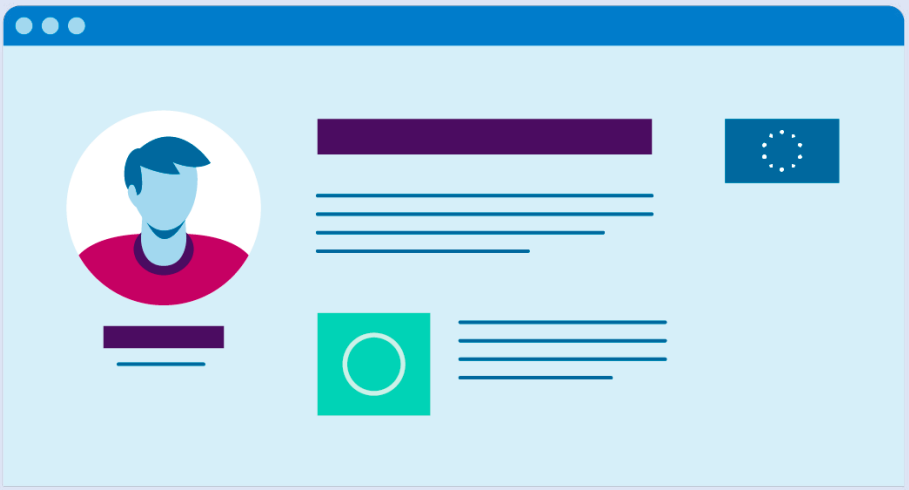
15 Digitale infrastructuur als geopolitiek machtsinstrument

18 Digitale autonomie hoog op politieke agenda

22 Wetgeving in spagaat tussen risicobeheersing en digitale innovatie

Synthetische identiteiten verhogen druk op digitale vertrouwensstelsels

Impact **middel** Termijn **<3 jaar**



Een nieuwe uitdaging voor vertrouwen in de digitale wereld is de vloed aan informatie die door AI wordt gegenereerd. Waar er voorheen vaak hooguit 'geknoeid' werd met media als foto en video kunnen media nu snel maar levensecht vanaf de grond af worden opgebouwd. Een onderwerp waar dit grote impact op heeft is digitale identiteit. Steeds vaker worden met behulp van AI bijvoorbeeld 'deepfakes' gegenereerd, die ingezet worden om digitale identiteiten te vervalsen om zo identiteitsfraude te kunnen plegen. Ook volledig door AI gegenereerde (sythentic) identiteiten komen steeds meer voor.

Impact

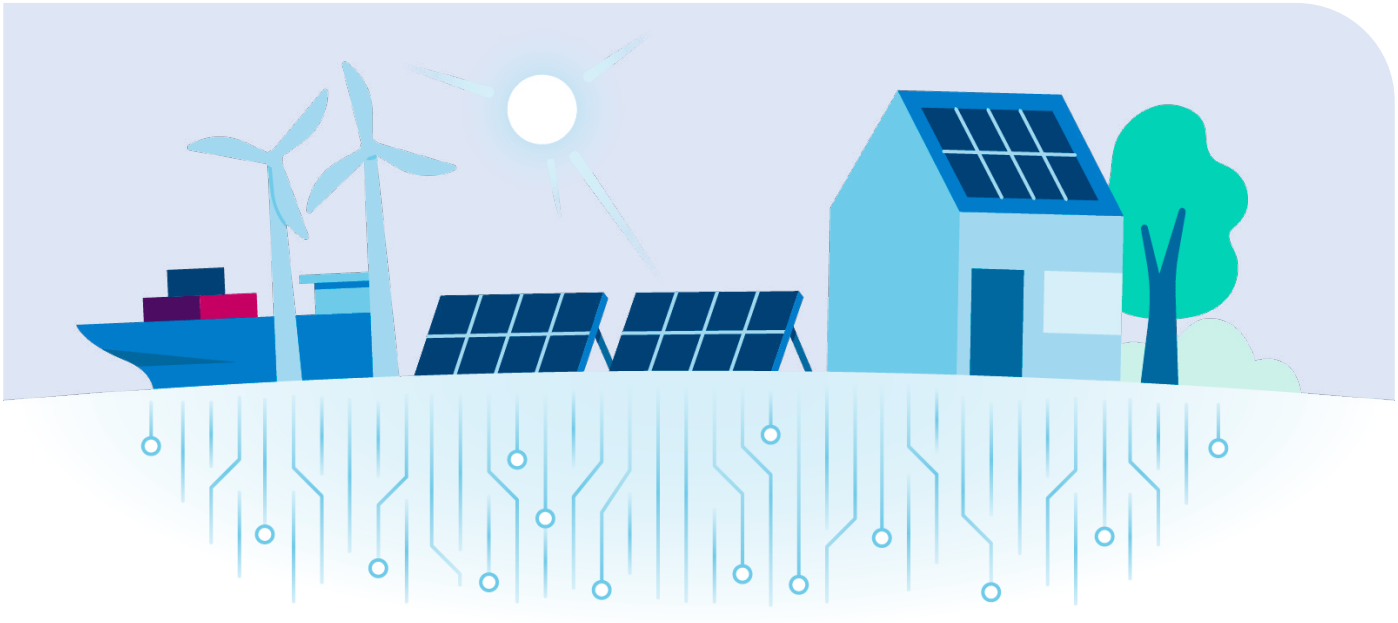
Het wordt steeds moeilijker om vast te stellen of digitale informatie authentiek is. Tegelijkertijd neemt het gebruik van digitale identiteiten toe.

Een mogelijke oplossing voor de toenemende hoeveelheid door AI gegenereerde content wordt gezocht in digitale herkomst (digital provenance). Hierbij worden de oorsprong en wijzigingsgeschiedenis van een bestand vastgelegd in de metadata. Dit vereist breed geaccepteerde technische standaarden, maar ook een afweging tussen transparantie over de totstandkoming van een bestand en de privacy van betrokkenen.

De groeiende rol van digitale identiteit zien we terug in maatschappelijke en politieke discussies, bijvoorbeeld over online anonimiteit en leeftijdsverificatie op sociale media. De herziene eIDAS-verordening speelt hierop in. Uiterlijk eind 2026 moeten alle EU-lidstaten een digitale wallet aanbieden, waarmee inwoners identiteitskenmerken veilig online kunnen delen. Bijvoorbeeld uitsluitend de bevestiging dat zij ouder zijn dan 18 jaar.

Toenemend beslag op energie en water

Impact **middel** Termijn **<3 jaar**



Een grote stijging van verbruik van energie en water ontstaat door een toenemend aantal datacenters, High Power IoT, 5G/6G en AI. Dit leidt tot (lokale) overbelasting van elektriciteitsnetten en concurrentie met andere sectoren om elektriciteitsaansluitingen. Meer inzet op redundantie verhogen het verbruik nog verder.

Ook watertekorten leiden tot beperkingen, zowel voor gebruik van de digitale infrastructuur als het maken van nieuwe onderdelen (chips en hardware). De digitale infrastructuur concurreert ook met andere sectoren zoals drinkwatervoorziening en landbouw, met name in Zuid-Holland.

Impact

Door de groeiende behoefte aan energie ontstaat er schaarste en uitval door overbelasting. Deze ontwikkeling belemmert de beschikbaarheid, continuïteit en groei van de digitale infrastructuur. Andersom hindert uitval van digitale infrastructuur ook de continuïteit van stroomlevering.

Er ontstaat concurrentie om nieuwe aansluitingen, bijvoorbeeld tussen datacenters en woningbouw. Dit betekent een verslechtering van het vestigingsklimaat. De toenemende druk op de energievoorziening uit zich ook in hoge energiekosten voor datacenters en netwerken, met als gevolg mogelijke prijsstijgingen voor eindgebruikers.
Bovendien schuilt er een geopolitiek risico in de bestaande afhankelijkheid van fossiele brandstoffen voor de productie van elektriciteit.

Deze ontwikkeling werkt ook ongelijkheid in de hand: alleen eindgebruikers met voldoende middelen en ruimte voor back-ups (zoals brandstoffen en batterijen) kunnen zichzelf voorzien bij uitval.

Een mogelijke positieve impact van de noodzaak om efficiënter om te gaan met energie, water en grondstoffen is dat het de ontwikkeling stimuleert van bijvoorbeeld energiezuinigere netwerken, efficiëntere chips en neuromorphic computing.

Zie ook

12 Fotonische chips

31 Extemer weer vergroot kwetsbaarheid digitale infrastructuur

Instroom niet-conforme apparatuur vergroot veiligheidsrisico's

Impact **middel** Termijn **0-3 jaar**



Sinds de coronapandemie is er naast de reguliere containerstromen een moeilijk beheersbare stroom van individuele e-commercepakketten ontstaan. Deze pakketten komen vaak via lichtere douanecontroles de EU binnen. Nederland speelt hierin een sleutelrol als doorvoerland: sinds 2024 passeren jaarlijks meer dan 1 miljard pakketten onze grenzen.

De bijbehorende aangiftes zijn vaak onjuist of onvolledig, waardoor toezichthouders beperkt zicht hebben op de inhoud. 85 tot 95% van de producten voldoet niet aan EU-regelgeving, bijvoorbeeld op het gebied van cyberbeveiliging.

Sinds 1 juli 2026 is er een EU-heffing (fee) op pakketjes. Het sturen van individuele pakketjes zal daarmee enigszins afnemen. Maar tegelijk zullen VLOPS ('very large online platforms', zoals grote internationale webwinkels) in toenemende mate gebruik gaan maken van distributiecentra in de Europese Unie. Hierdoor zal er een verplaatsing plaatsvinden van de pakkettenstroom, maar niet per se een afname.

Impact

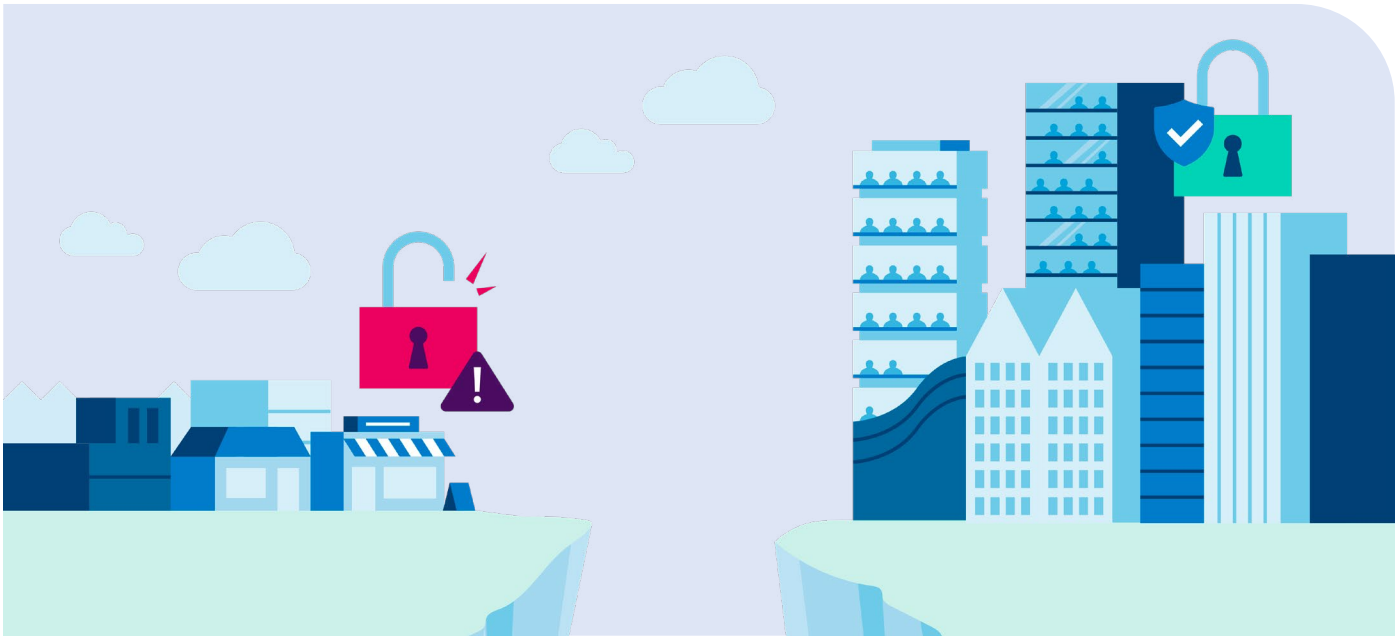
De instroom van niet-conforme producten (zoals apparatuur met draadloze communicatie en IoT-devices) veroorzaakt meer verstoringen in het radiofrequentiespectrum. Daarnaast kunnen storingen in kritieke systemen ontstaan, bijvoorbeeld in de communicatie van hulpdiensten. Ook nemen de veiligheidsrisico's voor consumenten toe, zoals brandgevaar door onveilige opladers, kwetsbaarheden door apparaten met malware en blootstelling aan schadelijke stoffen.

Zie ook

27 Digitale weerbaarheidskloof tussen mkb en grootbedrijf

Digitale weerbaarheidskloof tussen mkb en grootbedrijf

Impact **middel** Termijn **0-3 jaar**



Net als het grootbedrijf opereert het mkb binnen ketens die kritiek zijn voor de digitale infrastructuur. Tegelijkertijd blijft de cyberweerbaarheid van het mkb achter, vooral bij complexere maatregelen zoals data-encryptie. Dit terwijl het aantal cyberaanvallen op het mkb toeneemt. Deze groeiende kloof in cyberweerbaarheid tussen mkb en grootbedrijf maakt kritieke systemen kwetsbaarder. Dat geldt met name voor bedtrijven die een kritieke rol binnen de keten vervullen.

Impact

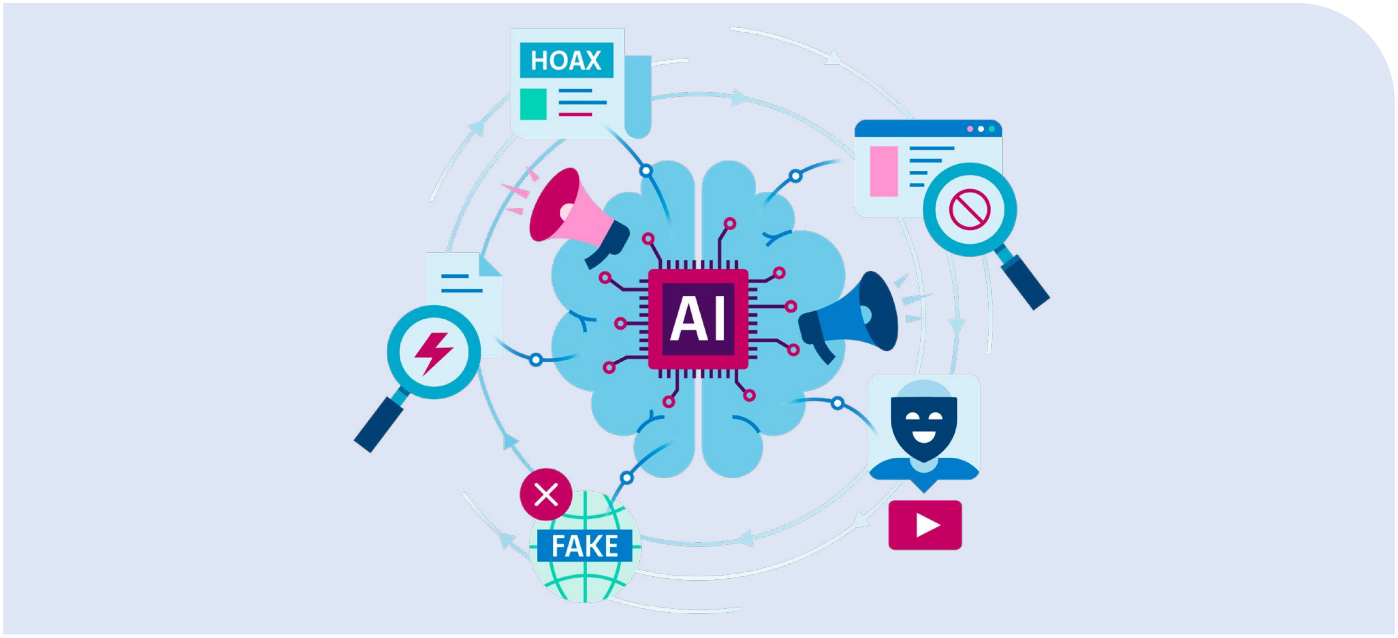
Het mkb is een belangrijke schakel van de Nederlandse economie en van de digitale infrastructuur. Structurele beperkingen van de digitale weerbaarheid van het mkb, betekenen een verhoogde kwetsbaarheid van de hele digitale infrastructuur.

Zie ook

29 Beschikbaarheid digitale infrastructuur onder druk

De vicieuze cirkel van AI en desinformatie

Impact **middel** Termijn **0-3 jaar**



Generatieve AI maakt het mogelijk om snel, goedkoop en op grote schaal overtuigende misleidende teksten, beelden en audio te creëren en gericht te verspreiden. Vervolgens kan desinformatie uit online beïnvloedingscampagnes terechtkomen in de trainingsdata of informatiebronnen van AI-systemen, waardoor deze misleidende informatie gaan reproduceren.

Impact

Desinformatie heeft geen directe impact op de digitale infrastructuur zelf, maar kan wel de benutting van die infrastructuur beïnvloeden, zoals door het aantasten van het vertrouwen van burgers in digitale diensten, overheidscommunicatie of online informatievoorziening.

Zie ook

15 Digitale infrastructuur als geopolitiek machtsinstrument

Beschikbaarheid digitale infrastructuur onder druk

Impact **hoog** Termijn **3-6 jaar**



Nederland kent hoge percentages van beschikbaarheid en bereikbaarheid van de kritieke infrastructuur (>99,98%). De vraag is hoe houdbaar deze niveaus zijn, gezien de sterke toename van hybride dreigingen die de digitale infrastructuur verstoren.

Daarom klinkt de oproep om in te zetten op robuuste en weerbare digitale diensten. Dat is niet hetzelfde als de garantie dat digitale diensten continu beschikbaar zijn. Robuustheid en weerbaarheid vergroten het vermogen om verstoringen op te vangen en de continuïteit van essentiële diensten te waarborgen wanneer deze zich voordoen.

Deze ontwikkeling betekent een breuk met het huidige beleid en de maatschappelijke verwachting dat digitale infrastructuur altijd beschikbaar en bereikbaar is. Oproepen tot voorbereiding kunnen ervoor zorgen dat gebruikers uitval minder als disruptie ervaren en meer als een te verwachten incident.

Impact

De kwaliteit en continuïteit van de digitale infrastructuur zal minder vanzelfsprekend worden. Specifieke partijen zouden daarbij voorrang kunnen krijgen qua beschikbaarheid, zoals nu ook met stroom gebeurt. Daarmee kunnen de verwachtingen van hoe betrouwbaar de infrastructuur is, aangetast worden. Ook kan er een digitale kloof ontstaan tussen de partijen die meer en minder (stabiele) toegang hebben tot de digitale infrastructuur. Dit kan ook invloed hebben op het bredere maatschappelijke vertrouwen in digitale systemen en de concurrentiepositie van Nederland. In Caribisch Nederland is de verwachting van beschikbaarheid al anders doordat er frequentere dreigingen zijn vanuit weersomstandigheden en de redundantie beperkt is.
Deze beweging kan de behoefte aan analoge alternatieven aanwakkeren, wat juist tot meer redundantie zal leiden.

Zie ook

5 Meer vraag naar frequentiespectrum vergroot schaarste en kwetsbaarheid

27 Digitale weerbaarheidskloof tussen mkb en grootbedrijf

Tekort professionals zet beschikbaarheid en innovatie onder druk

Impact **middel** Termijn **3-6 jaar**



Het aanhoudende tekort aan ICT-professionals blijft naar verwachting bestaan, ook op de lange termijn, want de instroom neemt zowel in het voortgezet als in het hoger onderwijs niet toe. Demografische ontwikkelingen versterken het tekort: door vergrijzing stromen ervaren professionals uit, terwijl minder jongeren instromen. Ook zijn er zorgen over de kwaliteit van de instroom, met dalende PISA-scores in lezen, wiskunde en natuurwetenschap.

Automatisering, met name AI, kan delen van het ICT-werk overnemen en tekorten deels opvangen. Tegelijkertijd neemt AI vooral delen van junior-ICT-werk over. Hierdoor kunnen op termijn minder professionals doorgroeien naar seniorfuncties, waardoor tekorten aan ervaren ICT-professionals ontstaan.
Nederland kan met relatief hoge salarissen nationale en internationale professionals aantrekken. Of dit, in combinatie met automatisering, voldoende is om het tekort op te vangen, blijft onzeker.

Impact

Het wordt waarschijnlijk ingewikkelder om met de beperkt beschikbare professionals de digitale infrastructuur op peil te houden, van onderhoudsmonteurs tot cybersecurityspecialisten. Ook lopen we het risico dat de prioriteit verschuift naar enkel hoognodig onderhoud en het oplossen van incidenten (‘brandjes blussen’), terwijl structurele innovatie naar de achtergrond verdwijnt.

Zie ook

29 Beschikbaarheid digitale infrastructuur onder druk

Extremer weer vergroot kwetsbaarheid digitale infrastructuur

Impact **middel** Termijn **>6 jaar**



Betrouwbaarheid van energie en digitale connectiviteit wordt bedreigd door extreem weer, dat vaker voorkomt en minder voorspelbaar wordt. Juist dan is betrouwbare communicatie van levensbelang.
Extreme neerslag, hittegolven, wind en grondverzakkingen kunnen leiden tot schade aan datacenters, zendmasten, kabels en elektriciteits-infrastructuur. Dit kan zorgen voor uitval van communicatie, falende koelsystemen, oververhitting en verlies van data.
De risico's verschillen per gebied. In Europees Nederland spelen vooral overstroming, hitte en stormschade een rol. In Caribisch Nederland zijn de risico's groter door de geografische ligging en de blootstelling aan extreme weersomstandigheden. Orkanen veroorzaakten op de eilanden al meermaals uitval van essentiële of zelfs totale communicatie.

Impact

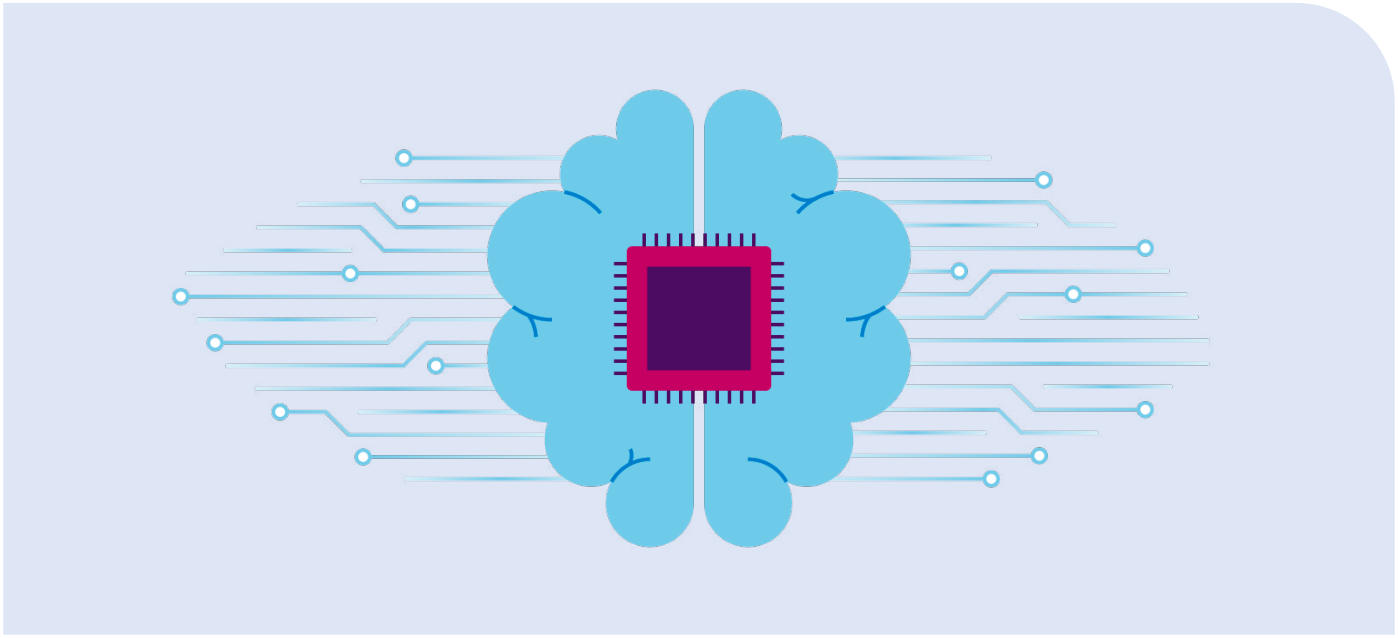
In Europees Nederland is het grootste risico van overstroming nabij rivieren en onder NAP, waar het merendeel van de datacenters staat.
Bij stormschade aan antennes is vervangend materiaal niet of nauwelijks aanwezig. Hierdoor ontstaat grootschalige uitval van digitale infrastructuur met mogelijk lange hersteltijden.
In Caribisch Nederland vergroten orkanen, zeespiegelstijging en erosie de kwetsbaarheid van de telecommunicatie-infrastructuur.
Redundantie is beperkt: één onderzeese kabel of zendmast kan hele delen van de eilanden offline halen. Zendmasten en satellietverbindingen zijn kwetsbaar voor wind en bliksem. Hierdoor ontstaat uitval van digitale infrastructuur met impact op de economie en vitale sectoren.
Datacenters zijn schaars, maar wel uitgerust met dieselgeneratoren en back-up batterijen. Herstel kan langere tijd duren door beperkte logistiek en voorraden. De toenemende kwetsbaarheid vraagt om investeringen in de telecommunicatie-infrastructuur om de continuïteit ervan te kunnen waarborgen.
Innovatieve oplossingen zoals hurricane-proof zendmasten, back-up via satelliet, microgrids met hernieuwbare energie, voorraden van kritieke onderdelen en waterbestendige of drijvende datacenters kunnen de weerbaarheid verhogen.

Zie ook

29 Beschikbaarheid digitale infrastructuur onder druk

Nieuwe mens-machine interfaces

Impact **laag** Termijn **>6 jaar**



De manier waarop mensen met de digitale wereld communiceren verandert. We benaderen de digitale wereld nu nog veelal via het glazen scherm van een smartphone of tablet waar we naar staren, op swipen en tappen. Maar nieuwe interfaces dienen zich aan. Technologieën zoals augmented reality (AR), virtual reality (VR), mixed reality (MR) en neurotechnologie markeren een fundamentele verschuiving in de interactie tussen mens en technologie.

Met AR, VR en MR wordt de fysieke werkelijkheid aangevuld of vervangen door digitale objecten en omgevingen. AR, VR en MR zijn inmiddels commercieel beschikbaar. Een brede doorbraak is vooralsnog uitgebleven, uitgezonderd niche-toepassingen zoals head-up displays in auto's of in videogames. Desalniettemin is de verwachting dat dit op de langere termijn gaat veranderen, want er wordt fors in geïnvesteerd door grote bedrijven.

Hetzelfde geldt voor neurotechnologie, dat directe communicatie tussen hersenen en machines mogelijk maakt, en op termijn mogelijkheden biedt om menselijk gedrag of cognitieve processen te beïnvloeden. Op dit moment zijn er vooral toepassingen in het medische domein, maar op de middellange termijn kan neurotechnologie klaar zijn voor introductie in consumentenproducten.

Impact

Door technologische beperkingen, maatschappelijke en ethische vraagstukken worden grootschalige brain-to-machine-interfaces voorlopig nog niet verwacht. Ook zijn er grote juridische vraagstukken; neurotechnologie is nog geen expliciet onderdeel van wetgeving op het gebied van AI, privacy of productveiligheid.

Hiernaast stellen neurotechnologische toepassingen en geavanceerde AR/VR-systemen, zoals (AI-gestuurde) real-time vertaling, objectherkenning en gedragsanalyse, hoge eisen aan de onderliggende digitale infrastructuur. Deze toepassingen en systemen zijn afhankelijk van snelle en betrouwbare 5G- en toekomstige 6G-netwerken, gecombineerd met lokale dataverwerking ('edge computing') om de vertraging te beperken. Ook stelt deze ontwikkeling hogere eisen aan de veiligheid van systemen om privacygevoelige gegevens te beschermen.

Een belangrijk risico van geavanceerde mens-machine-interfaces is de kwetsbaarheid voor cyberaanvallen. Overheden besteden daarom steeds meer aandacht aan de regulering van neurotechnologie. Zo was Chili in 2021 het eerste land dat specifieke wetgeving invoerde ter bescherming van neurologische gegevens. In Europa wordt onderzocht hoe neurotechnologie past binnen bestaande kaders zoals de AVG en de AI-verordening.

Zie ook

23 Alle aspecten van ons leven doordrongen van digitale infrastructuur

Tot slot

Deze vijfde editie van de Trendradar bood een actueel overzicht van 26 ontwikkelingen waarvan we verwachten dat deze de digitale infrastructuur de komende tien jaar zullen vormgeven. Deze ontwikkelingen vragen om voortdurende aandacht en aanpassingsvermogen. De RDI houdt in haar toezicht continu rekening met deze ontwikkelingen. Of het nu gaat om de impact van AI, de kwetsbaarheid van onderzeese datakabels of de toenemende druk op energievoorzieningen: het is zaak om nú de juiste stappen te zetten. Dit rapport laat zien welke ontwikkelingen op de radar staan, maar de vertaling naar beleid, investeringen en samenwerking is aan ons allemaal.

Deze Trendradar is tot stand gekomen dankzij de inbreng van vele experts, stakeholders en collega's binnen en buiten de RDI. Wij danken iedereen die heeft bijgedragen.

Vragen, suggesties of verdere dialoog zijn altijd welkom via trendradar@rdi.nl

Bronnen

- ABN AMRO - Mkb vaker doelwit van cybercrime dan grootbedrijf
- Adviescollege toetsing regeldruk (ATR) - ATR opent meldpunt signalen regeldruk
- AIVD - Dreigingsbeeld Statelijke Actoren 2025
- AIVD - Tussen vrede en oorlog. De oorlog in Oekraïne en de Russische dreiging in Europa
- Allianz - Code, carbon, kilowatts: AI's hidden toll and the race to green the grid
- Centraal Bureau voor de Statistiek (CBS) - Datacenters verbruiken 4,6 procent van de elektriciteit
- Centre for Emerging Technology and Security (CETaS) - Adding Fuel to the Fire: AI Information Threats and Crisis Events
- Centre for Emerging Technology and Security (CETaS) - Beyond Spam Bots: The Rise of AI-Powered Disinformation Machines and the Imperative for Strategic Response
- Clingendael - Nederland en de EU: Benoem, bescherm en beheer strategische digitale infrastructuur
- College voor de Rechten van de Mens - EU-wetswijzingen 'digitale omnibus' zorgelijk voor grondrechten
- Cyber Security Raad (CSR) - AI als wapen bedreigt digitale veiligheid
- Denk vooruit - Uitval telecommunicatie
- Digital Forensic Research Lab (DFRLab) - Russia-linked Pravda network cited on Wikipedia, LLMs, and X
- Europese Commissie - Space Traffic Management
- Gaia-X Hub the Netherlands
- Joint Research Centre (JRC) - The Role of Artificial Intelligence in Scientific Research
- KNMI - KNMI'23-klimaatscenario's
- Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) - Cybersecuritybeeld Nederland 2025
- Nationaal Cyber Security Centrum (NCSC) - Anthropic's frontiermodel Mythos vraagt om directe actie
- Nationaal Cyber Security Centrum (NCSC) - Cybersecuritymonitor 2025: minder cyberaanvallen, weerbaarheidskloof blijft
- Nationaal Groeifonds - Creative Industries Immersive Impact Coalition (CIIIC)
- Nationaal Groeifonds - PhotonDelta
- Planbureau voor de Leefomgeving (PBL) - Strategische autonomie vraagt om regio- en bedrijfstakspecifiek beleid
- Planbureau voor de Leefomgeving (PBL) - Voorbij de risico's: keuzes voor een klimaatbestendige leefomgeving
- Radboud Universiteit - De toekomst van dataopslag schuilt in microbolletjes met DNA
- Rathenau Instituut - Neurotechnologie
- Rijksinspectie Digitale Infrastructuur (RDI) - Toepassingen van 6G
- Rijksoverheid - Economische veiligheid | Maak je bedrijf weerbaar
- Rijksoverheid - Nieuwe visie legt fundament voor een autonome en soevereine digitale overheid
- Rijksoverheid - Ruimtelijk Ontwikkelingsprogramma Caribisch Nederland
- Rijksoverheid - Themarapportage Rijksbrede Risicoanalyse Caribisch deel van het Koninkrijk der Nederlanden
- Rijksoverheid - Verkenning van het raakvlak van cybersecurity en AI
- Sociaal-Economische Raad (SER) - Digitalisering: kansen en risico's
- Tweede Kamer der Staten-Generaal - Economische Veiligheid
- Tweede Kamer der Staten-Generaal - Kabinetsinzet nationale grondstoffenstrategie
- Tweede Kamer der Staten-Generaal -Nationale handling fee op e-commercezendingen
- UWV - ICT-beroepen in beeld
- Wetenschappelijke Raad voor het Regeringsbeleid (WRR) - Markt, overheid en strategische autonomie

Meer lezen op de website van RDI

- Rijksinspectie Digitale Infrastructuur (RDI) - De route naar digitale autonomie
- Rijksinspectie Digitale Infrastructuur (RDI) - Elektronische vertrouwensdiensten
- Rijksinspectie Digitale Infrastructuur (RDI) - Kunstmatige intelligentie (AI)
- Rijksinspectie Digitale Infrastructuur (RDI) - Nederlandse toezichthouders: gezamenlijke aanpak e-commerce producten nodig om consumenten te beschermen
- Rijksinspectie Digitale Infrastructuur (RDI) - Onderzoek dynamisch spectrumgebruik
- Rijksinspectie Digitale Infrastructuur (RDI) - Quantumcomputers en digitale weerbaarheid: waarom organisaties nu al moeten handelen

Dit is een uitgave van
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Emmasingel 1 Groningen
088 - 041 60 00
info@rdi.nl
www.rdi.nl

Spetember 2026

#wijzijnRDI